Unity Journal
Vol.6, 120-135, Feb 2025
https://doi.org/10.3126/unityj.v6i1.75557
Prithvi Narayan Shah Research Center
Directorate General of Military Training, Nepali Army
Kathmandu, Nepal

ISSN - 2717-4751

Article history
Received: 08 Nov 2024
Accepted: 23 Jan 2025

Cybersecurity Awareness amongst University Students: Legal Remedies and Policies to Mitigate Risks

Bhuwan Bhandari*

Abstract

This article examines digital threats, learning safe online practices, and identifying available legal remedies. As technology advances more quickly, Nepal is becoming more vulnerable to ransomware, phishing scams, data breaches, and other forms of online crime. The word 'cyber' pertains to the tech environment encompassing networks, software, systems, and data, while security involves safeguarding all these cyber aspects. The data was gathered through a multilingual online questionnaire format administered to university students from Undergraduate to M.Phil.-Ph.D. levels. The target sample size is 65 students who were enrolled in the previous academic session in 2023. Through surveys, we assess students' knowledge of cybersecurity measures and their responsiveness to common threats. A closed-ended questionnaire is a key tool to collect quantitative data and employ statistical methods to analyze it. The findings of this survey reveal significant gaps in cybersecurity awareness among students. Notably, 67.2% of respondents were familiar with the term 'hacking,' while only 46.9% showed awareness of Nepal's cybersecurity legal framework. This suggests a critical lack of understanding regarding basic legal protections and risk mitigation practices. However, this study suggests multi-faceted approaches such as legal education, practical cybersecurity training, curriculum designing, and institutional policies to safeguard students' digital interactions. This mini-survey aims to educate students about cyber challenges and protect them from accessing harmful digital platforms. It is supported by the National Cyber Security Policy 2023, which addresses key cybersecurity issues and vulnerabilities.

***Keywords**: Cybersecurity, awareness, cybercrimes, university student, mitigate risks*

Introduction

In the digital age, cybersecurity is aimed at preventing cyberattacks. It safeguards data from hackers and malicious actors seeking illegal financial gain. Protecting internet-connected networks, computers, servers, and mobile devices from harmful websites presents a global challenge. Early results from an investigation into students' attitudes and knowledge of cybersecurity in a highly technologically advanced environment are presented in this study. The

* Lecturer, MPhil–PhD Scholar in Mass Communication
Email ID : bhuwanb044@gmail.com

present state of cybersecurity awareness in educational institutions is examined in this study, which also looks for areas that could use improvement. The UNO (2021) acknowledges that cybersecurity has become crucial for international organizations in today's digitalized world, including the United Nations. The digital transformation, heightened reliance on information and communications technology (ICT), and escalating cyber threats, which are becoming more sophisticated and disruptive, have resulted in significant cybersecurity risks for the United Nations system. The word 'cyber' pertains to the tech environment encompassing networks, software, systems, and data, while security involves safeguarding all these cyber aspects. Cybersecurity is defined as the protection of cyberspace itself, the electronic information, the Information and Communication Technologies (ICTs) that support cyberspace, and the users of cyberspace in their personal, societal, or national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace. Solms & Niekerk (2013). Recent studies have assessed college students' understanding of information security topics, including comparable research in Malaysia, India, and California. The findings from these studies revealed a lack of adequate cybersecurity awareness, highlighting the need for a program to enhance awareness and reduce successful cyberattacks (Talpe, 2023). Mueller (2022) highlights that cybersecurity vulnerabilities arise from software flaws, human errors, outdated hardware, and weak network security, making them targets for attackers. As our reliance on digital media and interconnected devices grows, so does the threat of cybercrime, underscoring the need for stronger cybersecurity measures. Maheyzah et al. (2020) discovered that their research on cybersecurity awareness in Nigerian universities reveals a lack of essential skills, particularly in password management, among students. The survey highlighted a significant need for a cybersecurity awareness program, with respondents advocating for more education on the topic and the incorporation of a related course into the university curriculum.

'Users' understanding of the significance of information security and their responsibilities to implement adequate information control to safeguard the organization's data and networks" is a concise definition of cybersecurity awareness (Shaw et al. 2009). Security concerns and cyber intrusions are becoming more evident. With the expansion of technology, cyber risks and weaknesses are similarly escalating, demanding immediate focus (Chandarman &amp; Niekerk, 2017).The amount of information involved in smartphones is not only more comprehensive and richer than that of personal computers but also more valuable due to its dynamic, real-time, and holographic nature (Yang et al., 2022). To improve cybersecurity, the Nepali government should establish a reliable legal framework initiated by the National Cyber Security Policy 2023 and prioritize digital literacy. The Ministry of Information and Communications Technology committed to protecting cyberspace and the digital domain, which formulated a nationwide cybersecurity policy in 2023 after a wide range of consultations with stakeholders. The government plans to set up a 24/7 National Cyber Security Centre and confirmed that the process of setting it up is already underway. The center is necessary for cyber protective measures for state institutions and provides immediate information, damages, surveys, and rules. Weak structures, cyberattacks, and hacking pose similar risks.

The International Labor Organization (ILO) is actively addressing the critical need for skills that enhance the well-being of employers, workers, and the economy. This includes a range of competencies, from basic digital skills to advanced technology expertise. The

Government of Nepal has issued an important 24-point advisory aimed at safeguarding people and organizations against cyberattacks and offences. Named "The Cyber Hygiene Advisory 2023," it highlights the need for awareness and the implementation of best practices to reduce the risks associated with cyber threats such as phishing emails, which should be confirmed before any response.

