Cybersecurity Awareness and Practices Among Teachers in Mahendranagar, Kanchanpur, Nepal: An Exploratory Protection Motivation Perspective

Santosh Bhatt

Santosh.bhatt@nsu.edu.np
https://orcid.org/0009-0003-5059-8055
https://doi.org/10.3126/srj.v1i2.99148

Abstract

This study examined cybersecurity awareness and practices among 165 school and higher education teachers in Mahendranagar, Kanchanpur, Nepal, using Protection Motivation Theory (PMT) as its theoretical framework. The study investigated teachers' perceptions of cyber threats, online security behaviors, and cybersecurity practices in their professional roles. Data were collected using a 23-item structured questionnaire developed from the study objectives and reviewed by subject experts for content relevance and clarity. It contained Likert-scale and open-ended items. Quantitative data were analyzed using IBM SPSS Statistics, Version 26, through descriptive statistics, independent-samples t-tests, one-way analysis of variance, and Pearson correlation.

The findings indicate a clear gap between cybersecurity awareness and the use of secure cybersecurity practices. Although awareness of common threats such as phishing was relatively high ($M = 3.82$), use of key security measures such as Multi-Factor Authentication (MFA) ($M = 2.42$) and regular password rotation ($M = 2.15$) was limited. Statistical analysis showed that gender was not significantly associated with cybersecurity awareness ($p > .05$). However, cybersecurity practice scores differed significantly across institutional types, $F(2, 162) = 8.21$, $p < .001$, $\eta^2 = .092$. Tukey's HSD post-hoc comparisons indicated that teachers from private/institutional schools reported significantly higher practice scores than those from government schools ($p = .004$). Moreover, teaching experience was weakly negatively correlated with secure digital practices ($r = -.18$, $p = .021$), suggesting that educators with greater teaching experience reported slightly lower levels of cybersecurity practice adoption. Limited awareness of the Electronic Transactions Act, 2063 (2008) ($M = 2.10$) also revealed a gap in cybersecurity-related legal knowledge.

Overall, the findings suggest that cybersecurity practices vary across institutions and have not been consistently integrated into teachers' professional routines. To improve cybersecurity in educational settings, the findings support the adoption of Multi-Factor Authentication by educational institutions, the development of locally relevant cybersecurity law-awareness programs, and the appointment of dedicated

cybersecurity coordinators to facilitate implementation of the National Cyber Security Policy, 2023.

Keywords: Cybersecurity Awareness; Cybersecurity Practices; Nepal Education; Teacher Professional Development; Protection Motivation Theory; Electronic Transactions Act; Nepal.

Introduction

The online age has revolutionized the Field of education, so cybersecurity is now a critical issue of school educators around the globe.The widespread adoption of online learning environments has increased educators' exposure to cybersecurity risks, so that teachers are now the first line of defense against cybercrime like phishing, data breaches, and malware, which can put both teachers and students in danger. In resource strained areas like Nepal where internet penetration has soared yet protection is still behind, teachers tend to navigate such dangers without proper preparation. This paper will target teachers in Mahendranagar changes to investigate their practices and awareness. Even basic knowledge of risks, including identifying suspicious emails or locking devices, can help to prevent incidents, but most educators are focused on teaching rather than on self-protection in the environment of daily stress. This study highlights how well-informed teachers can create safer online learning conditions among the youth in Nepal by analyzing these dynamics using a structured questionnaire.

Nepal's transition toward digital technologies has increased the importance of cybersecurity in the education sector. The Government of Nepal has progressively developed legal and policy frameworks to address emerging digital and cybersecurity risks, including the Electronic Transactions Act, 2063 (2008) and the National Cyber Security Policy, 2023. The National Cyber Security Policy 2023 emphasizes strengthening cybersecurity awareness, institutional capacity, information security, and the skills required to respond to emerging cyber threats. The expansion of internet connectivity, digital devices, online learning platforms, and electronic communication in educational institutions has consequently increased the need for cybersecurity awareness and appropriate security practices among teachers. However, the availability of cybersecurity infrastructure, technical support, and professional development opportunities remains uneven across educational institutions, particularly outside major urban centers. Previous studies in Nepal have also reported gaps in teachers' cybersecurity awareness, practical skills, and institutional support. These challenges highlight the need for localized research examining teachers' cybersecurity awareness and practices in areas such as Mahendranagar, Kanchanpur.

