Evaluating the Level of Cybersecurity Literacy Among Bachelor's Degree Students in Nepal

Authors:
Amrit Acharya[1] Oxford college of engineering and management
Biplov Bartaula[1] Oxford college of Engineering and Management
Kritish Devkota1 Oxford college of Engineering and Management
Saroj Dhungana[9] Oxford college of Engineering and Management
Arbin Chhatkuli[9] Oxford college of Engineering and Management
Ankur Ghimire[9] Oxford college of Engineering and Management
Basanta Prasad Adhikari (PHD)[2] Oxford Research Department

Introduction

Cybersecurity is the practice, method and tool that protect devices, network and hardware from digital threats and risk. It is the practice of protecting systems, networks, and programs from digital attacks. These cyberattack are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users through ransom or interrupting normal business processes. (Cisco, n.d.) In today's digital world where every aspect of work has been digitalized, cybersecurity has become a critical skill for everyone who use internet, especially students as they use internet most of the time. As the use of digital devices, online services increase so does the risk of cybercrime such as phishing, hacking and data breaches also increase. The teenage youth are more in the risk of cyberattack and awareness of cybersecurity is most important for them to make their digital engagement safe.

Statement of the Problem

The Education system of Nepal is gradually shifting towards digital platforms with online classes, digital assignments, internet-based research which becomes the common practices among students. However, many students have limited knowledge and awareness about cybersecurity which make them victim of cyber-attacks. They may not know how to protect their personal data, recognize cyber threats or safely use digital service. This gap in cybersecurity literacy can make students vulnerable to online threats, scams, data leaks and cyberbullying. There have been growing concerns about student mistakenly sending sensitive information, using weak passwords or clicking unknown links and harmful links. While most of the institution are working on improving IT infrastructure, they are giving less attention towards training and awareness for students. Without proper understanding, talented and tech savvy students may fall victim to cyber-attacks. Therefore, evaluating the present state of cybersecurity literacy among bachelor student in Nepal is important to identify various existing gaps and

address them through education and awareness program.

The Effects:

- Increased risks of cybercrime and data breaches.
- Affects educational integrity through cyber cheating.
- Leads to misuse of digital tools due to a lack of proper knowledge.
- Affects personal privacy and online reputation.
- Reduce student confidence in using online platforms.

Justification of the Research

This study is important because it shows the current level of cybersecurity awareness and literacy among bachelor's level students. As the use of internet increases in the education sector, it is very important to know how students maintain their online presence. The results can help colleges, universities, policy makers, training programs and awareness campaigns to improve the cybersecurity literacy. This study will also encourage students to use internet safely and maintain a safer online academic environment.

Aims And Objective

Our study aims to examine and understand the level of cybersecurity literacy among bachelor's degree students in Nepal. Our study also aims to identify the areas where they lack awareness and knowledge about cybersecurity.