Objectives

Regardless of the level of study, research encompasses a specific goal or objective. The study's question or problem establishes the minimum scope and level necessary for achieving its objective, enabling the researcher to follow the outlined plan and attain the defined goal. Recently, every sector has embraced technology, impacting all classes and professions significantly. Similarly, the scope of potential risks and challenges is expanding. In other words, while the unexpected growth and advancement of information technology are making our daily lives more convenient, we are also encountering numerous challenges and cyber risks. The rapid expansion and accessibility of new technologies are broadening the foundation of information intervention. The risk of serious cybercrimes is escalating globally due to software misuse and unawareness in the pursuit of engaging with global networks. Even in a country like Nepal, which has a low level of digital and information literacy, the increased attraction and access to technology have not significantly improved users' knowledge of cybersecurity precautions and risk reduction methods. Research from various countries indicates that children, adolescents, and individuals with low digital literacy are particularly vulnerable and at risk regarding cybersecurity. The nature of the complaints filed with the Cyber Bureau of Nepal Police regarding such crimes is also revealing. It has been demonstrated that youth participate in it to the greatest extent. Thus, there are several factors contributing to the swift growth of cybercrime, including the propensity to exploit social media. Assassinating an individual's character, invading privacy, gaining unauthorized access to computer systems, hacking, employing malware attack techniques, utilizing cyber fraud methods, interfering with intellectual property, and committing sexual offenses are categorized as significant cybercrimes. Awareness of such crimes extends beyond cybersecurity; every class should equally understand the policy foundations, legal provisions, and established legal frameworks set by the state. In light of these considerations, this mini-research project has been undertaken. This will assess the level of knowledge regarding cybersecurity among students from undergraduate to MPhil and Ph.D. levels and will evaluate their understanding of identifying groups that may be at risk of cybercrime, as well as their engagement with legal and policy measures for cyber risk reduction. Thus, three objectives have been established to ensure that this research is result-oriented, which include:

(a) To determine university students' awareness of cybercrime based on their research and experience.

(b) To ascertain the students' knowledge of the legislative and policy actions taken by the government to reduce cybercrime, and

(c) To evaluate students' general understanding of cybersecurity protocols and risk-reduction strategies for cybercrime, among other associated subjects.

Review of Literature

Researching on cyber issues in Nepal is severely hampered by a lack of data and resources, making it difficult to identify target audiences. Neglect of proper data management by authorities further stifles progress. While university students are a key demographic, their participation in research is disappointingly low, often due to a lack of awareness that leads to unintentional regulatory violations. This highlights the urgent need for comprehensive cybersecurity education. Despite some advancements in Indian universities, there is a significant lack of research from other South Asian countries. While gender-based studies exist, comprehensive academic research is lacking. The limited resources complicate outreach, and many students show minimal interest in cybersecurity and little understanding of its legal aspects. To advance the understanding of cybersecurity challenges, it's essential to utilize research from the UK, USA, Malaysia, China, and Indian studies. By prioritizing thorough investigations, we can address crucial knowledge gaps and foster a culture of cybersecurity awareness for a safer digital landscaape in Nepal.

Kelley (2024) says that knowing is having power. She contends that it is essential for students to be aware of online hazards. To achieve this, it is imperative to instruct them on the fundamental practices of maintaining computer security. This includes not only knowing the best ways to act in the work world, but also how companies should run things and how to spot and tell about any bad actions. The Cybercrime Magazine 2025 predicts that the annual cost of cybercrime worldwide will reach $10.5 trillion, with global cybercrime expenses anticipated to increase by nearly 15 percent each year over the next four years. Concepts such as the pandemic, crypto currency, and the increase in remote working are converging to create a target-rich environment for criminals to exploit. Berki et al. (2017) reveal in their study that learners (prospective IT professionals) from five countries–China, Finland, Greece, Nepal, and the UK–scrutinize information. The researchers aimed to investigate the knowledge, conceptualizations, and awareness of cybersecurity among future IT professionals, specifically concerning the use of cloud-based services by current IT students enrolled in higher education degree programs and curricula related to cybersecurity. The majority of participants recognized the importance of cybersecurity in education, given the growing reliance on the internet and the increasing incidents of cybercrime. A significant statistical relationship was observed between the awareness levels of undergraduate students and their interests in cybersecurity education (Onyema et al., 2021). The majority of university students are more vulnerable to cyberattacks, this shows they lack security concerns about using the internet. At the same time, they lack the knowledge of security threats and the methods necessary to avoid them (Pramod & Raman, 2014). To understand the awareness of risks related to social networking sites (SNSs), a study by Grainne, H., et al (2017) was conducted among Malaysian undergraduate students, of whom 295 took part. This study reported that more than one-third of participants had fallen victim to SNS scams. The study focused on investigating student awareness and attitudes toward cybersecurity and the resulting risks in the most advanced technology environment. The composition of students in Silicon Valley is very ethnically diverse. Reyns et al. (2012) found that just 4.9 percent of students have gone through cyberstalking. The truth is that knowing more about cybersecurity can help cut down on simple attacks on people. It also shows that students face more risks from cyberattacks. Likewise, Alotaibi et al. (2016) also investigated the level of cybersecurity knowledge among college students. Their investigation revealed that cybersecurity awareness in Saudi university students is poor since most students were unaware of their data protection.

