IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Study of Awareness about Cyber Safety and Security Practices among Pre-Service Teacher Trainees

Dr. Vineeta Singh
Lecturer (Social Work)
District Institute of Education and Training, Etawah

ABSTRACT

Introduction: With the increasing integration of technology in education, awareness of cyber safety among educators has become crucial. This study focuses on pre-service teacher trainees, evaluating their knowledge and understanding of cyber safety concepts, identifying training gaps, and suggesting improvements for teacher education programs. The analysis is based on the responses of 97 trainees enrolled in the Diploma in Elementary Education (D.El.Ed.) program. **Material and methods:** The research employed a quantitative approach, collecting data from 97 pre-service teacher trainees. The study examined demographic characteristics, self-reported knowledge, and cyber safety practices. Statistical techniques were applied to identify patterns, levels of awareness, and areas requiring further attention. **Results:** Participants were primarily young (Mean±SD=23.39+2.89, Minimum=20, Maximum=35), with a balanced gender ratio and moderate levels of computer training. While 81.4% had prior knowledge of cyber safety, their understanding of specific threats like phishing was moderate. Despite high concerns about online privacy, confidence in managing cyber risks was relatively low. Poor password management practices and frequent password sharing highlighted substantial security vulnerabilities among trainees. **Conclusion:** The findings indicate that while pre-service teacher trainees possess basic cyber safety awareness, significant gaps remain in their knowledge and practices. The study emphasizes the need for enhanced digital security training within teacher education programs to better equip future educators in safeguarding themselves and their students from cyber risks.

Keywords: Cyber safety, pre-service teachers, digital security, cyber awareness, teacher training.

INTRODUCTION

The integration of digital technologies into education systems has reshaped the landscape of learning, leading to global adoption of strategies that incorporate Information and Communication Technology (ICT). The National Education Policy (NEP) 2020 underscores the importance of children's safety, including in digital environments. The COVID-19 pandemic has accelerated the adoption of digital technologies in education, transforming classrooms and learning experiences. These technologies not only serve as knowledge providers but also as mentors and evaluators. However, this digital shift comes with concerns over privacy, security, and cyber threats. Cybersecurity involves the protection of digital devices and networks from unauthorized access, data breaches, and other malicious activities. The growing number of cyberattacks highlights the urgent need for robust cybersecurity measures and awareness, especially in education, where the online learning environment exposes students to potential risks like cyberbullying and fraud. The NEP 2020 emphasizes protecting students from these threats, recognizing that the shift to online learning extends classroom boundaries into the digital realm.

The rationale behind this study is driven by the critical need to assess and enhance cybersecurity awareness among pre-service teacher trainees, who play a pivotal role in shaping future generations. Measuring their level of cybersecurity awareness is crucial to establishing a culture of safety and preparedness. This study focuses on assessing the awareness of cyber safety and security practices among pre-service teacher trainees, who are future educators responsible for guiding students in a digitalized world.

MATERIAL AND METHODS

This study employed a descriptive research design, ideal for providing a comprehensive understanding of the subject and related variables. The study's population consisted of 97 pre-service teacher trainees enrolled in a two-year teacher training program at the District Institute of Education and Training (DIET) in Etawah, Uttar Pradesh.

Data collection was carried out using a questionnaire designed to gather demographic information and insights into the trainees' knowledge, attitudes, and practices related to cyber safety and security. The questionnaire included sections on general awareness, specific knowledge of cybersecurity concepts, and practical security behaviors. The collected data were analyzed using SPSS and MS Excel, employing statistical techniques to identify patterns, assess levels of awareness, and highlight areas requiring further attention. The analysis focused on demographic characteristics, self-reported knowledge, and cyber safety practices.

RESULTS

Demographic characteristics

The demographic profile of the 97 study participants shows a young cohort with a mean age of 23.39 years (SD = 2.89). The participants' ages ranged from 20 to 35 years. The gender distribution was relatively even, with 54.6% female and 45.4% male participants. A significant portion of the participants (58.8%) were from urban areas, while 41.2% resided in rural regions. Most participants held a graduate degree (81.4%), while 50.5% lacked any computer certification (Table 1).