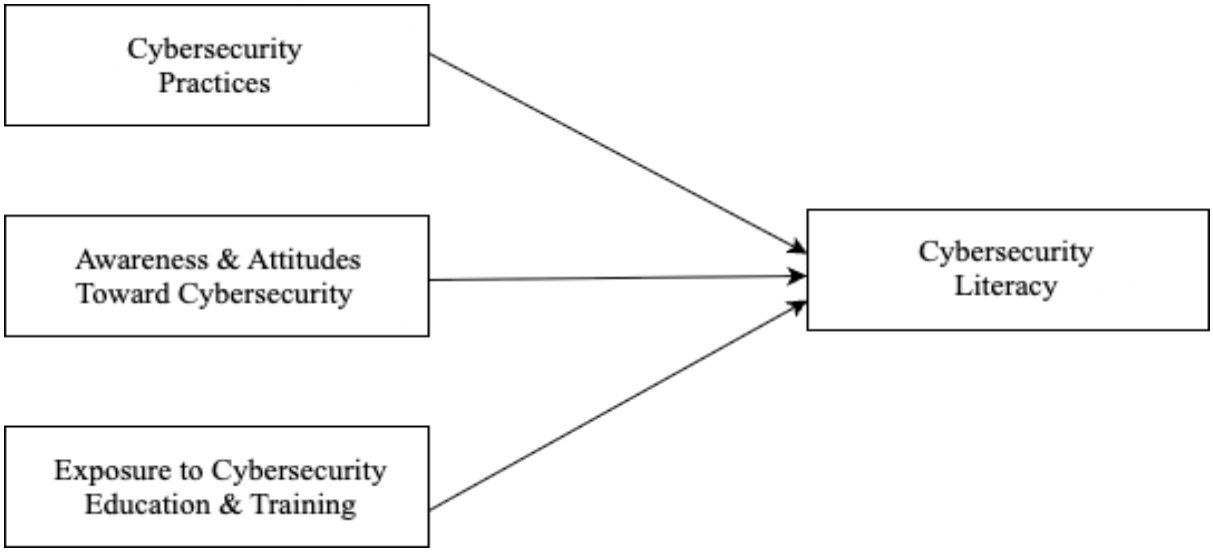
The specific Objectives are as: -

- **To examine the basic understanding of cybersecurity among bachelor's degree students.**
- **To analyse the student's behaviour and habits related to digital safety.**
- **To identify the various cybersecurity threats that students face.**
- **To understand the role of educational institutions in promoting the awareness about cybersecurity.**

Research Questions

1. What is the current level of cybersecurity awareness among bachelor's degree students?
2. What digital behaviour and habit do students have that affect the cybersecurity and digital safety?
3. What are the common cyberthreats and attacks encountered by students?
4. What role educational institute play to promote the cybersecurity education and awareness among students?

Conceptual Framework



Hypothesis

H1: There is an association between Cybersecurity Literacy and Cybersecurity Practices.

H2: There is an association between Cybersecurity Literacy and Awareness & Attitudes Toward Cybersecurity.

H3: There is an association between Cybersecurity Literacy and Exposure to Cybersecurity Education & Training.

Theoretical Foundation of this Study

This research is based on two foundational theories: Protection Motivation Theory (PMT) and the Technology Acceptance Model (TAM). Protection Motivation Theory, first introduced by R.W. Rogers (1975), was developed to explain how individuals respond to messages that evoke fear and encourage protective behavior. The theory suggests that people's motivation to protect themselves arises from two key factors. The first is threat appraisal, which involves assessing how severe a threat is and how vulnerable an individual feels to that threat. The second is coping appraisal, which concerns the belief in the effectiveness of the recommended protective action and one's confidence in successfully carrying out that action. Complementing this, the Technology Acceptance Model (TAM), proposed by Fred Davis (1986), focuses on how users decide to accept and use new technologies. According to TAM, two major perceptions guide this decision-making: how useful a person believes the technology is for enhancing their performance, and how easy they think it is to use. Together, these theories offer a solid framework for exploring how cybersecurity literacy affects both individuals' and organizations' awareness of cyber risks and their willingness to implement security measures and technologies.

The Theory of Planned Behavior (TPB), proposed by Icek Ajzen (1991), explains that an individual's intention to undertake a particular action is determined by three factors: their personal attitude toward the behavior, the social pressures they perceive from others, and their belief in their own ability to successfully carry out the behavior. Attitude refers to the extent to which the behavior is viewed favourably or unfavourably, while subjective norms relate to the perceived expectations or social demands to engage in or refrain from the behavior. Perceived behavioural control represents how much control individuals believe they have over successfully performed the behavior. These factors interact and shape whether a person forms the intention to act. When attitudes are positive, social norms are encouraging, and confidence in ability is high, the likelihood of forming a strong behavioural intention increase. This model suggests that cybersecurity literacy, by deepening individuals' understanding of potential threats and how to respond, promotes more positive attitudes toward cybersecurity, heightens awareness of social expectations for safe online behavior, and boosts confidence in practicing secure habits.

Furthermore, the Diffusion of Innovation Theory, introduced by Everett Rogers (1962), describes the process through which new ideas and practices spread within communities or organizations. Rogers (1962) outlined that individuals move through several stages when adopting innovations: becoming aware, developing interest, evaluating the innovation, trying it out, and finally adopting it. The speed and extent of adoption depend on factors such as an individual's readiness, influence from others, and perceived advantages of the innovation. In parallel, Constructivist Learning Theory, grounded in the research of Jean Piaget and others, highlights how learners actively construct understanding by linking new information to what they already know, using experience, reflection, and interaction with others. When applied to cybersecurity, exposure to education and training supports this learning process by providing relevant knowledge and practical experiences that help individuals progress through these stages. This develops the development of cybersecurity literacy, enabling people to know cybersecurity principles and adopt safer online behaviours.