The ITU's Global Cybersecurity Index 2024 emphasizes the evolving nature of cybersecurity, essential for countries pursuing secure and meaningful connectivity. The GCI not only assesses current standings but also offers a roadmap for improvement. Countries must commit to continually enhancing their cybersecurity efforts for maximum impact. Classified into tiers from 1 to 5, Nepal is currently in Tier 4, reflecting its dedication to advancing cybersecurity. Correspondingly, Senthilkumar and Easwaramoorthy (2017) studied university students in Tamil Nadu's key towns to examine their attentiveness to cybersecurity. Which discovered that university students in Tamil Nadu had an above-average level of cybersecurity knowledge, but that it still has to be bolstered further. Moallem (2018) investigated students' opinions regarding cybersecurity in California's Silicon Valley. Since learners' behavior is variable, the author assessed the cybersecurity level in the largest and most influential technology environment. Even when they were aware that their actions were being seen and tracked, college students were unaware that their data was not safely transported across university systems. As a result, institutions should offer training regularly to influence students' behavior and increase their awareness of the basics of cybersecurity and cyber threats Taha and Dahabiyeh (2021). Grainne et al. (2017) assert that the reasons why individuals who utilized fewer devices for social networking sites were more prone to victimization remain unclear. CHEN (2021) highlights the alarming rise of cybersecurity incidents among university students in China. It is crucial to examine their Information Security Awareness (ISA) regarding smartphone usage and the relationship between their knowledge and behaviors related to smartphone security. This analysis will identify challenges and inform effective educational measures for enhancing students' information security awareness.

Methodology

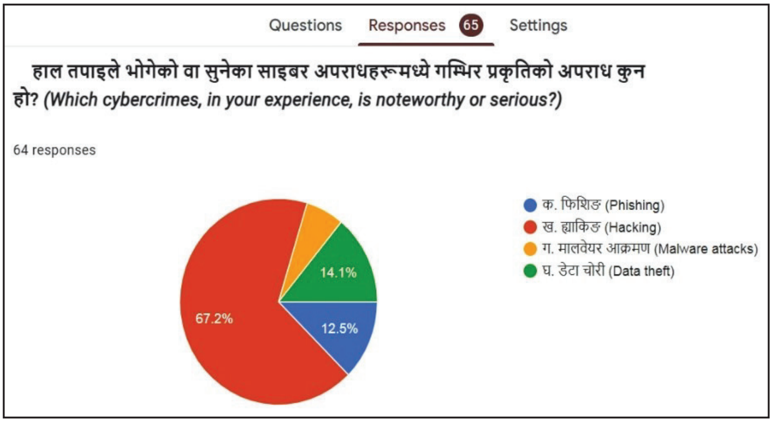
An online questionnaire was used to collect data, employing a simple random sampling method for choosing a related population as a sample size. The data collection took place at two universities in Nepal, targeting undergraduate to MPhil-PhD levels of students of all ages and gender status who have been enrolled in the Humanities and Social Sciences Stream in the previous academic session in 2023.The close-ended questionnaire was generated using the Google RSVP Form, which is easy to handle for collecting survey data. The survey link was shared through popular platforms such as WhatsApp, Messenger, and Gmail, which took almost a month to collect the quantitative data. Additionally, to maximize the survey response rate, three faculties from each selected university collected the data during the survey. They actively motivated students within their respective institutions to participate and provide careful responses. The final sample size during the data collection process is 65 students. In the sample, the number of male participants is 43, and the number of female participants is 22. As regards the data tabulation and analysis, Google Excel is used, and the desktop analysis technique is applied for data interpretation. Secondary data is a powerful tool to link contemporary studies with historical ones, enriching our understanding through narrative and archival methods. By analyzing collected statistical or numerical data, it effectively presents findings in a clear and engaging pie chart format.

Results

The growing dependence on digital tools for education renders faculty, students, and institutions more vulnerable to cyberattacks. Proper training for all participants in the educational process is essential, as lack of knowledge can lead to risky online behaviors that increase susceptibility to cyber threats. It is important to recognize that unsafe behaviors can affect both individuals and educational institutions. These behaviors include the distribution of inappropriate images, revenge-driven posting of explicit content on social media, dissemination of malware, extortion of devices, and breaches of both governmental and private websites. Statistics from the Nepal Police Cyber Bureau for the year 2081 indicate a significant rise in male victims of cybercrime and online fraud. Reported cases increased from 1,898 in the fiscal period of 1978/79 to 7,717 in 1980/81, marking increases of 49.2% and 51.6%, respectively. Males are particularly targeted through various manipulative and hacking methods. Additionally, a report by Cyber Bureau Nepal dated May 2024 states that 3,956 individuals filed complaints related to cybercrime involving Facebook and Messenger during the fiscal year 2078-079, with 233 complaints associated with TikTok. Understanding cybersecurity is crucial for students, as their educational environments are vulnerable to cyber threats. From July 2022 to March 23, the Cyber Bureau of Nepal Police documented 13,330 cybercrime incidents. There were 11,425 cases linked to social media and 1,905 financial offenses related to information technology. The Cyber Bureau has apprehended 51 individuals in connection with these cybercrimes. While large corporations remain attractive targets for cybercriminals, educational institutions also face significant risks due to the potential exposure of passwords, personally identifiable information (PII), and financial credentials. In Nepal, the Central Investigation Bureau is investigating cybercrime activities. As previously mentioned, the findings outlined in this section seek to illustrate the level of students' comprehension of cybersecurity. These findings are depicted as pie charts derived from seven questionnaires, each providing four possible response options. Furthermore, it explores the diverse viewpoints of university students concerning their self-assessed knowledge, which are represented statistically. A total of 65 students, spanning from undergraduate to MPhil-PhD levels, took part in this survey. Data collection was conducted through seven closed-ended questionnaires, each offering four response alternatives, administered utilizing Google Forms. Responses were received from between 63 and 65 individuals for each questionnaire. The analysis of the gathered data, presented in both narrative and statistical formats, assesses university students' awareness and understanding of cybercrime and cybersecurity.