Table 1. Distribution of participants based on their demographic characteristics

Variables		Frequency (N)	Proportion (%)
Age (in years)	≤ 20	12	12.4
	21-25	80	82.5
	≥ 26	05	05.2
	Total	**97**	**100.0**
Mean±SD=23.39±2.89, Minimum=20, Maximum=35			
Gender	Female	53	54.6
	Male	44	45.4
	Total	**97**	**100.0**
Area of Residence	Rural	40	41.2
	Urban	57	58.8
	Total	**97**	**100.0**
Educational Qualification	Graduate	79	81.4
	Postgraduate	18	18.6
	Total	**97**	**100.0**
Possess any Computer Certificate	O Level	02	02.1
	ADCA	09	09.3
	CCC	37	38.1
	Doesn't have	49	50.5
	Total	**97**	**100.0**

Awareness of Cyber Safety and Security

Participants generally have a solid foundation of awareness regarding cyber safety, with 81.4% claiming prior knowledge and 72.2% having attended relevant educational events. Despite this awareness, there are gaps in understanding sensitive personal information and in recognizing certain online threats, like phishing and unexpected pop-ups (Table 2).

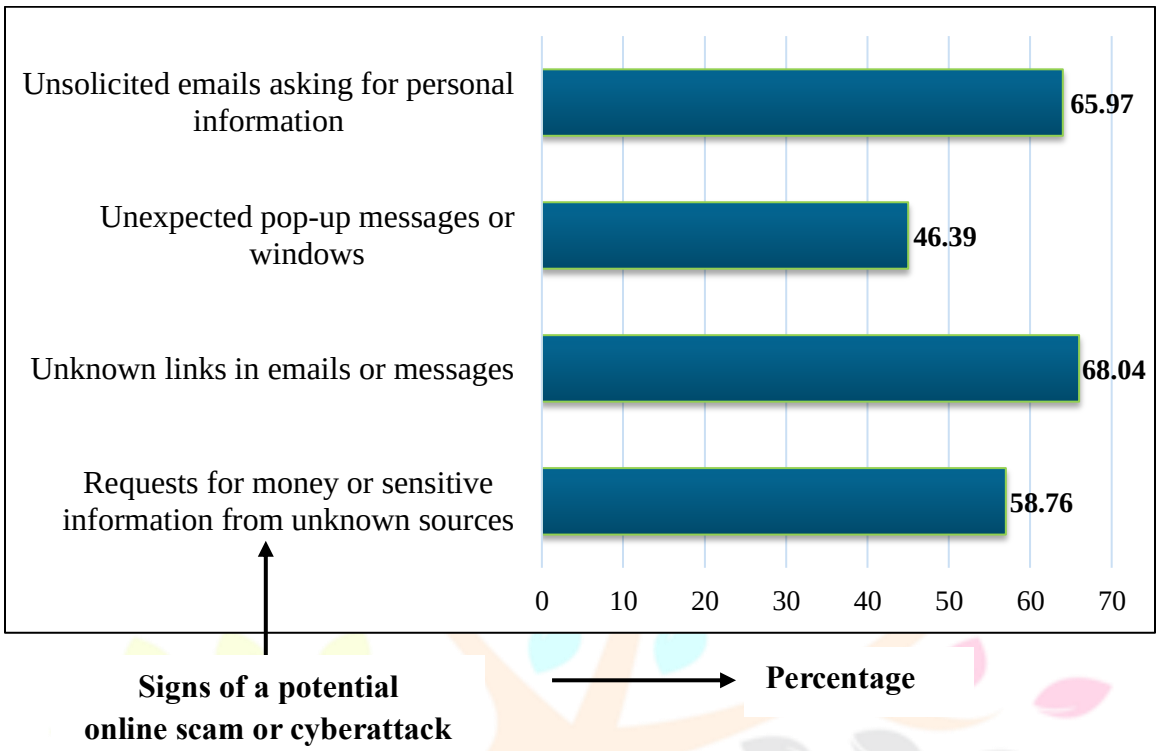
Table 2. Distribution of participants based on their general awareness and knowledge about cyber safety and security

