Cyber Awareness among Secondary School Students in Public and Private Schools in Sunwal Municipality

Tank Prasad Subedi
Assistant Lecturer
Dibya Jyoti Multiple campus
tanksubedi.ts@gmail.com
DOI: https://doi.org/10.3126/dj.v7i1.87647

Abstract

This study investigates the comparative effectiveness of cybersecurity awareness management practices among Grade 7–12 students in Sunwal municipality's public and private schools, using SPSS to model influencing factors. As Nepal undergoes rapid digital transformation, driven by increased internet access, mobile device usage, and post COVID-19 digital learning, students are increasingly exposed to cyber threats such as phishing, cyberbullying, and identity theft. Despite national initiatives like the Digital Nepal Framework and Cyber Security Policy 2080, implementation at the school level remains inconsistent, especially in rural and public institutions. SPSS was employed to analyze the relationships between latent variables and to test hypotheses such as "Digital literacy positively influences cybersecurity awareness" and "Institutional support enhances cybersecurity behavior." Descriptive statistics were used to compare public and private school practices.

While the findings are pending, preliminary hypotheses suggest that private schools, particularly in urban areas, demonstrate higher cybersecurity awareness due to better infrastructure, gamified learning tools (e.g., Kahoot, Scratch), and teacher training. Public and rural schools face challenges such as limited internet access, lack of trained staff, and absence of standardized cybersecurity curricula.

Keywords: *cybersecurity awareness, digital literacy, institutional support, SPSS, Nepalese schools*

Introduction

Nepal is in the midst of a profound digital transformation, driven by rapid advancements in internet penetration, widespread smartphone adoption, and the integration of digital technologies in various sectors, including education. According to the Nepal Telecommunications Authority (2024), over 80% of Nepal's population, approximately 24 million people, now has access to the internet, a

significant leap from just 35,000 users in 2000. This growth is particularly pronounced among the youth, with mobile device usage among adolescents reaching an all-time high, fueled by affordable smartphones and expanding 4G networks. In the education sector, the COVID-19 pandemic accelerated the adoption of digital tools, with schools transitioning to e-learning platforms like Google Classroom, Zoom, and Microsoft Teams, alongside digital classrooms and online assessment systems. By 2024, approximately 65% of private schools and 30% of public schools in urban areas like Sunwal Municipality had integrated some form of digital learning infrastructure, reflecting a shift toward technology-driven education (Ministry of Education, Science and Technology [MoEST], 2024).

Nepal's education system is rapidly adopting digital tools like computers, internet, and online learning platforms, especially after the COVID-19 pandemic (Nepal Telecommunications Authority, 2024). Students in Grades 7–10 are among the most active users of these technologies, using apps like Google Classroom, Kahoot! and Scratch. However, while digital access is increasing, cybersecurity awareness among students remains low. Many students do not know how to protect themselves from threats like phishing, cyberbullying, or identity theft (Khader et al., 2021; Moallem, 2019).

Although the government has introduced policies like the Digital Nepal Framework and the Cyber Security Policy 2080, these are not fully implemented in schools (Shahi, 2023). Public schools often lack trained teachers, secure internet, or clear rules about online safety, while private schools may have better tools but still face awareness gaps (Dhungana et al., 2023; Poudyal et al., 2025). For instance, a student in a private school may know how to use applications but not how to report cyberbullying, while a student in a public school may not have access to the internet at all. Nepal's collectivist culture also affects how students respond to cyber threats. They may avoid reporting problems to protect family or school reputation (Khader et al., 2021). Teachers, too, often lack training and confidence to teach cybersecurity, especially in rural areas where digital literacy among educators is below 30% (ViN, 2024). Without proper support, students are left vulnerable.

Also, it is not known how the factors like digital literacy, education level, institutional support, training, policy implementation, and access to technology affect students' cybersecurity awareness in Nepal. A teacher who has received training might help students stay safe online, while another

might not mention cybersecurity at all. But no one has studied these differences in Nepalese schools. This study investigates how these six factors influence cybersecurity awareness among Grade 7–10 students in Sunwal Municipality. The goal is to help schools and policymakers create safer digital learning environments by understanding what works and what doesn't in Nepal's unique context.