Table 1: Noteworthy or serious cybercrime

1. Which cybercrimes, in your experience is noteworthy or serious?		**Color options**
Reason		**Reactions**
a.	**Phishing**	**8**
b.	**Hacking**	**43**
c.	**Malware attacks**	**4**
d.	**Data theft**	**9**
	Total Responses	**64**



हाल तपाइले भोगेको वा सुनेका साइबर अपराधहरूमध्ये गम्भिर प्रकृतिको अपराध कुन हो? ***(Which cybercrimes, in your experience, is noteworthy or serious?)***

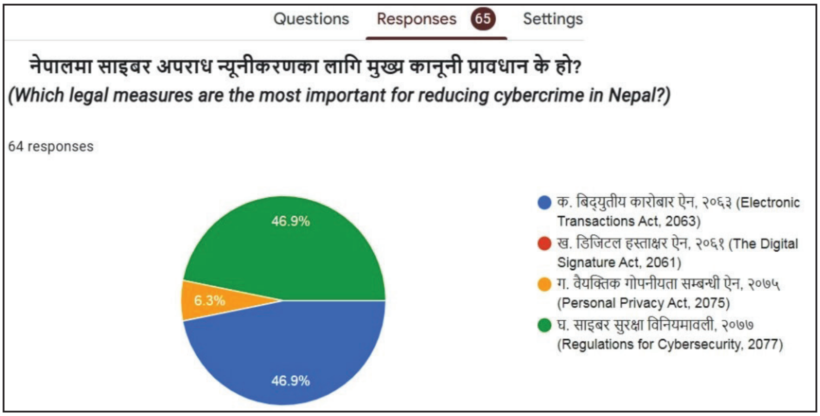
64 responses

Data Source:https://docs.google.com/forms#responses

In the initial question, pertaining to the students' experiences, a majority identified hacking as the most serious cybercrime, with 43 out of 64 respondents selecting this option, covering **67.2** percent of total participants. This reflects that hacking is the most recognized and encountered cybercrime incident in Nepal. In recent years, there have been numerous incidents of data breaches involving government agencies. Which is shown in the above table 1. Presumably, the unexpected percentage of responses suggests that almost all individuals have encountered data breach incidents while engaging with social media on a daily basis.

Table 2: Legal measures for reducing cybercrime

2. Which legal measures are the most important for reducing cybercrimes in Nepal?		**Color options**
Reason		**Reactions**
a.	**Electronic Transaction Act, 2063**	**30**
b.	**The Digital Signature Act, 2061**	**0**
c.	**Personal Privacy Act, 2075**	**6**
d.	**Regulations Cybersecurity, 2077**	**30**
	Total Responses	**64**



नेपालमा साइबर अपराध न्यूनीकरणका लागि मुख्य कानूनी प्रावधान के हो?
(Which legal measures are the most important for reducing cybercrime in Nepal?)

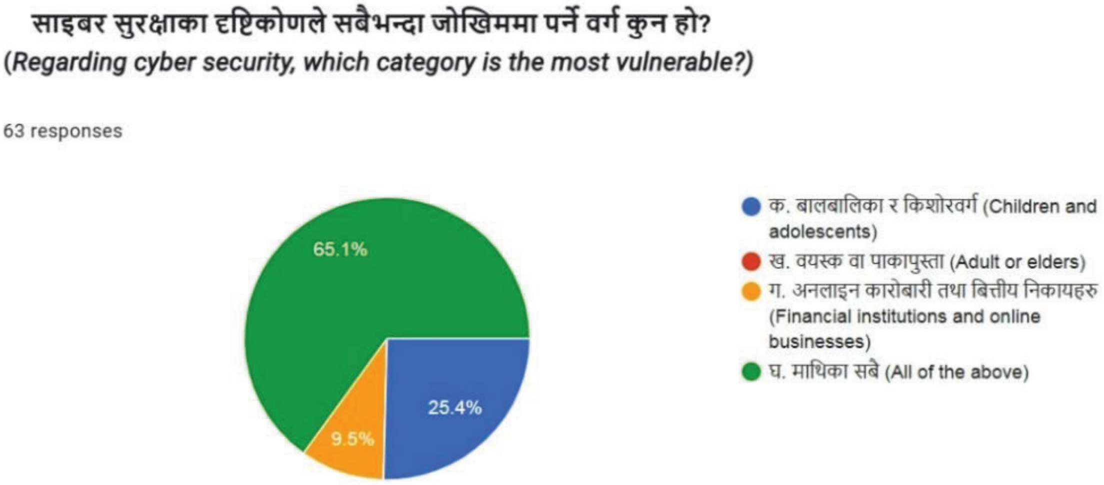
64 responses

Data Source:*https://docs.google.com/forms#responses*

The results indicate that 30 out of 64 participants chose the ‘Electronic Transactions Act 2063’ option, which is **46.9** percent, while 30 individuals also selected the fourth option covers the ratio of total. This suggests that an equal number of students are unfamiliar with cybercrime and cybersecurity regulation provisions, as demonstrated in Table 2 above. It is accurately stated that ignorance of the law is not an acceptable excuse. Consequently, it is essential for all citizens to possess relevant personal knowledge, and it is imperative for stakeholders to engage actively in the institution.

Table 3: Most vulnerable category of society

3. Regarding cybersecurity, which category is the most vulnerable?		**Color options**
Reason		**Reactions**
a.	**Children and adolescents**	**16**
b.	**Adults or elders**	**0**
c.	**Financial or business institutions**	**6**
d.	**All of the above**	**41**
	Total Responses	**63**



साइबर सुरक्षाका दृष्टिकोणले सबैभन्दा जोखिममा पर्ने वर्ग कुन हो?

(Regarding cyber security, which category is the most vulnerable?)