Variables	Frequency (N)	Proportion (%)
Prior knowledge of Cyber Safety and Security		
Yes	79	81.4
No	18	18.6
Total	**97**	**100.0**
Ever attended any workshops, seminars or lecture on cyber safety and security		
Yes	70	72.2
No	27	27.8
Total	**97**	**100.0**
Having knowledge about personal information that is considered sensitive online (e.g., passwords, addresses, etc.)		
Yes	56	57.7
No	31	32.0
Not sure	10	10.3
Total	**97**	**100.0**
Ability to identify common online threats such as phishing, malware, and social engineering		
Yes	56	57.7
No	31	32.0
Not sure	10	10.3
Total	**97**	**100.0**
Awareness about the importance of regularly updating your software and applications for security reasons		
Yes	90	92.8
No	05	05.2
Not sure	02	02.1
Total	**97**	**100.0**

The data on common signs of potential online scams or cyberattacks among the participants reveals varying levels of awareness regarding different types of cyber threats. A substantial majority (68.04%) recognize unknown links in emails or messages as a significant warning sign, indicating a high level of vigilance against phishing attempts. Similarly, unsolicited emails asking for personal information are identified by 65.97% of participants, reflecting a strong awareness of this common tactic used by cybercriminals.

However, fewer participants are aware of other indicators. For instance, unexpected pop-up messages or windows are recognized by only 46.39% of participants, suggesting that nearly half may not fully understand the risks associated with malicious pop-ups, which can lead to malware infections or phishing sites. Requests for money or sensitive information from unknown sources are identified as a red flag by 58.76% of participants, showing a moderate level of awareness regarding this common scam tactic (Figure 1).

Figure 1. Common signs of a potential online scam or cyberattack



Cybersecurity Practices

Participants demonstrated good password practices, but many still reuse passwords or store them insecurely. Device security practices are mixed, with 32% of participants not using antivirus software and 19.6% not regularly updating their devices. Internet usage revealed a diverse range of activities, but there are privacy concerns with significant portions still sharing personal information online (Table 3).

Table 3. Distribution of participants based on device security practices

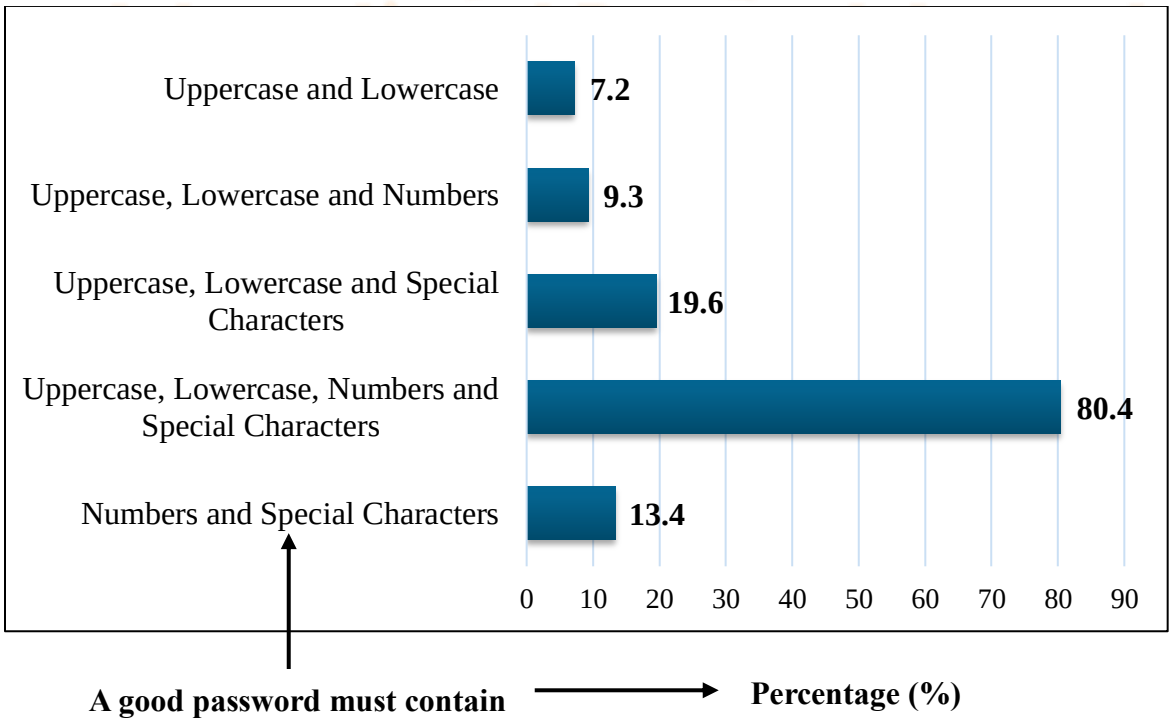
Variables	Frequency (N)	Proportion (%)
Have you installed antivirus software on your devices?		
Yes	66	68.0
No	31	32.0
Total	**97**	**100.0**
Do you have a password, PIN, or biometric protection (such as fingerprint or facial recognition) enabled on your smartphone or laptop?		
Yes	89	91.8
No	08	08.2
Total	**97**	**100.0**