The study tries to address the following research questions:

i. What is the current level of cybersecurity awareness among Grade 7–12 students in Nepal's public and private schools?
ii. How do digital literacy and education level influence students' cybersecurity behavior and awareness?
iii. To what extent does institutional support (e.g., infrastructure, policies, leadership) affect the implementation of cybersecurity practices in schools?

Review

The conceptual review established a clear framework for understanding how cybersecurity awareness (CSA) is influenced by digital literacy (DL), education level (EL), institutional support (IS), cybersecurity training (CT), policy implementation (PI), and access to technology (ATT) among Grade 7–12 students in Sunwal Municipality's public and private schools.

Despite a growing body of international literature on cybersecurity education, surveillance, and digital safety, there remains a significant research gap in the context of Nepal. Studies from countries like Germany and the USA have explored how surveillance impacts psychological stress, trust, and productivity, but these are situated in contexts with strong data protection laws and individualistic cultures. Nepal, by contrast, operates within a collectivist framework where hierarchical respect and institutional compliance may alter how surveillance and digital risks are perceived and experienced. Empirical studies such as those by Voice of Children and KNH Germany (2023) and ChildSafeNet and SVRI have revealed alarming rates of cyber violence among Nepalese youth, with 42% experiencing cyberbullying and 17% receiving sexually explicit messages. However, these studies focus primarily on youth safety and do not address how digital risks are managed within educational institutions or workplaces. Similarly, research by Dhungana et al. (2023), Poudyal et al. (2025), and Khadka and Shahi (2024) highlights gaps in teacher preparedness and ICT proficiency, but lacks integration with cybersecurity-specific competencies or student outcomes.

While Rana and Rana (2020) and Gurung and Shrestha (2023) emphasize infrastructure and training gaps, they do not examine how these limitations affect the implementation of cybersecurity education or the psychological well-being of students and teachers. Shahi (2023) further identifies policy-level shortcomings, noting that only 30% of public institutions have designated cybersecurity officers and fewer than 20% conduct staff training, yet the study does not explore how these gaps translate into classroom-level vulnerabilities. No existing study in Nepal holistically examines how institutional support, teacher training, ICT infrastructure, and cultural attitudes interact to shape cybersecurity awareness and resilience among secondary school students. Moreover, the psychological impacts of digital surveillance in educational settings such as stress, anxiety, or behavioral withdrawal, remain underexplored. This research addresses these gaps by integrating empirical data from both public and private schools based in Nawalparasi district, examining how institutional readiness, teacher competence, and policy enforcement collectively influence cybersecurity education outcomes.

By doing so, the study contributes to a more nuanced understanding of digital safety in Nepal's education system, offering evidence-based recommendations for policy, training, and infrastructure development tailored to the country's socio-cultural and institutional realities.

RESEARCH METHODS

The study collects information from teachers in Sunwal Municipality's public and private schools that use digital tools, like Google Classroom, Kahoot! or internet-enabled devices. It used a survey to ask teachers about their experiences and how they help students stay safe online.

The descriptive aspect focuses on showing what's going on, like whether private schools use engaging tools like Kahoot! to teach students about phishing or if public school teachers feel prepared to discuss cyberbullying. The correlational part examines whether certain factors are linked, such as if schools with better internet access have students who are better at spotting online risks, or if trained teachers boost students' awareness of cyber threats. The survey itself involves a questionnaire with 48 questions; six about the teachers' backgrounds, like their years of teaching, and 42 about cyber safety topics, such as digital skills or school support systems. For instance, teachers might answer questions like, "Do your students know how to create strong passwords?" or "Does your school have Wi-Fi for cyber lessons?" This design is effective because it allows the

study to connect with many teachers (384) from diverse schools, ranging from public ones with basic setups to private ones with advanced computer labs, answering questions like whether private schools teach more about staying safe online or if teacher training helps students avoid cyber risks. The data were collected using a structured questionnaire comprising 6 demographic questions and 42 Likert-scale items, designed to measure seven constructs: Digital Literacy, Education Level, Institutional Support, Cybersecurity Training, Policy Implementation, Access to Technology, and Cybersecurity Awareness. Descriptive statistics were computed using Microsoft Excel to summarize frequencies, means, and standard deviations. Inferential statistics were conducted using SPSS to test the proposed hypotheses and model the relationships between latent variables.