In spite of these policies, there are limitations to implementation such as poor infrastructure, training budgets and congested curricula in the peripheral schools in

Kanchanpur. Although Nepal has developed national cybersecurity laws and policies, the implementation of cybersecurity practices may vary across educational institutions because of differences in technical resources, training opportunities, and institutional support (Government of Nepal, 2008; Government of Nepal, Ministry of Communication and Information Technology, 2023). The present study therefore examines these issues among teachers in Mahendranagar, Kanchanpur.

The research questions guiding this study are:

- What is the level of cybersecurity awareness among teachers in Mahendranagar, Kanchanpur?
- What cybersecurity practices are followed by teachers in their daily digital activities?
- What improvements can be suggested to enhance cybersecurity awareness and practices among teachers?

To answer these questions, the study was conducted with the following objectives:

- To assess cybersecurity awareness among teachers in Mahendranagar, Kanchanpur, teaching in public schools, private schools, and higher secondary campuses.
- To evaluate their cybersecurity practices and suggest context-specific improvements for strengthening digital safety in educational institutions.

Method

This study employed a quantitative descriptive survey design to examine cybersecurity awareness and practices among school and higher education teachers in Mahendranagar, Kanchanpur. Data were collected using a structured 23-item questionnaire administered through Google Forms. The questionnaire consisted of four sections: demographic information, cybersecurity awareness, cybersecurity practices, and teachers' experiences and suggestions. The awareness section included eight Likert-scale items related to threats such as phishing and malware, while the practice section included eight items related to password management, software updates, and other protective behaviors. The questionnaire was reviewed by experts to assess its content relevance and clarity.Data were collected between January and February 2025. Participation was voluntary, and informed consent was obtained from all participants. Anonymity and confidentiality were maintained throughout the study. Participants required approximately 10–12 minutes to complete the questionnaire. Data were analyzed using descriptive statistics (means, frequencies) using SPSS version 26, inferential statistics (t tests, ANOVA) to determine demographic correlations at α 0.05, and thematic analysis of two open ended questions to determine training gaps, which allowed specific recommendations to be made based on the objectives of the study.

Literature Review

Cybersecurity awareness has become critical in the education sector because of the rapid expansion of digital technologies, online learning platforms, cloud services, and internet-based communication across schools and campuses. Teachers are crucial in safeguarding educational environments, as they regularly use digital devices, handle student data, engage in online communication, and teach students how to use the internet safely. However, many studies have revealed that teachers are often not sufficiently aware of cybersecurity and safe digital practices, making them vulnerable to cyber threats like phishing, malware, identity theft, weak password use, cyberbullying and unsafe information sharing.

Research has emphasized that educational institutions must develop digital-safety awareness and practical cybersecurity skills among teachers. UNESCO (2023) explains that the expansion of technology in education creates important benefits but also increases concerns related to privacy, safety, and cybersecurity. Similarly, CISA (2023) recommends that K–12 institutions establish organized cybersecurity programs, provide staff training, protect sensitive information, and implement technical safeguards. These recommendations are relevant to teachers because they regularly use digital platforms, manage student information, and communicate through institutional systems.

Research from South Asia points to similar concerns. According to Rahman et al. (2020), cybersecurity education in schools is necessary due to the rise of cyber threats such as cyberbullying, online fraud, exposure to pornography, identity theft and unsafe internet usage. Key barriers include limited teacher expertise, inadequate training and scarce resources. Awareness programs, curriculum integration and teacher training are recommended to promote safer digital practices. This supports the present study by emphasizing the significance of evaluating teachers' cybersecurity awareness and practices within educational institutions. Previous research on teachers' cybersecurity awareness has emphasized the importance of continuous training, practical guidance, and institutional support (Ravichandran et al., 2025; Sapanca & Kanbul, 2022).Teachers' information-security awareness can vary across different security practices and digital environments, indicating the need for training that addresses practical behaviors rather than general awareness alone (Sapanca & Kanbul, 2022).

Nepal has established national legal and policy frameworks to address emerging cybersecurity risks. The Electronic Transactions Act, 2063 (2008) provides a legal basis for addressing electronic transactions and cyber-related offenses, while the National Cyber Security Policy, 2023 emphasizes cybersecurity awareness, institutional capacity, information security, and preparedness (Government of Nepal, 2008; Government of Nepal, Ministry of Communication and Information Technology, 2023). However, the present study provides localized evidence concerning teachers in Mahendranagar,

Kanchanpur, a population that is not directly represented by these national policy documents.