Do you regularly update your devices and software?		
Yes	78	80.4
No	19	19.6
Total	**97**	**100.0**

The data on participants' understanding of the components of a good password reveals varying levels of awareness regarding strong password practices. The majority (80.4%) correctly identify that a good password must include uppercase letters, lowercase letters, numbers, and special characters. This comprehensive approach reflects a high level of awareness about creating strong, secure passwords that are difficult to guess or crack.

However, there are notable gaps in understanding among the remaining participants. A smaller proportion (19.6%) believe that a good password needs only uppercase, lowercase, and special characters, omitting numbers. This is less secure, as including numbers adds another layer of complexity. Similarly, 13.4% of participants think that only numbers and special characters are necessary, which overlooks the importance of using a mix of letter cases to enhance security. Some participants (9.3%) believe that a combination of uppercase, lowercase, and numbers suffices without special characters, while 7.2% consider that merely using uppercase and lowercase letters is adequate. Both groups miss the critical importance of special characters in making passwords more resilient against brute-force attacks and other common hacking methods (Figure 2).

Figure 2. A good password must contain



Challenges and Risks

In the digital age, protecting personal privacy and sensitive information is more crucial than ever. With the widespread use of the internet for daily activities—ranging from social interactions to financial transactions—individuals must take proactive measures to safeguard their online presence. Managing privacy settings across various platforms is one of the primary steps to achieving this. By carefully configuring these settings, individuals can ensure that sensitive information is only visible to trusted connections, reducing the risk of unauthorized access. Social media platforms, in particular, are common targets for cybercriminals, as people often unknowingly expose personal details that could be exploited. Ensuring that these settings are optimized to limit access can significantly enhance one's digital safety. However, while many people are cautious when it comes to social media and general privacy settings, there is still a considerable gap in overall cybersecurity practices.

Over 55% of participants continue to use unsecured public Wi-Fi networks without the added protection of a VPN, leaving their data vulnerable to cyberattacks. Public Wi-Fi networks, though convenient, are notorious for their lack of encryption, making them a hotspot for cybercriminals seeking to intercept data. Phishing attacks, another major cybersecurity threat, remain a persistent issue. Although there is a moderate level of awareness regarding phishing—scams where attackers disguise themselves as legitimate entities to steal personal information nearly 30% of individuals have still fallen victim to these attempts. Phishing can take various forms, such as deceptive emails, fake websites, or fraudulent phone calls, all designed to trick users into providing sensitive information or downloading malicious software. This underscores the importance of maintaining vigilance and adopting secure online practices to mitigate potential threats (Table 4).

Table 4. Distribution of participants based on secure internet practices

Variables	Frequency (N)	Proportion (%)
Do you know about virtual private networks (VPNs)?		
Yes, I am familiar with VPNs and use them regularly	30	30.9
Yes, I have heard of VPNs but do not use them regularly.	39	40.2
No, I am not familiar with VPNs.	28	28.9
Total	**97**	**100.0**
When using public Wi-Fi, do you use a virtual private network (VPN) for added security?		
Yes, always	17	17.5
Yes, sometimes	24	24.7
No, I do not use a VPN on public Wi-Fi	56	57.7
Total	**97**	**100.0**