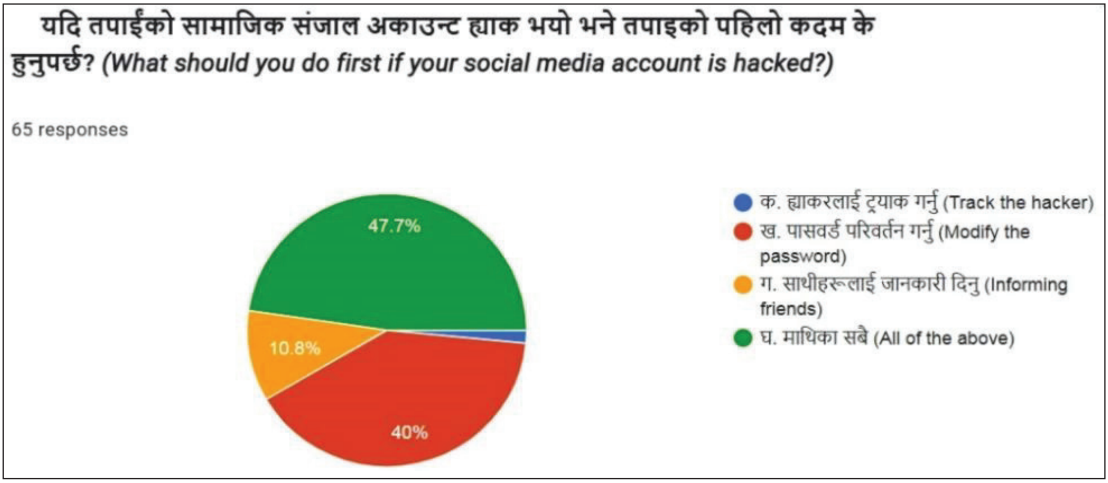
63 responses

Data Source:https://docs.google.com/forms#responses

Research conducted worldwide on cybercrime indicates that children and teenagers represent the most sensitive and vulnerable demographic. However, university-level students cast 41 votes out of 63 responses for the fourth option of the questionnaire, which is about 65.1 percent, whereas only 16 votes were submitted for the first option, covering only 25.4 percent of understanding, indicating a lack of study and engagement. In Nepal, children and teenagers are considered to be at an elevated risk of cybercrime due to their limited awareness of the issue, resulting in many instances of exploitation by others for the purpose of executing criminal activities. The laws of Nepal encompass legal provisions designed to safeguard children from cyber activities. Table 3 above shows the data clearly.

Table 4: Remedy after social media hacked

4. What should you do first if your social media account is hacked?	**Color options**
Reason	**Reactions**
a. Tracking the hacker	**1**
b. Modify the password	**26**
c. Informing friends	**7**
d. All of the above	**31**
Total Responses	**65**



यदि तपाईंको सामाजिक संजाल अकाउन्ट ह्याक भयो भने तपाइको पहिलो कदम के हुनुपर्छ? ***(What should you do first if your social media account is hacked?)***

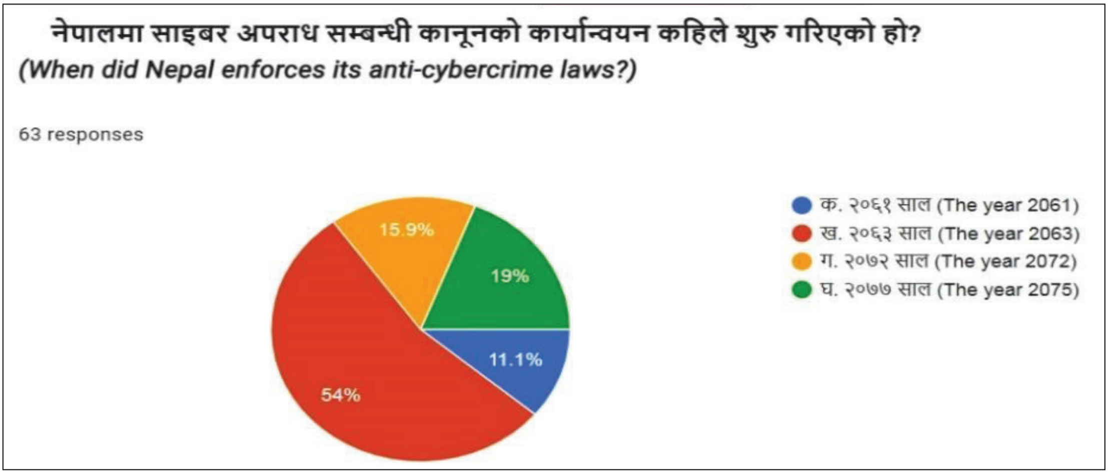
65 responses

Data Source:https://docs.google.com/forms#responses

In recent years, social media and various platforms have encountered hacking incidents. In this context, regarding the question, 31 out of 65 respondents selected the fourth option, which covers 47.7 percent, while 26 chose the option to change the password, which covers 40 percent. When there is a possibility of an account or site being hacked, it is advisable to change the password immediately to reduce the risk associated with any existing vulnerabilities. This suggests that students lack proper knowledge and experience concerning such events and may have chosen different options, as shown in Table 4 above.

Table 5: Enforcement of anti-cybercrime laws

5. When Nepal did enforce its anti-cybercrime laws?	**Color options**
Reason	**Reactions**
a. The year 2061	**7**
b. The Year 2063	**34**
c. The year 2072	**10**
d. The year 2075	**12**
Total Responses	**63**



नेपालमा साइबर अपराध सम्बन्धी कानूनको कार्यान्वयन कहिले शुरु गरिएको हो?

(When did Nepal enforces its anti-cybercrime laws?)