Protection Motivation Theory explains how perceived threat severity, perceived vulnerability, response efficacy, and self-efficacy can influence protective behavioramong educators (Rogers, 1975).Rogers (1975) originally proposed Protection Motivation Theory, explaining that perceived severity, vulnerability, response efficacy, and self-efficacy predict protective behaviors. PMT provides a useful theoretical lens for interpreting teachers' cybersecurity intentions and actions.

International evidence shows that the use of technology in education creates both opportunities and cybersecurity risks, including threats to privacy, data protection, and online safety (UNESCO, 2023). For schools, CISA (2023) recommends staff training, risk management, multi-factor authentication, patch management, and institutional cybersecurity planning. In Nepal, official Nepal Police statistics provide evidence of cybercrime complaints and incidents, including cyber-related offenses reported during fiscal year 2080/81 (Nepal Police, 2024).

Nepal's National Cyber Security Policy, 2023, emphasizes cybersecurity awareness, digital safety practices, institutional capacity, and preparedness across sectors, including education (Government of Nepal, Ministry of Communication and Information Technology, 2023).

Despite this body of work, research specifically focused on teachers in Mahendranagar, Kanchanpur (western Nepal) remains limited. Existing literature and policy reports provide broader information about cybersecurity and digital safety in education; however, localized evidence concerning school and higher education teachers in Mahendranagar, Kanchanpur, remains limited. This study addresses that gap by examining teachers' cybersecurity awareness, reported practices, and training needs across different institutional settings.

The differerent literature shows substantial international and national attention to cybersecurity awareness in education, yet gaps remain that this study addresses. First, there is limited evidence from studies that specifically target school and campus teachers in Mahendranagar, Kanchanpur. Existing research tends to focus on students, university populations, or general internet users, paying less attention to teachers' roles and preparedness in fostering cybersecurity in schools.Second, most prior studies measure general cybersecurity awareness, while comparatively fewer investigate teachers' practical cybersecurity behaviors such as password management, phishing recognition, software update habits, and safe handling and sharing of information in educational settings.Third, there are limited localized comparisons between teachers across different institutional contexts such as public schools, private schools, and campuses in Nepal. By generating empirical data on teachers' cybersecurity awareness and practices in Mahendranagar and comparing these across institutional types, this study addresses an important evidence gap and supports the design of targeted interventions to strengthen cybersecurity preparedness in the region's educational settings.

Methodology

This study used a quantitative descriptive survey design to study the level ofcybersecurity awareness and practices among school and higher education teachers in Mahendranagar, Kanchanpur. Data were collected using a structured online questionnaire conducted via Google Forms. The questionnaire measure teachers' ability to recognize common cyber threats in their daily professional work and their use of key cybersecurity measures, such as strong password management, safe internet practices, and regular software updates.

A non-probability convenience sampling approach was used. The questionnaire link was distributed through teachers' email networks and institutional communication groups, and participation was voluntary.

The final sample consisted of 165 teachers. This sample size was considered adequate for the descriptive and inferential analyses used in the study, while the interpretation of inferential results was based on the observed effect sizes, significance levels, and assumptions of the respective statistical tests.

Data Collection

Data were collected between January and February 2025 using a structured 23-item questionnaire distributed through Google Forms to teachers from public schools, private schools, and higher secondary campuses in Mahendranagar, Kanchanpur. A total of 165 teachers participated in the study.

The questionnaire was developed in accordance with the objectives of the study and existing research on teacher cybersecurity awareness and practices. The questionnaire included four sections: demographic information (4 items), cybersecurity awareness (8 Likert-scale items related to recognition of threats such as phishing and malware), cybersecurity practices (8 Likert-scale items related to behaviors such as password management and software updating), and experience and feedback (3 descriptive questions related to cybersecurity interests, activities, and suggestions). The questionnaire was reviewed and validated through expert consultation to ensure content relevance and clarity.