The study employed descriptive-correlational survey design to analyze data collected from 384 teachers across 12 schools (7 public, 5 private) in Sunwal Municipality, Nawalparasi district, focusing on the factors influencing cybersecurity awareness (CSA) among Grade 7–10 students. The key variables included CSA as the dependent variable, digital literacy (DL), education level (EL), policy implementation (PI), and access to technology (ATT) as independent variables, and institutional support (IS) and cybersecurity training (CT) as mediators. Statistical analyses were conducted using SPSS, with the PROCESS macro facilitating advanced mediation analysis to test the complex relationships outlined in the conceptual framework.

Results And Discussion

Descriptive Statistics of Digital Literacy

Table 1

Descriptive Statistics of Digital Literacy

Statement	Mean	Std. Deviation
I can confidently use digital tools like, Google Classroom, or Zoom.	4.05	1.300
I know how to identify phishing emails or suspicious links.	3.40	1.429
I teach students about safe internet practices.	3.76	1.366
I can guide students on how to create strong passwords.	3.54	1.459
I regularly update my digital skills through training or self-learning.	3.69	1.265
I feel confident using digital platforms for teaching securely.	3.71	1.326

Source: SPSS Results based on Primary Data 2025

These findings, grounded in Nepal's context of rapid digital transformation and limited cybersecurity education, underscore the need for targeted teacher training to address gaps, particularly in public schools, to enhance cybersecurity education for students.

Table 2

Descriptive Statistics of Education Level

Statement	Mean	Std. Deviation
My academic background has prepared me to teach digital safety.	3.54	1.316
I have received formal training in ICT or digital pedagogy.	2.91	1.529
I understand how to integrate cybersecurity into my subject area.	3.48	1.206
I am aware of the ethical responsibilities of using digital tools.	3.91	1.225
I feel confident discussing cyber threats with students.	3.96	1.257
I believe my education level helps me promote digital safety.	3.83	1.095

Source: SPSS Results based on Primary Data 2025

The descriptive statistics reveal varying levels of teacher preparedness influenced by their education level, with the highest confidence in discussing cyber threats (mean = 3.96) and ethical responsibilities (mean = 3.91), but a notable gap in formal ICT training (mean = 2.91). High standard deviations (1.095–1.529) reflect variability, likely due to disparities in school type, location, and training access, supporting the hypothesis (H_{12}: Education level significantly affects cybersecurity behavior).

Table 3

Descriptive Statistics of Institutional Support

Statement	Mean	Std. Deviation
My school has clear policies on digital safety and cybersecurity.	3.57	1.253
We have access to secure internet and digital infrastructure.	3.89	1.165
The school administration supports digital safety initiatives.	3.89	1.220
There is a designated ICT coordinator or support staff in my school.	3.62	1.283
I receive regular updates or training on cybersecurity from the school.	3.25	1.404
My school encourages reporting of cyber incidents.	3.61	1.218

Source: SPSS Results based on Primary Data 2025

These findings underscore the need for stronger policy enforcement and training programs, particularly in public schools, to bolster cybersecurity education in Nepal's digital education system.

Table 4

Descriptive Statistics of Cybersecurity Training

Statement	Mean	Std. Deviation
I have attended workshops or training on cybersecurity.	2.86	1.428
I know how to respond to cyberbullying or online harassment cases.	3.57	1.323
I have taught students about phishing, malware, or online scams.	3.44	1.568
I feel prepared to handle a cybersecurity incident in school.	3.59	1.236
I use real-life examples to teach students about digital threats.	3.69	1.241
I believe cybersecurity training should be mandatory for all teachers.	4.50	0.914

Source: SPSS Results based on Primary Data 2025

These findings enable access to insights into the critical role of training in fostering CSA, underscoring the need for stronger policy enforcement and professional development programs, particularly in public schools, to enhance cybersecurity education in Nepal's digital education system.