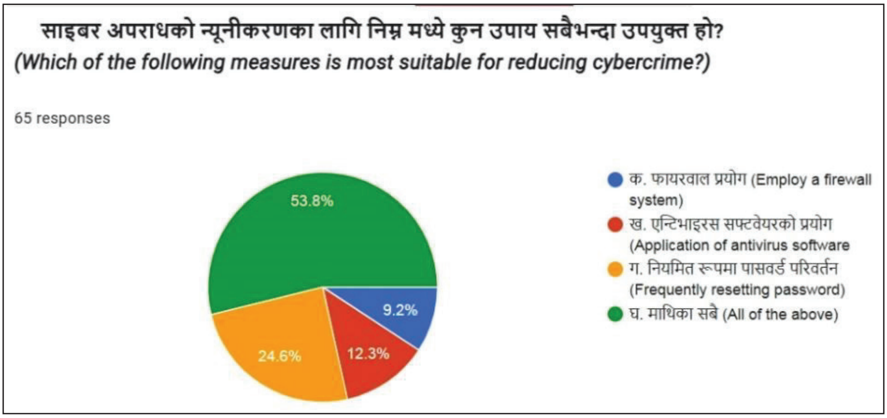
63 responses

Data Source:https://docs.google.com/forms#responses

Since the Government of Nepal established legal provisions in 2063 BS to regulate all forms of electronic transactions, it is crucial for every citizen to be informed about this issue. In this questionnaire, of the 63 respondents who supported the implementation of the cybercrime law, 26 chose the second option as the correct response, which is about **54** percent of the total. The other participants preferred alternative options, demonstrating a lack of knowledge and understanding concerning the law's implementation. The absence of a comprehensive course on this subject within the university curriculum highlights a deficiency in legal knowledge among students at the MPhil level, as evidenced by Table 5 above.

Table 6: Most suitable measure for reducing cybercrime

6. Which of the following measures is most suitable for reducing cybercrime?		**Color options**
Reason		**Reactions**
a.	**Employ a firewall system**	**6**
b.	**Application of antivirus software**	**8**
c.	**Frequently resetting password**	**16**
d.	**All of the above**	**35**
	Total Responses	**65**



साइबर अपराधको न्यूनीकरणका लागि निम्न मध्ये कुन उपाय सबैभन्दा उपयुक्त हो?

(Which of the following measures is most suitable for reducing cybercrime?)

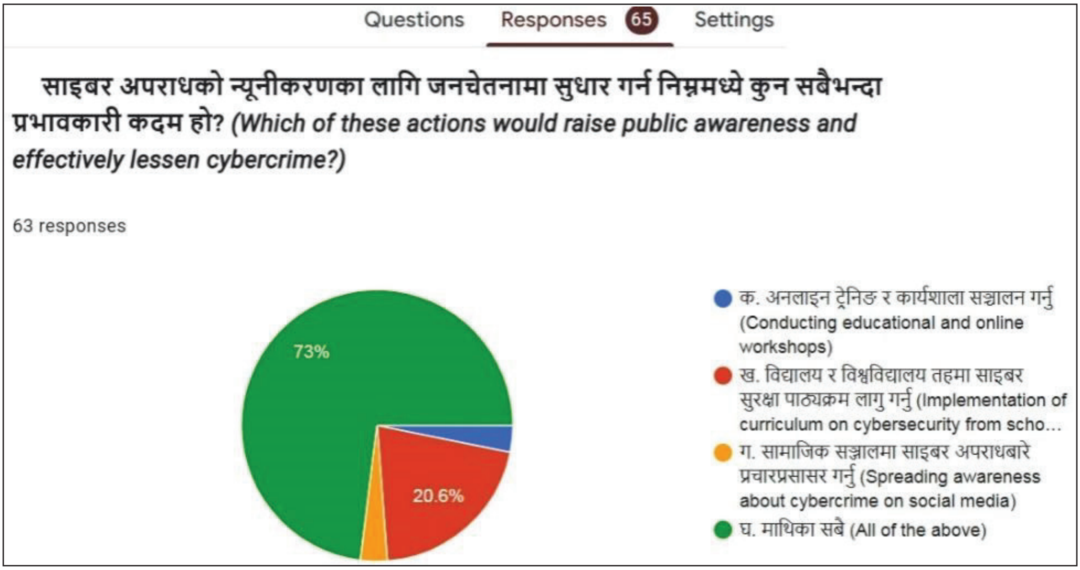
65 responses

Data Source:https://docs.google.com/forms#responses

Enhancing awareness and preparedness among students about cybersecurity is essential for reducing crime. In this context, only 35 of the 65 individuals chose the fourth option, which covers about **53.8** percent. Similarly, 16 individuals selected the option 'to change the password'; however, it is important to evaluate all three options as a whole. It may be beneficial to consider all available options, such as utilizing different software or applying firewall conditions, to protect social media accounts from potential cyber threats. The results are shown in Table 6 above.

Table 7: Suitable actions that raises public awareness on cybercrime

7. Which of these actions would raise public awareness and effectively lessen cybercrime?	**Color options**
Reason	**Reactions**
a. Conducting educational and online workshops	**2**
b. Implementation of curriculum on cybersecurity from school to University levels	**13**
c. Spreading awareness about cybercrime on social media	**2**
d. All of the above	**46**
Total Responses	**63**


Questions
Responses 65
Settings
73%
20.6%
● क. अनलाइन ट्रेनिङ र कार्यशाला सञ्चालन गर्नु (Conducting educational and online workshops)
● ख. विद्यालय र विश्वविद्यालय तहमा साइबर सुरक्षा पाठ्यक्रम लागु गर्नु (Implementation of curriculum on cybersecurity from scho...
● ग. सामाजिक सञ्जालमा साइबर अपराधबारे प्रचारप्रसार गर्नु (Spreading awareness about cybercrime on social media)
● घ. माथिका सबै (All of the above)

साइबर अपराधको न्यूनीकरणका लागि जनचेतनामा सुधार गर्न निम्नमध्ये कुन सबैभन्दा प्रभावकारी कदम हो? *(Which of these actions would raise public awareness and effectively lessen cybercrime?)*

63 responses

Data Source:https://docs.google.com/forms#responses

In the seventh question concerning the most effective measure to improve public awareness for reducing cybercrime, 46 out of 63 respondents selected the fourth option, which covers **73** percent, while the other participants preferred different alternatives. While all options are considered equally important, it is also advisable to periodically organize online training and workshops, incorporate cybercrime into the curriculum at all educational levels, and broadly publicize the nature of cybercrime on social media. However, the fact that most students chose all three options–as well as the fourth–could be interpreted as a sign of awareness. The outcome displayed in Table 7 suggests that in order to prevent specific harm from cybercrimes and attacks, curricula from the elementary school level to the university level must be created and implemented. Overall, in this survey, although the students were unable to select the correct options for questions related to cybersecurity and reducing the growing cybercrime, it was evident that they had a limited understanding of cybercrime. Their knowledge of legal provisions and policies implemented by the Nepal government to combat cybercrime is also insufficient.