The Google Form link was shared through teachers' email networks and school communication groups, allowing participants to complete the survey using their mobile phones or digital devices within approximately 10–12 minutes. Ethical considerations were carefully maintained throughout the study, including informed consent, voluntary participation, anonymity, and confidentiality of responses. After collection, the data were checked and entered twice to ensure accuracy and reliability before analysis.

Data Analysis

Quantitative data from the 165 valid survey responses were analyzed using IBM SPSS Statistics (Version 26.0) at a significance threshold of $\alpha = .05$. Initial data

screening verified completeness and distributional normality before computing descriptive statistics (M, SD, frequencies, and percentages) to summarize baseline cybersecurity awareness and practice levels. Inferential tests were conducted to examine selected group differences and associations. Specifically, an independent-samples t-test was used to compare cybersecurity awareness scores by gender, a one-way Analysis of Variance (ANOVA) with Tukey's HSD post-hoc comparisons was used to examine differences in cybersecurity practice scores across institution types, and Pearson correlation was used to examine the relationship between teaching experience and cybersecurity practices.

Qualitative responses from the open-ended survey items were analyzed using Braun and Clarke's reflexive thematic analysis framework across six iterative phases: data familiarization, initial inductive coding, theme generation, theme review, theme definition, and narrative synthesis. The analysis identified institutional constraints, including limited structured cybersecurity training, inadequate IT infrastructure, and insufficient administrative support, while also capturing teachers' preferences for practical professional development. The qualitative findings were used to complement the quantitative results and inform context-specific recommendations aligned with Protection Motivation Theory (PMT) and Nepal's National Cyber Security Policy (2023).

Demographic Profile of Respondents

A total of 165 educators from selected schools and higher secondary institutions in Mahendranagar, Kanchanpur participated in the survey. The sample represented diverse age groups, teaching experience levels, and institutional contexts, providing a foundation for examining cybersecurity awareness and practices among educators. Table 1 presents the demographic characteristics of the respondents.

Table 1 Demographic Characteristics of Teacher Respondents (N = 165)

Variable	**Category**	**n**	**%**
Age Group	20–30 years	16	9.7
	31–40 years	123	74.5
	41–50 years	26	15.8
	51+ years	0	0.0
Gender	Male	83	50.3
	Female	82	49.7
Teaching Experience	0–5 years	33	20.0
	6–10 years	96	58.2
	11–20 years	29	17.6
	21+ years	7	4.2
Institutional Type	Government School	65	39.4
	Private/Institutional	60	36.4
	Higher Secondary/Campus	40	24.2

The sample consisted primarily of mid-career educators. Nearly three-quarters of the respondents were between 31 and 40 years of age (74.5%, n=123), while no respondents were older than 50 years. Regarding teaching experience, most respondents reported 6 -10 years of experience (58.2%, n=96), indicating that the sample mainly represented educators with moderate professional experience.

The gender distribution was relatively balanced, with 83 male respondents (50.3%) and 82 female respondents (49.7%). This distribution provided relatively comparable groups for gender-based analysis.

Regarding institutional affiliation, government-school teachers represented the largest group (39.4%, n=65), followed by private/institutional-school teachers (36.4%, n=60). Higher-secondary or campus teachers represented 24.2% of the sample (n=40). This distribution supported comparisons of cybersecurity awareness and practices across institutional contexts.

Teachers' Awareness of Cybersecurity Threats and Concepts (N=165)

To assess teachers' awareness of cybersecurity threats and protective measures, respondents rated eight awareness-related statements using a five-point Likert scale ranging from 1 (Strongly Disagree/Minimal Awareness) to 5 (Strongly Agree/High Awareness). The mean scores across the major cybersecurity awareness domains are presented in Figure 1.