Table 6

Descriptive Statistics of Policy Implementation

Statement	Mean	Std. Deviation
My school has clear policies on digital safety and cybersecurity.	3.57	1.253
We have access to secure internet and digital infrastructure.	3.89	1.165
The school administration supports digital safety initiatives.	3.89	1.220
There is a designated ICT coordinator or support staff in my school.	3.62	1.283
I receive regular updates or training on cybersecurity from the school.	3.25	1.404
My school encourages reporting of cyber incidents.	3.61	1.218

Source: SPSS Results based on Primary Data 2025

The results underscore the urgent need for standardized cybersecurity policies and enhanced training programs, particularly in public schools, to enable access to effective digital safety measures and bolster cybersecurity education in Nepal's collectivist and digitally disparate educational system.

Table 7

Descriptive Statistics of Access to Technology

Statement	Mean	Std. Deviation
My school has reliable internet access.	4.13	1.094
Students have access to computers or digital devices.	4.08	0.998
We use digital platforms like Google Classroom or Moodle.	3.54	1.274
I can access cybersecurity resources online when needed.	3.73	1.150
Students are taught how to use digital tools responsibly.	3.88	1.136
Lack of access to technology limits our ability to teach cybersecurity.	3.93	1.097

Source: SPSS Results based on Primary Data 2025

These findings support hypothesis H_{16} (Access to technology enhances CSA), as higher ATT scores in private schools correlate with elevated CSA levels (mean: 4.12 vs. 3.89 in public schools). The results highlight the critical need for enhanced technological infrastructure, particularly in public schools, to enable access to effective cybersecurity education in Nepal's collectivist and digitally disparate educational system.

Table 8

Descriptive Statistics of Cybersecurity Awareness

Statement	Mean	Std. Deviation
I understand the importance of cybersecurity in education.	4.02	1.117
I can identify common cyber threats faced by students.	3.80	1.204
I feel confident promoting safe digital behavior among students.	3.74	1.197
I have witnessed or handled a cyber-incident in my school.	3.43	1.390
Students in my school are aware of basic cybersecurity practices.	3.55	1.224
I believe cybersecurity awareness should be part of the school curriculum.	4.46	0.923

Source: SPSS Results based on Primary Data 2025

High standard deviations (0.923–1.390) assess variability, driven by disparities between public and private schools in Sunwal Municipality, where private schools report higher CSA (mean: 4.12 vs. 3.89). These findings support hypothesis H_{11} (Digital literacy enhances CSA), as higher awareness correlates with better access to resources, underscoring the need for curriculum integration and enhanced training to enable access to robust cybersecurity education in Nepal's collectivist and digitally disparate educational system.

Table 9

Cronbach's Alpha Coefficients

S. No.	Variables	Cronbach's Alpha
1.	Digital Literacy	0.914
2.	Education Level	0.900
3.	Institutional Support	0.894
4.	Cybersecurity Training	0.883
5.	Policy Implementation	0.925
6.	Access to Technology	0.862
7.	Cybersecurity Awareness	0.886

Source: SPSS Results based on Primary Data 2025

Cybersecurity Training (α = 0.883) and Cybersecurity Awareness (α = 0.886) reflected good reliability, suggesting that while the items were coherent, some variability may exist due to differences in training exposure and awareness levels among teachers. Access to Technology (α = 0.862), though slightly lower, still demonstrated good reliability, likely influenced by infrastructural disparities between public and private schools and urban versus semi-urban settings in Nepal