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	Methods	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, Technology and Management	To analayze about how much students, teachers and university staffs in nepal are aware about cybersecurity	Quantitative survey method	The result show the current level of cybersecurity practices, knowledge and awareness among faculty, administrators and students in Nepal's Universities	There is not enough research about cybersecurity in nepal's universities,especially about teachers and staffs views,how awareness changes over time,and if current training prorams really help.
Bhandari (2025).	Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks	*Unity Journal*	To analyze how much university students in nepal know about cybersecurity threats like hacking, phising.	Quantative survey method	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 legal and practical cybersecurity knowledge.	There is a lack of research on how well university students in nepal understand cybersecurity threats and laws,leaving a gap in knowledge about their anticipation to handle digital risks.
Zwilling, Klien, ,Lesjak, Wiechete, Cetin and Basim (2022)	Cyber security awareness, knowledge and behavior: A comparative study	*Journal of Computer Information Systems*	This study focus to examine the relationship between cybersec	Quantative survey based comparative study	This study found that while internet users across four countries have good cyber threat awareness and knowledge,they	There is limited understanding of why individuals,despite being aware of cyber threats,fail to adopt strong protective behaviors and how

			urity awarene ss,knowl edge,and behaviou r espaciall y the use of protectio n tools across individu als in four countries ,and to provide recomm endation s for effective cybersec urity training program s.		tend to use only basic protection tools,with notable differences in behavior and awareness patterns between countries.	these patterns vary across different countries.
Chandarm an and Van Nieker (2017)	Students' cybersecurity awareness at a private tertiary educational institution	*The African Journal of Information and Communic ation*	This study aims to examine the level of cybersec urity awarene ss among students at a private tertiary institutio n in south africa by evaluatin g their knowled	Quanti tative survey based approa ch	The study found that students often think they are good at cybersecurity,b ut their actual knowledge and behaviour dont match,making them more at risk of cyber attacks	There is limited research on the mismatch between students perceived and actual cybersecurity knowledge and behavior especially within private tertiary institutions in South Africa, making it difficult to design targeted awareness programs

			ge,self-perception,actual skills and behaviour,and attitude towards cybersecurity.			
Garba,Siraj, and Othman(2022)	An assessment of 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	quantitative approach	The study show that most students know the fundamental of Cybersecurity, especially about internet banking , but have only neutral understanding of things like internet addiction, cyber-bullying and how to protect themselves online	The study lacks of complete analysis across demographics , behavior executions, longitudinal changes and influencing factors, limiting its depth and generalizability in accessing in awareness in cybersecurity.
Szumski(2018)	Cybersecurity best practices among Polish students	*Procedia Computer Science*	The objective of this study is to evaluate students' cybersecurity knowledge and behavior pattrens,	CAWI method (Computer-Assisted Web Interviewing)	The study found that students mostly depend on the internet and peers for cybersecurity knowledge, leading to poor behavior patterns, while good training and institutional	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

			particularly focusing on information's source and protection of password practices.		support are largely ruined.	demands of various groups
Alzubaidi(2021)	Measuring the level of cyber-security 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.	Quantitative survey	This study show less cybersecurity awareness among participants where 51% used personal information in password, 32.5% were unaware of phishing attacks, and only 29.2% reported as victim of cybercrimes.	The research gap locate in the absence of analysis of demographic factor and effectiveness of existing cybersecurity awareness programs.
Yadav(2024)	*A study on the adequacy and appropriateness of computer science curricula in*	Doctoral dissertation, Tribhuvan Universit	To study how the current Computer Science (CS)	Questionnaires	The CS curriculum includes basic programming (HTML, CSS, QBasic, C) and	More practical learning and teacher support is required.

	Nepali secondary schools	y Kathmandu	curriculum for Grades 9 and 10 is designed and taught in Nepal.		database (MS Access).	
Hong,Chi, Liu, Zhang, Lei and Xu(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.	Questionnaire	This means social and work environments reshape a person's cybersecurity awareness in many ways.	More research is needed to understand how work environment shapes behavior over time.