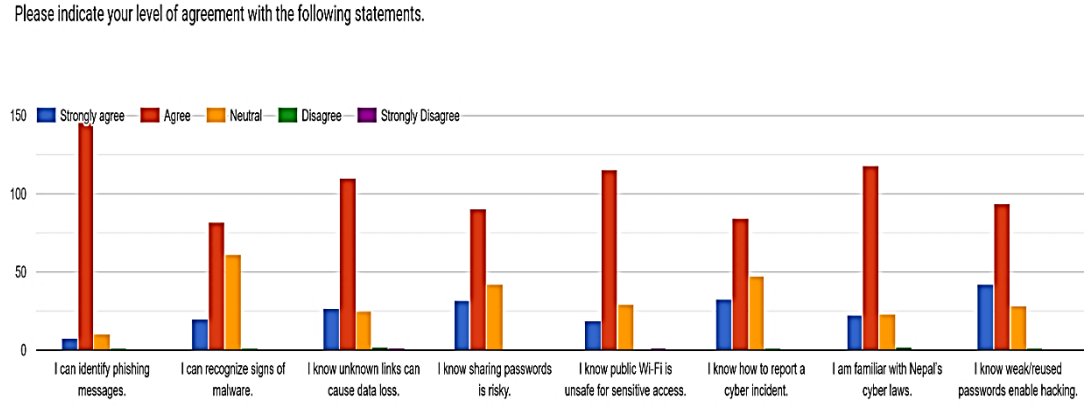


Figure 1: Mean Awareness Scores Across Key Cybersecurity Domains

The results demonstrate a clear structural divide in cybersecurity awareness among educators in Mahendranagar, Kanchanpur. While participants exhibited solid recognition of everyday, high-visibility cyber threats, their understanding of technical safeguards and

legal frameworks remained notably underdeveloped. This uneven profile indicates that general digital literacy does not automatically translate into procedural or regulatory security knowledge.

Among the assessed domains, awareness of phishing threats yielded the highest mean score (M = 3.82, SD = 0.89). This finding suggests that respondents were relatively familiar with phishing-related threats. Framed within Protection Motivation Theory (PMT), this strong performance reflects heightened Threat Appraisal; frequent exposure to phishing attempts makes the risk tangible, immediate, and easily recognizable to educators.

In contrast, awareness of Nepal's cybersecurity legal framework, specifically the *Electronic Transactions Act, 2063 (2008),* recorded the lowest score (M=2.10, SD=0.95). This lower score suggests a gap between recognizing common online threats and understanding Nepal's cybersecurity-related legal framework. Although teachers recognize suspicious digital activity, they lack clarity regarding institutional obligations and state mechanisms for handling data breaches or cyber harassment.

Awareness of malware-related threats was moderate (M = 2.95, SD = 1.02), showing that while teachers understand the existence of malicious software, they lack technical insight into how malware spreads, executes, or gets mitigated. Similarly, awareness of Multi-Factor Authentication (MFA) was low (M = 2.64, SD = 0.88). Within the PMT framework, this indicates a deficit in Coping Efficacy; educators recognize that digital environments carry risk, but they lack exposure to and confidence in using modern authentication technologies designed to mitigate those risks.

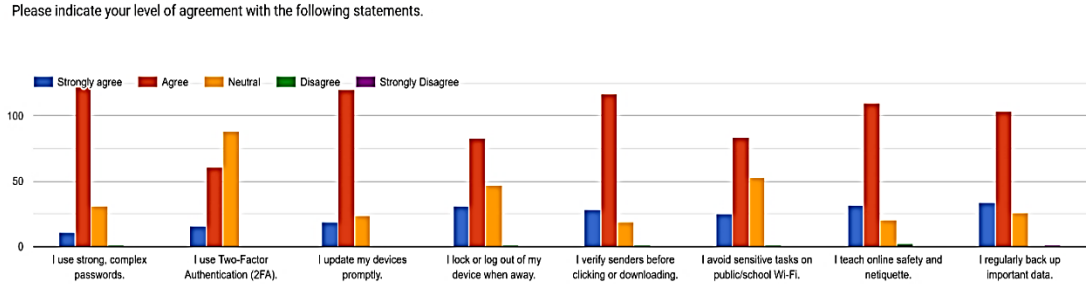
Synthesizing these findings highlights an explicit awareness–preparedness gap. Educators can identify visible threats, but they lack the technical capability and legal knowledge required to execute proactive defenses. Bridging this gap requires educational institutions in Kanchanpur to transition from generic computer training to structured cybersecurity curricula focused on MFA adoption, credential protection, and regulatory compliance.

Given that the vast majority of respondents are mid-career educators aged 31–40 years (74.5%), this cohort represents a stable, highly influential demographic within local schools. Targeted professional development for this group can establish lasting institutional standards, transforming basic threat recognition into sustained, protective cybersecurity habits.

Cybersecurity Practices among Educators

To examine how educators apply cybersecurity knowledge in their daily digital activities, participants responded to eight practice-related statements using a 5-point

Likert scale ranging from 1 (*Never*) to 5 (*Always*). Figure 2 presents the mean scores of reported cybersecurity practices across different digital behavior domains.