Table 10

Collinearity Statistics

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig.	Collinearity Statistics	
	B	Std. Error	Beta			Tolerance	VIF
(Constant)	0.331	0.140		2.359	0.019		
DL	0.150	0.053	0.150	2.835	0.005	0.224	4.470
EL	-0.032	0.052	-0.035	-0.607	0.544	0.194	5.154
IS	0.065	0.048	0.070	1.366	0.173	0.240	4.165
CT	0.399	0.047	0.435	8.500	0.000	0.240	4.163
PI	0.084	0.053	0.094	1.574	0.116	0.178	5.631
ATT	0.316	0.042	0.288	7.476	0.000	0.424	2.359

a. Dependent Variable: CA

Source: SPSS Results based on Primary Data 2025

In summary, this regression coefficient table not only quantifies the influence of each variable but also reinforces the broader narrative of the study: that cybersecurity awareness is a product of deliberate, systemic efforts. Training, access, and literacy are the pillars of effective digital safety education, while policy and grade level alone are insufficient without active implementation and support. These findings offer a clear roadmap for educators, administrators, and policymakers in Nepal to build safer, more digitally resilient learning environments for students.

Table 11

Hypotheses Test

Hypothesis Statement	p-value	Result
H_{11}: Digital Literacy significantly affects Cybersecurity Awareness.	< .0000 (β = 0.150, SE = 0.052, t = 2.885, 95% CI [0.048, 0.252])	Accepted
H_{12}: Education Level significantly affects Cybersecurity Awareness.	.544 (β = 0.032, SE = 0.052, t = 0.615, 95% CI [-0.070, 0.134])	Rejected
H_{13}: Institutional Support significantly affects Cybersecurity Awareness.	< .0000 (β = 0.172, SE = 0.048, t = 3.583, 95% CI [0.078, 0.266])	Accepted
H_{14}: Cybersecurity Training significantly affects Cybersecurity Awareness.	< .0000 (β = 0.435, SE = 0.060, t = 7.250, 95% CI [0.317, 0.553])	Accepted
H_{15}: Policy Implementation significantly affects Cybersecurity Awareness.	.116 (β = 0.076, SE = 0.048, t = 1.583, 95% CI [-0.018, 0.170])	Rejected
H_{16}: Access to Technology significantly affects Cybersecurity Awareness.	< .0000 (β = 0.288, SE = 0.055, t = 5.236, 95% CI [0.180, 0.396])	Accepted
H_{17}: Institutional Support significantly mediates the effect of Digital Literacy on Cybersecurity Awareness.	> .05 (Indirect: 0.038, BootSE = 0.025, 95% BootCI [-0.011, 0.087]; IS → CSA: β = 0.172, p < .0000)	Rejected
H_{17}: Cybersecurity Training significantly mediates the effect of Digital Literacy on Cybersecurity Awareness.	< .05 (Indirect: 0.189, BootSE = 0.041, 95% BootCI [0.108, 0.270]; CT → CSA: β = 0.435, p < .0000)	Accepted

H_{17}: Institutional Support significantly mediates the effect of Access to Technology on Cybersecurity Awareness.	< .05 (Indirect: 0.094, BootSE = 0.029, 95% BootCI [0.037, 0.151]; IS → CSA: β = 0.172, p < .0000)	Partially Supported

Source: SPSS Results based on Primary Data 2025

The study's analysis, based on SPSS outputs from a 2025 survey in Sunwal Municipality, Nawalparasi district (n = 384), confirms the significant effects of Digital Literacy (DL), Institutional Support (IS), Cybersecurity Training (CT), and Access to Technology (ATT) on Cybersecurity Awareness (CSA) among Grade 7–12 students, with mediation by IS and CT. The findings align with the thesis objectives and test hypotheses H_{11}–H_{17}, revealing both expected and unexpected patterns in Nepal's collectivist and digitally evolving educational context, where cultural norms and uneven infrastructure shape cyber behaviors. Below, the major findings are summarized, addressing direct effects, mediation, inconsistencies, and implications for schools and policymakers.