References

Lohani, A., & Kumar, E. S. Impact of Cyber Security Awareness Among Higher Studies: Case Study of Nepal.

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

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.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication*, *20*, 133-155.

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

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

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

Yadav, A. K. (2024). *A study on the adequacy and appropriateness of computer science curricula in Nepali secondary schools* (Doctoral dissertation, Tribhuvan University Kathmandu).

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.

Summary of literature

The study of Bhandari(2025), Chandarman and Van Nieker (2017), Garba,Siraj, and Othman(2022), Szumski(2018) and Alzubaidi(2021) highlight that students have only background information and knowledge about the cybersecurity. Likewise study of Yadav(2024), Szumski(2018) indicates that the educational institutions have weak curriculum about the cybersecurity and cyberthreats. Furthermore our review revealed that quantitative research methods along with the survey study was used as research methods in our reviewed articles. However, the quantitative interview methods was also leastly used in the reviewed articles. Our review highlight that there was a big gap for the knowledge and awareness among students because of the lack of proper research conducted specially in the field of cybersecurity in Nepal. All reviews articles applied quantitative method, but applying a single method cannot provide proper knowledge on the topic. So it is necessary to apply mixed method approach because this method try to understand the views and opinions of students in two different lens.

Research Gap

Based on our review, it is clear that many previous studies have focused on student's knowledge of cybersecurity, but they do not look deeper into various influencing factors that influence the student's actual behavior and habits. Most of the study only focus on surface level awareness and do not identify various factors that affect how students act in real life digital situations. In the context of Nepal, there are less studies that investigate deeper issues, which create a major gap in the research. Another important gap is the lack of long-term

studies that track the changes over time. Most of the existing research is based on one time survey and fail to show how awareness and literacy changes or grow after training or education programs. Likewise there is also very less study to understand the effectiveness of cybersecurity education and curriculum. By addressing these gaps, future research can provide better support to universities, schools and policymakers in Nepal to improve cybersecurity education and awareness among students.

Method and Materials

Our study applied quantitative approach to understand the problem of this study. The survey methods has applied to understand the opinions, ideas and experience of bachelor level students about the awareness of cyber threats. We applied survey method because this method is cost effective, less time consuming, covering large sample population at once and easy to understand the people opinions and ideas (Creswell & Plano Clark, 2018).

Sample Selection and Data Collection

We have applied purposive sampling methods at first and random sampling methods in the second step to select the sample population. Our sample are 210 bachelor level students from Chitwan & Nawalpur districts. The survey questionnaire is used as research instrument to collect data. Our study has followed all the ethical issues during the research procedure. First of all we administered the survey questionnaire based on our literature review and distributed the survey questionnaire to five sample population as a pilot study to understand the weakness of the research instrument (Adhikari, 2025). After our pilot study we were suggested to adjust some comment of the respondents. The main issue was difficult language and some double meaning questionnaire. After that we tried to find out correct sample population. We went at different campus and colleges to find out sample. At first we contacted with institutional head and send them request letter for the data collection. We were called to have meeting in different institution at different time. After meeting they permitted us to go and talk with bachelor level students. The next time we went to different campus and colleges for the possible sample populations. Before collecting data with our sample, we send them a consent form to collect data for 250 bachelor level students but the respondent sent back 210 consent form. On the basis of 210 sample, first we send our questionnaire online but we got only 70 responses. We realize that only online survey would not meet our demand. After that we printed 130 survey questionnaire and conducted face to face survey. After collecting data form 210 sample, we clean our data and became ready to analyze.

Data Analysis

We choose SPSS to Analyze our data. Descriptive statistics method was used to analyze data where factors reductions method was applied to find the Principle Components (PC) from the survey instruments. We have applied some AI templates to generate images, graphs, charts, and figures.

1. **Descriptive statistics**

   At initial level, analysis summarized the data using means, frequencies, percentage and standard deviation. These descriptive statistics help us to understand the awareness level, behavior and habit of bachelor's degree students in Nepal.

2. **Factor Reduction Method**

   To identify various key factor that influence the cybersecurity literacy and awareness, Principal Component Analysis (PCA) was used. This method helps to reduce survey items or questions into smaller components.