The analysis of self-reported cybersecurity behaviors reveals a pronounced awareness–practice gap among educators. Although teachers demonstrated relatively strong awareness of common cyber threats in the preceding section, their adoption of routine, protective security practices remain limited. This disparity confirms that recognizing digital risks does not automatically translate into the consistent execution of defensive behaviors within educational environments.

Among the assessed practices, creating complex passwords received the highest mean score (M = 3.65, SD = 0.92). This indicates that teachers generally recognize strong credentials as an essential first line of defense. However, this positive practice was severely offset by an exceptionally low rate of routine password rotation (M = 2.15, SD = 0.84). Viewed through Protection Motivation Theory (PMT), this contrast highlights a clear divide between Self-Efficacy and perceived Coping Cost. Teachers demonstrate high confidence in performing one-time setup tasks, but experience behavioral inertia when faced with recurring maintenance tasks that introduce perceived friction into their daily workflow.

Similarly, the implementation of Multi-Factor Authentication (MFA) was low (M = 2.42, SD = 0.90), directly mirroring the low awareness scores observed for this mechanism. This alignment demonstrates that educators systematically underutilize one of the most effective technical safeguards against unauthorized account access and identity theft.

A critical vulnerability identified in the data is the frequent convergence of personal and professional digital activities (M = 3.52, SD = 1.05). A substantial proportion of respondents reported using institutional devices or school networks for personal administrative and financial tasks. In the operational context of schools in Mahendranagar, Kanchanpur where may exist in some educational settings this practice

significantly elevates the risk of credential interception, cross-contamination, and sensitive institutional data exposure.

Gender	n	M	SD	t	df	p-value	Effect Size (Cohen's d)	Result
Male	83	3.12	0.64	1.42	163	0.157	0.22	Not Significant
Female	82	2.98	0.62					

Furthermore, software updating habits remained moderate (M = 2.88, SD = 1.01), indicating that routine system patching is not consistently prioritized. Deferring operating system and application updates leaves devices exposed to known vulnerabilities, undermining existing perimeter defenses.

Overall, the findings demonstrate that teachers' cybersecurity practices are characterized by passive, initial security steps rather than active, continuous protection. Resolving this gap requires moving beyond generic ICT awareness toward structured institutional governance. Establishing clear school-level policies, enforcing mandatory MFA adoption, automating system updates, and providing context-specific training will be essential to transform passive threat awareness into a sustained culture of proactive cybersecurity practice.

Impact of Gender on Cybersecurity Awareness (T-Test)

An independent-samples t-test was conducted to evaluate whether cybersecurity awareness differed significantly between male and female educators. The analysis compared composite mean awareness scores across both groups to determine whether gender influenced teachers' overall understanding of digital threats and protective concepts.

Table 3 T-test Comparison of Awareness by Gender

Note: Statistical significance was evaluated at $\alpha = .05$. Composite awareness scores were measured on a 5-point Likert scale.

The results indicate that while male teachers reported a slightly higher mean awareness score (M = 3.12, SD = 0.64) than female teachers (M = 2.98, SD = 0.62), this difference was not statistically significant, $t(163) = 1.42$, $p = .157$, $d = 0.22$. The small effect size further confirms that gender exerts a minimal practical impact on awareness levels among respondents.

These comparable mean scores suggest that male and female educators in Mahendranagar, Kanchanpur maintain similar baseline levels of cybersecurity threat

recognition and procedural knowledge. This equity likely stems from shared institutional dynamics: teachers across genders face similar workplace environments, handle common administrative digital tasks, and experience identical institutional limitations regarding formal cybersecurity training and policy support.

This outcome aligns with the broader empirical pattern established in this study namely, that cybersecurity awareness deficits are structurally driven rather than demographically determined. Rather than reflecting gender-based disparities, gaps in technical knowledge, legal literacy, and Multi-Factor Authentication (MFA) usage are broadly distributed across the teaching workforce. Consequently, institutional intervention programs, professional development workshops, and capacity-building initiatives should be designed for universal delivery across the entire academic staff without requiring gender-targeted differentiation.