Discussion

Regarding the expectations set forth by the survey, it was carried out employing a series of closed-ended questionnaires, which revealed the varying experiences of college students engaging with social media. The percentages of student responses to seven multiple-choice inquiries concerning minimum cybersecurity standards, legal and policy frameworks, and statutory regulations are presented. Nonetheless, students across undergraduate, graduate, and doctoral levels have shown an understanding of cybersecurity standards. Consequently, there is an ongoing discussion regarding the necessity of including this subject in university curricula. Furthermore, stakeholders have acknowledged the significance of immediate orientation and training. This study will also establish that the state should enhance university students' awareness levels of the various threats posed by cybercrime through further research and examination.

Conclusion and Implications

The survey findings indicate that participants possess substantial knowledge of cybersecurity. However, fewer students understand internet threats and the importance of monitoring. Misconceptions regarding the effectiveness of antivirus software and the scope of cybersecurity are prevalent. Most students believe that cybersecurity education is crucial for businesses and academic institutions. The increase in criminal activities on platforms like Facebook, Twitter (X), and TikTok, along with rising financial fraud on Facebook and WhatsApp, highlights this need. University curricula should integrate cybersecurity research and strategies to combat online crime. This program enhances awareness and improves students' understanding of the topic. Furthermore, inappropriate social media use poses risks to the mindset and ethical development of students and young people.The initial survey results indicated that only 30 of the 64 respondents chose the first option for the cyber law question, while approximately 46.9 percent selected the correct response, highlighting a deficiency in knowledge. The same ratio of responses favoring other options further demonstrated a lack of understanding of the laws and regulatory mechanisms.

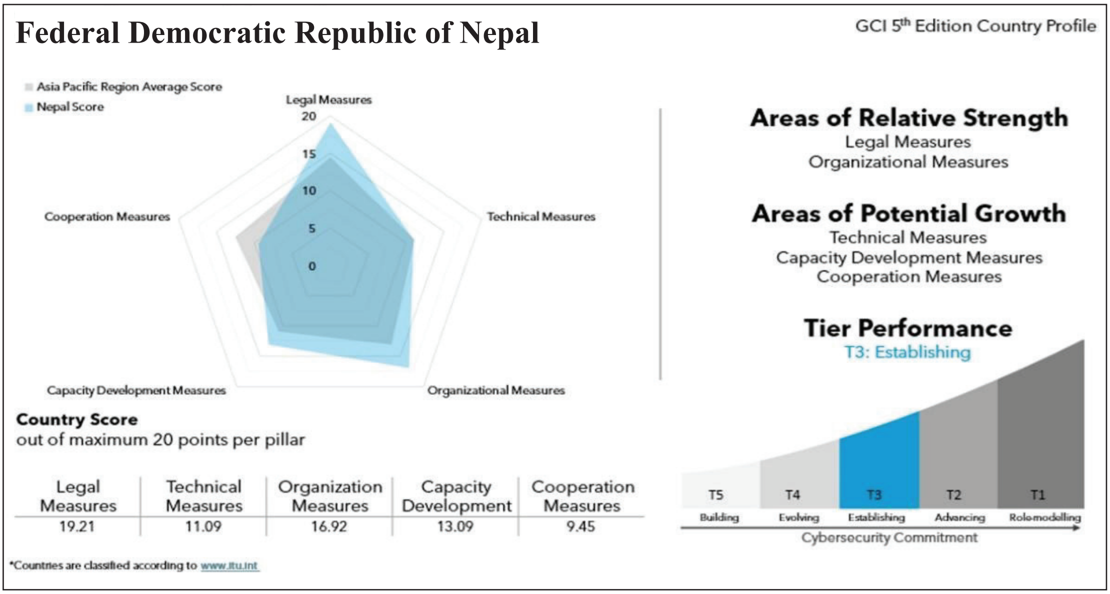
In Nepal, youth and students are highly engaged with social media and digital devices in the current digital era. However, improving the index ranking alone is inadequate. Sustainable cybersecurity requires a practical approach to policy development and collaboration among security agencies, ICT providers, industries, academia, and the public. The Electronic Transactions Act of 2063 establishes the legal framework for cybercrime in Nepal, outlining offenses such as theft, destruction, alteration, or interference with computer systems. Violations may result in up to three years of imprisonment, a fine of up to two lakh rupees, or both. Legislation, including Section 47 of the Electronic Transaction Ordinance and relevant sections of the Some Public (Crime and Punishment) Act and Children's Act, ensures online protection for children. The Cyber Security Policy, 2023, reflects Nepal's dedication to creating a safer digital environment and establishes a framework that fosters business trust, innovation, and growth. This survey emphasizes the need for comprehensive cybersecurity education to address knowledge gaps and enhance online security practices. To protect students' digital interactions, it recommends strategies such as curriculum development, practical cybersecurity training, legal education, and institutional policies. Despite underreporting, global cybersecurity communities frequently identify incidents, highlighting the need for proactive and reactive measures against cyber threats. Further research is crucial to identify digital vulnerabilities and mitigate future risks.

Acknowledgements

It is to recognize the essential contributions of Shanta Ram Bidari from Tribhuvan University, Santosh Raj Pandey from Far Western University, and Sunil Paudel from Bajra Multiple Campus, who were instrumental to the success of this study. Furthermore, I express my appreciation to all those students and colleagues who contributed a lot to this initiative. Additionally, let us expand upon this base of cooperation and positive intent for future efforts.