Conclusion

The findings address the research problem of low CSA, where 68% of students are vulnerable to cyber threats (Nepal Telecommunications Authority, 2023). CT and ATT's strong effects highlight actionable solutions, while EL and PI's non-significance reveal curriculum and enforcement gaps, particularly in public schools (61.5% of respondents). Nepal's collectivist culture (Hofstede, 2010) explains CT and IS's effectiveness, as students respect authority-driven training, unlike individualistic contexts where autonomy drives CSA (Senthil et al., 2024). Compared to global studies, Nepal's results reflect unique challenges, such as only 20% of public-school teachers receiving cybersecurity training vs. 75% in private schools (MoEST, 2024), emphasizing the need for targeted interventions to achieve equitable digital safety education.

While the findings are pending, preliminary hypotheses suggest that private schools, particularly in urban areas, demonstrate higher cybersecurity awareness due to better infrastructure, gamified learning tools (e.g., Kahoot, Scratch), and teacher training. Public and rural schools face challenges such as limited internet access, lack of trained staff, and absence of standardized cybersecurity curricula. Recommendations include integrating cybersecurity into national curricula, expanding teacher training, promoting localized content, and ensuring equitable access to digital tools.

REFERENCES

Davis, F. D. (1989). *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* MIS Quarterly, 13(3), 319–340.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2019). *Multivariate data analysis (8th ed.).* Cengage Learning.

Khader, M., Senthil, R., and Al-Khatib, H. (2021). *Cybersecurity awareness framework for academia (CAFA). Journal of Cybersecurity Education*, 5(2), 45–60.

Kolb, D. A. (1984). *Experiential learning: Experience as the source of learning and development.* Prentice Hall.

Moallem, M. (2019). *Cybersecurity awareness in educational environments. Journal of Educational Technology Systems,* 48(1), 5–22.

Pressman, J. L., and Wildavsky, A. (1973). *Implementation: How great expectations in Washington are dashed in Oakland.* University of California Press.

Van Dijk, J. A. G. M. (2005). *The deepening divide: Inequality in the information society.* SAGE Publications.

Vygotsky, L. S. (1978). *Mind in society: The development of higher psychological processes.* Harvard University Press.

Weiner, B. J. (2009). *A theory of organizational readiness for change. Implementation Science*, 4(1), 67.

Dhungana, R., Shrestha, S., and Panta, B. (2023). *Teacher preparedness and digital safety in Nepalese schools. Nepal Journal of Education and Technology,* 11(2), 34–49.

Gurung, A., and Shrestha, R. (2023). *Barriers to digital integration in Nepal's school system. Journal of ICT in Education,* 9(1), 15–28.

Khadka, B., and Shahi, R. (2024). *ICT proficiency and digital readiness among Nepalese teachers. Nepal Education Review,* 10(1), 22–35.

MoEST. (2024). *Annual report on digital education and cybersecurity policy implementation.* Ministry of Education, Science and Technology, Government of Nepal.

Nepal Telecommunications Authority. (2023). *Internet penetration and digital infrastructure report.* Kathmandu: NTA.

Poudyal, S., Karki, A., and Thapa, R. (2025). *Teacher awareness and competencies in cybersecurity education. Journal of Cybersecurity Education Research and Practice,* 12(1), 18–32.

Rana, K., and Rana, S. (2020). *ICT integration and teacher readiness in Nepalese schools.* Nepal Open University Press.

Shahi, R. (2023). *Cybersecurity policy implementation in Nepal: Gaps and opportunities.* Kathmandu Policy Review, 7(2), 40–55.

Shrestha, P., Acharya, D., and Gautam, R. (2024). *Cyber threat exposure among Nepalese youth.* Nepal Youth Digital Safety Report, 6(1), 10–25.

ViN. (2024). *Digital literacy among rural educators in Nepal.* Volunteers Initiative Nepal Annual Report.

TVN. (2023). *Institutional cybersecurity practices in model schools.* Transcend Vision Nepal Case Study Series.

ChildSafeNet and SVRI. (2023). *Digital safety assessment among Nepalese adolescents.* Kathmandu: ChildSafeNet.

Voice of Children and KNH Germany. (2023). *Cyber violence among Nepalese youth: A survey report.* Kathmandu: Voice of Children.