Comparison of Practices by School Type (ANOVA)

A one-way Analysis of Variance (ANOVA) was conducted to evaluate whether teachers' self-reported cybersecurity practices differed significantly across three types of educational institutions: Government (Public) Schools, Private/Institutional Schools, and Higher Secondary Schools/Campuses.

Table 4 One-way ANOVA for Cybersecurity Practices across Institutions

Source	**SS**	**df**	**MS**	**F**	**p**	**η^2**
Between Groups	11.28	2	5.64	8.21	< .001	.092
Within Groups	111.26	162	0.69			
Total	122.54	164				

*Note.*Statistical significance was evaluated at $\alpha = .05$. Post-hoc comparisons were conducted using Tukey's Honest Significant Difference (HSD) test. $\eta^2 = 0.092$ indicates a medium effect size.

The one-way ANOVA revealed a statistically significant difference in cybersecurity practice scores across the three institution types, $F(2, 162) = 8.21$, $p < .001$, $\eta^2 = .092$. The effect size indicates a medium magnitude of institutional differences in reported cybersecurity practices. The mean practice score was highest among teachers in Private/Institutional Schools ($M = 3.45$, $SD = 0.81$), followed by Higher Secondary Schools/Campuses ($M = 3.10$, $SD = 0.87$) and Government Schools ($M = 2.85$, $SD = 0.82$).

This finding represents a pivotal insight for the study. While demographic factors such as gender yielded uniform threat awareness levels, practical security

implementation is strongly moderated by the institutional environment. Viewed through Protection Motivation Theory (PMT), This difference may reflect variations in institutional resources, digital policies, or administrative support; however, these factors require further investigation. which act as external facilitators that reduce the perceived Coping Cost (friction) of maintaining secure digital habits.

In contrast, the lower practice scores in government schools highlight structural constraints, such as unmanaged shared workstations, lack of institutional IT policy enforcement, and absent administrative mandates. This divergence confirms that individual awareness alone is insufficient to sustain secure behaviors; organizational support, technical enforcement (e.g., mandatory MFA and automated updates), and active administrative governance are critical determinants of actual cybersecurity practice among educators.

Correlation Between Teaching Experience and Cybersecurity Practices

A Pearson correlation analysis was conducted to examine the relationship between teaching experience and educators' self-reported cybersecurity practices. A Pearson correlation showed a statistically significant but weak negative relationship between teaching experience and self-reported cybersecurity practices, $r(163)=-.18$, $p=.021$ This indicates that educators with greater teaching experience tended to report slightly lower adoption of cybersecurity practices. Although the relationship was weak, the finding suggests that some experienced educators may require additional support when adopting newer security measures, such as Multi-Factor Authentication (MFA), regular password updates, and other technology-based protection practices. From a Protection Motivation Theory (PMT) perspective, this pattern may reflect differences in educators' familiarity, confidence, and ability to adopt unfamiliar protective measures. Therefore, cybersecurity training programs should consider educators' professional backgrounds and provide practical, user-friendly guidance that helps teachers at different career stages develop consistent and effective cybersecurity practices.

Conclusion

The findings of this study highlight a significant awareness–practice gap among educators in Mahendranagar, Kanchanpur. Although teachers increasingly depend on digital platforms for instruction, communication, and administrative tasks, their cybersecurity practices have not developed at the same pace as their technology adoption. The demographic profile of respondents with the majority belonging to the 31–40 age group (74.5%) represents a digitally engaged teaching workforce with established technology habits; however, the empirical evidence demonstrates a critical need for structured cybersecurity training and institutional support.

Specifically, the results show that while teachers demonstrated relatively high awareness of visible cyber threats, particularly phishing (M = 3.82, SD = 0.89), their implementation of routine technical defenses remained limited, most notably Multi-Factor Authentication (MFA) adoption (M = 2.42, SD = 0.90) and software updating (M = 2.88, SD = 1.01). Furthermore, the statistically significant variation in security practices across institutional types, $F(2, 162) = 8.21$, $p < .001$, $\eta^2 = .092$, suggests that institutional context is associated with differences in reported cybersecurity practices. Additionally, widespread unfamiliarity with Nepal's Electronic Transactions Act, 2063 (2008) (M = 2.10, SD = 0.95) reveals that many educators operate without adequate understanding of cybersecurity-related legal responsibilities and reporting mechanisms. Ultimately, these findings indicate that improving cybersecurity in educational institutions requires moving beyond passive threat recognition toward practical, sustained, and institutionally supported security routines.