Which of the following best describes your understanding of the term "phishing"?		
I am familiar with the term and understand its meaning.	52	53.6
I have heard of the term but do not fully understand its meaning.	39	40.2
I am not familiar with the term.	06	06.2
Total	**97**	**100.0**
Have you ever fallen victim to a phishing attempt (e.g., clicking on a suspicious link or providing personal information to a fake website)?		
Yes	29	29.9
No	68	70.1
Total	**97**	**100.0**

DISCUSSION

The study's demographic analysis shows that the participants are mostly young, educated, and from urban backgrounds. The youthfulness of the sample may influence the study outcomes, particularly in areas related to technology adoption, educational pursuits, and lifestyle choices, as younger individuals are generally more adaptable to new technologies and innovations (Venkatesh et al., 2003). The urban participants are likely to have better access to educational facilities and technological infrastructure compared to their rural counterparts. This disparity can influence the study's findings, particularly regarding access to and familiarity with technology and educational resources (Hilbert, 2016). A significant majority (81.4%) of the participants claim to have prior knowledge of cyber safety and security. This indicates a substantial base level of awareness, which is encouraging given the increasing importance of cybersecurity in both personal and professional contexts (Jones & Heinrichs, 2012). The high awareness level can be attributed to the integration of these topics into the D.El.Ed. curriculum, which ensures that pre-service teacher trainees are exposed to essential concepts in cybersecurity (National Council for Teacher Education, 2014). The data reveals that 72.2% of the participants have attended workshops, seminars, or lectures on cyber safety and security. These educational interventions play a crucial role in enhancing understanding and staying updated with the latest developments in cybersecurity (Bada, Sasse, & Nurse, 2019). Such proactive engagement in cybersecurity education suggests that the participants are committed to improving their knowledge and skills, which is vital for their future roles as educators. Despite the high levels of general awareness and participation in educational programs, there is a noticeable gap in understanding what constitutes sensitive personal information online. Only 57.7% of participants claim knowledge of recognizing sensitive data such as credit card details, bank account details, passwords, mobile numbers, OTPs, and addresses. This gap is concerning because recognizing and protecting sensitive information is fundamental to maintaining personal and organizational security (Herath & Rao, 2009).

CONCLUSION

The findings align with existing research that suggests younger individuals are generally more adaptable to technological changes, but they still require more rigorous training on cybersecurity nuances. The study advocates for integrating comprehensive cyber safety modules in teacher training programs to better equip future educators. The research concludes that while pre-service teacher trainees possess a basic awareness of cyber safety, significant vulnerabilities remain due to inconsistent practices and incomplete knowledge. Future educational efforts should focus on bridging these gaps through targeted workshops and practical training. The study provides a foundation for future research in enhancing cybersecurity awareness and resilience in educational settings.

RECOMMENDATIONS

- **Develop Comprehensive Cybersecurity Modules:** Teacher education programs should integrate detailed modules covering the latest cybersecurity threats, practices, and tools.
- **Regularly Update Training Content:** As digital threats evolve; the curriculum should be regularly updated to reflect new challenges and best practices.
- **Promote Practical Cybersecurity Tools:** Encourage the use of tools like VPNs, password managers, and multi-factor authentication as part of regular digital hygiene.
- **Conduct Regular Workshops and Seminars:** Organizing frequent educational events can help reinforce key cybersecurity concepts and keep trainees informed about new risks.

REFERENCES

1. National Education Policy 2020. Ministry of Human Resource Development, Government of India.
2. Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. MIS Quarterly, 27(3), 425-478.
3. Hilbert, M. (2016). The bad news is that the digital access divide is here to stay: Domestically installed bandwidths among 172 countries for 1986–2014. Telecommunications Policy, 40(6), 567-581.
4. Jones, K. S., & Heinrichs, L. R. (2012). Social networking and E-commerce: The emergence of Facebook as a channel for personal commercial transactions. Business Horizons, 55(2), 141-151.
5. National Council for Teacher Education. (2014). Teacher education curriculum framework. Retrieved from https://www.ncte-india.org
6. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour? arXiv preprint arXiv:1901.02672.
7. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.
8. National Council for Teacher Education (NCTE). (2020). Diploma in Elementary Education (D.El.Ed.) Program Guidelines. Retrieved from https://ncte.gov.in/Website/D.El.Ed.aspx