Appendix: 1

According to the ITU's 2024 Report, Tier 4 (T4) includes developing countries scoring at least 20 out of 100, which reflects a basic commitment to cybersecurity through government actions. Nepal, however, scored below this threshold, with 19.21 points in legal measures, 11.09 in technical measures, 13.09 in capacity development, and 9.45 in cooperation measures in its cybersecurity performance.



Federal Democratic Republic of Nepal

GCI 5th Edition Country Profile

Areas of Relative Strength
Legal Measures
Organizational Measures

Areas of Potential Growth
Technical Measures
Capacity Development Measures
Cooperation Measures

Tier Performance
T3: Establishing

Country Score
out of maximum 20 points per pillar

Legal Measures	Technical Measures	Organization Measures	Capacity Development	Cooperation Measures
19.21	11.09	16.92	13.09	9.45

*Countries are classified according to www.itu.int

Source: ITU' Global Cybersecurity Index 2024.

Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

References

Acharya, G. P. (2023). Cyberintelligence for enhancing national security. *The Republic Online.* Retrieved from https://myrepublica.nagariknetwork.com/news/cyber-intelligence-for-enhancing-national-security

Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A survey of cybersecurity awareness in Saudi Arabia. In *Proceedings of the 11th International Conference for Internet Technology and Secured Transactions (ICITST)*, Barcelona, Spain.

Berki, E., Kandel, C., Zhao, Y., & Chaudhary, S. (2017). A comparative study of cybersecurity knowledge in higher education institutes of five countries. *Faculty of Natural Sciences, University of Tampere (Finland), Deerwalk Institute of Technology (Nepal)*. Retrieved from https://www.academia.edu/124107644/A_Comparative_Study_of_Cyber_Security_Knowledge_in_Higher_Education_Institutes_of_Five_Countries?

Chandarman, R., & Niekerk, B. V. (2017). Students' cybersecurity awareness at a private tertiary educational institution. *The African Journal of Information and Communication, 20*(5), 133–155. https://doi.org/10.23962/10539/23572

Chen, Z. (2021). An empirical analysis of contemporary college students' awareness of network security. *Network Security Technology and Application, 12*, 91–92.

Cybersecurity Awareness Assessment Report (2015). To establish a national cybersecurity awareness programme for Nepal. Retrieved from *Nepal Telecommunications Authority*. https://nta.gov.np/uploads/contents/Cybersecurity-Awareness-Report-2015.pdf

Emerging Practices in Cybersecurity-Related Public-Private Partnerships and Collaboration. Organization for Security and Co-operation in Europe Permanent Council (2023). Retrieved from https://www.osce.org/files/f/documents/2/7/539108_ 0.pdf

Gráinne, H. K., Fullwood, C., & Rooney, B. (2017). Risk factors for social networking site scam victimization among Malaysian students. *Cyberpsychology, Behavior, and Social Networking*. https://www.liebertpub.com/doi/10.1089/cyber.2016.0714

Hunt, T. (2016). Cybersecurity awareness in higher education. *CWU Source.* Retrieved from https://digitalcommons.cwu.edu/source/2016/cob/1

Kelley, K. (2024). What is cybersecurity and why it is important? Simplilearn. Retrieved from https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

Lindemulder, G., & Kosinski, M. (2024). What is cybersecurity? IBM. Retrieved from https://www.ibm.com/topics/cybersecurity

Maheyzah, B., Othman, S. H., Garba, A. A., & Dauda, I. B. (2020). Cyber security awareness among university students: A case study. Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia. Retrieved from https://www.researchgate.net/publication/378308636

Moallem, A. (2018). Cybersecurity awareness among college students. In *Proceedings of the International Conference on Applied Human Factors and Ergonomics*, Orlando, FL, USA.

Onyema, E. M., Edeh, C. D., Gregory, U. S., Edmond, V. U., Charles, A. C., & Richard-Nnabu, N. E. (2021). Cybersecurity awareness among undergraduate students in Enugu Nigeria. *International Journal of Information Security, Privacy and Digital Forensics, 5*(1). Retrieved from https://www.researchgate.net/publication/355716927_Cybersecurity_Awareness_Among_Undergraduate_Students_in_Enugu_Nigeria

Reyns, B. W., Henson, B., & Fisher, B. S. (2012). Stalking in the twilight Zone: Extent of cyberstalking victimization and offending among college students. *Deviant Behavior, 33*(1), 1–25. https://doi.org/10.1080/01639625.2010.538364

Rijal, B. (2079). Who will protect Nepal's risky cyberspace? *TechPana Online,* 4th Falgun Issue. Retrieved from https://techpana.com/2023/141041/birodh-rijal-article

Senthilkumar, K., & Easwaramoorthy, S. (2017). A survey on cybersecurity awareness among college students in Tamil Nadu. In *Proceedings of the IOP Conference Series: Materials Science and Engineering*, Vellore, India.

Shaw, R.-S., Chen, C., Harris, A., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. Computers & Education, 52(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Taha, N., & Dahabiyeh, L. (2021). College students' information security awareness: A comparison between smartphones and computers. *Education and Information Technologies, 26*, 1721–1736.

Talpe, Ganesh. (2023). Cyber security among college students. *Department of Information Technology B.K. Birla College of Arts, Commerce And Science.* Retrieved from https://www.irjmets.com/uploadedfiles/paper//issue_10_october_2023/45484/final/fin_irjmets1698293129.pdf

Van Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*. Elsevier Ltd, 1–6.

Yang, G., Ye, J., Yang, L., & Feng, K. (2022). Current situation and prospect of information security risks of intelligent devices. *Information Security and Communications Privacy, 2*, 17–22.

-◆◆◆-