Recommendations

Based on these conclusions, a multi-tiered strategy involving government agencies, institutional leadership, and practical professional development initiatives is recommended:

1. **Strengthen Legal Literacy and Institutional Responsibility:**

Educational institutions must actively promote understanding of Nepal's digital legal framework. The Ministry of Education, Science and Technology (MoEST), in collaboration with relevant cybersecurity authorities such as the Nepal Police Cyber Bureau, should develop targeted capacity-building programs focused on the The Electronic Transactions Act, 2063 (2008) and the National Cyber Security Policy (2023). These programs should clarify teachers' legal responsibilities, safe management of student records, and formal procedures for reporting cyber incidents. Schools should also consider designating a trained faculty member as a local Cyber-Safety Focal Person to coordinate security practices and guide staff on compliance matters.

2. **Establish Technical Administrative Safeguards:**

Institutions should reduce sole reliance on voluntary individual compliance by implementing supportive technical controls. Given the low adoption rate of MFA (M = 2.42, SD = 0.90), schools and campuses should mandate multi-factor verification for institutional portals containing sensitive administrative and student data. Furthermore, to address the high frequency of mixing personal and professional digital activities (M = 3.52, SD = 1.05), school leadership should enforce clear workstation management policies, including separate user profiles on shared laboratory computers, automated operating system patching, and secure access protocols for institutional devices.

3. **Deploy Experience-Sensitive Professional Development:**

Training programs should accommodate variations in teachers' career stages and technological confidence. The weak negative correlation between teaching experience and cybersecurity practices ($r(163) = -.18$, $p = .021$) indicates that Educators with longer teaching experience may benefit from additional practical support when adopting unfamiliar security tools. Implementing peer-supported learning frameworks such as reverse mentorship programs where digitally proficient teachers assist senior colleagues can build confidence while minimizing workflow disruption. Finally, institutions should prioritize continuous micro-learning modules (e.g., periodic mobile-based security tips, live demonstrations, and brief setup sessions) over infrequent, lengthy training lectures.

Reference

Cybersecurity and Infrastructure Security Agency. (2023). *Protecting our future: Partnering to safeguard K–12 organizations from cybersecurity threats*. https://www.cisa.gov/topics/cybersecurity-best-practices/K12cybersecurity

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences* (2nd ed.). Lawrence Erlbaum Associates. https://doi.org/10.4324/9780203771587

Dhungana, R. K., Gurung, L., & Poudyal, H. (2023). Cybersecurity challenges and awareness of the multi-generational learners in Nepal. *Journal of Cybersecurity Education, Research and Practice, 2023*(2), Article 5. https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/5

Government of Nepal. (2008). *The Electronic Transactions Act, 2063 (2008)*. Nepal Law Commission. https://lawcommission.gov.np/content/13397/

Government of Nepal, Ministry of Communication and Information Technology. (2023). *National cyber security policy, 2023*. https://giwmscdntwo.gov.np/media/pdf_upload/National%20Cyber%20Security%20Policy_Engl ish_version_dowpymd.pdfNepal Police. (2024). *Suicide and cyber crime: Fiscal year 2080/81*. https://www.nepalpolice.gov.np/media/filer_public/fd/3e/fd3e1c95-aaa1-41bd- 815e-0221254141d4/fy_2080-81_suicide__cyber_crime_-_en.pdf

Rahman, N. A. A., Sairi, I. H., Zizi, N. A. M., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology, 10*(5), 378–382. https://doi.org/10.18178/ijiet.2020.10.5.1393

Ravichandran, R., Singh, S., & Sasikala, P. (2025). Exploring school teachers' cyber security awareness, experiences, and practices in the digital age. *Journal of Cybersecurity Education, Research and Practice, 2025*(1), Article 1. https://doi.org/10.62915/2472- 2707.1214

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114. https://doi.org/10.1080/00223980.1975.9915803

Sapanca, H. F., & Kanbul, S. (2022). Risk management in digitalized educational environments: Teachers' information security awareness levels. *Frontiers in Psychology, 13*, Article 986561. https://doi.org/10.3389/fpsyg.2022.986561

UNESCO. (2023). *Global education monitoring report 2023: Technology in education—A tool on whose terms?* UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000385723