INTERNATIONAL RESEARCH JOURNAL OF HUMANITIES AND INTERDISCIPLINARY STUDIES
(Peer-reviewed, Refereed, Indexed & Open Access Journal)
DOI : 03.2021-11278686 ISSN : 2582-8568 IMPACT FACTOR : 8.031 (SJIF 2025)

Cybersecurity Knowledge and Behavioural Practices of Pre-Service Teachers: A Quantitative Study

Dr. (Prof.) Vinod Kumar Kanvaria
Professor,
Department of Education,
University of Delhi,
New Delhi, India.
E-mail: vinodpr111@gmail.com

Surabhi Verma
M.Ed. Student,
Department of Education,
University of Delhi,
New Delhi, India.
E-mail: verma.surabhi22@gmail.com

DOI No. 03.2021-11278686 **DOI Link ::** https://doi-ds.org/doilink/12.2025-41479551/IRJHIS2512012

Abstract:

This study examined the levels of cybersecurity knowledge and behaviour among 50 pre-service teachers. A structured questionnaire was used to assess their understanding of common cyber risks and the extent to which they follow safe online practices. The findings showed that while many participants demonstrated moderate to high cybersecurity knowledge, their actual behaviour online was less consistent. A noticeable gap emerged between what they knew and what they practiced, indicating that awareness alone does not automatically lead to safe digital habits. Overall, the study highlights the importance of strengthening practical cybersecurity training within teacher education programmes to better prepare future teachers to navigate and promote digital safety in educational settings.

Keywords: *Cybersecurity, Pre-service teachers, Knowledge–behaviour gap, Cyber safety education, Teacher training*

Introduction to Cybersecurity in Education:

The widespread integration of digital technology into global education systems has fundamentally transformed traditional learning environments, introducing new pedagogical possibilities alongside significant vulnerabilities (Rathnabai, 2023). Cybersecurity, defined broadly as "how individuals and organisations reduce the risk of cyber attacks," has become a critical concern for educational integrity and safety (Tiwari & Dhiman, 2025). Online safety, which refers to protecting individuals while they are engaging with computing systems, is often considered a component of the broader concept of cyber security.

Educational institutions are increasingly targeted by cyber threats such as phishing attempts, ransomware events, data breaches, and malicious software. Globally, the education sector is ranked

among the most vulnerable industries due to poor security infrastructures and user unawareness. Given that teachers are at the forefront of this digital shift, they urgently need to be prepared to handle these difficulties and safeguard their pupils' online settings (Rathnabai, 2023). The impacts of inadequate cybersecurity are estimated to have cost the global economy USD 945 billion in 2020 (Cremer et al., 2022).

Importance of Cybersecurity Competencies for Pre-Service Teachers:

Teachers today serve a multifaceted role, functioning as digital gatekeepers, facilitators, and role models whose digital practices significantly influence student behavior (Tiwari & Dhiman, 2025). They are essential agents in fostering a cyber security culture within educational institutions (Tiwari & Dhiman, 2025).

The necessity of integrating cyber security awareness into teacher training programmes is considered a matter of educational policy and public safety. Teachers need sufficient training to:

- **Protect Personal and Student Data:** Educators are responsible for handling sensitive information (grades, personal details) and must comprehend the importance of preventing unauthorized access (Sridevi. 2020).
- **Prevent Cyber Threats:** Teachers need to be aware of prevalent cyber dangers like ransomware, malware, and phishing attacks to take preventative measures (Rathnabai, 2023).
- **Ensure a Reliable Learning Environment:** Training helps teachers protect digital classrooms and instructional materials from disruptions caused by cyberattacks (Rathnabai, 2023).

Regrettably, both in-service and pre-service teachers (PSTs) are often found to be unprepared to teach students about cyber security and safety (Santhosh & Thiyagu, 2024). When educators lack this knowledge, they risk inadvertently transmitting risky behaviour to their students, creating a cascading exposure effect throughout educational communities. Preparing PSTs to teach cyber security is a daunting task, partially due to the already demanding coursework required in traditional teacher preparation programmes (Navarrete, 2023).

Research Questions:

- What is the overall level of cybersecurity knowledge among pre-service teachers?
- To what extent do pre-service teachers demonstrate safe cybersecurity behaviours and practices?
- Is there a gap between pre-service teachers' self-reported cybersecurity knowledge and their self-reported cybersecurity behaviour?

Research Objectives:

- To determine the overall level of cyber security knowledge among pre-service teachers
- To evaluate the prevalence of safe cyber security behaviours and practices among pre-service

teachers.

- To identify the Knowledge-Behaviour Gap by comparing the pre-service teachers' self-reported knowledge scores with their self-reported behaviour scores.

Theoretical Background:

The discourse on cyber security education often employs specific conceptual frameworks. The combination of cyber ethics, cyber safety, and cyber security is often referred to as the C3 framework (Sridevi. 2020). Cyber ethics encompasses the moral choices individuals make (e.g., copyright, online etiquette); Cyber safety involves actions taken to minimise encountered dangers (e.g., avoiding viruses, unwanted communications); and Cyber security involves technical interventions that protect data and hardware (e.g., antivirus, firewalls) (Sridevi. 2020).

Cyber security competency is defined as the combination of skills, knowledge, and attitude necessary for the confident, creative, and critical use of technologies for work, leisure, and communication (Santhosh &Thiyagu, 2024). The need for PSTs to possess skills and competencies for managing a safe digital environment and propagating this knowledge to students rests squarely on future educators (Santhosh & Thiyagu, 2024).

A common theoretical approach to understanding and measuring information security awareness is the Knowledge-Attitude-Behavior (KAB) model. Research based on the KAB model indicates that there are significant positive relationships between the components of knowledge, attitude, and behaviour concerning information security (Benzer & Karal, 2023). Improved knowledge is linked to improved attitudes, which should, in turn, lead to more appropriate secure actions.

Furthermore, Maslow's hierarchy of needs theory suggests that if individuals cannot meet the fundamental requirement of security (cyber security), they cannot fully satisfy higher needs such as education (Haseski, 2020). Therefore, the feeling of security in the virtual environment is thought to encourage a positive attitude towards computer-assisted education (Haseski, 2020).

Review of Related Literature:

Empirical studies conducted in schools and teacher education institutions globally reveal consistent patterns concerning awareness and practice:

Awareness Levels and Competencies:

Overall, the awareness levels of pre-service teachers on cyber security are often described as medium or moderate (Benzer & Karal, 2023). One study on secondary school teachers in Karnataka, India, found that the majority of participants (76.1%) possessed a medium level of awareness (Sridevi, 2020). Pre-service teachers surveyed in Nigeria claimed to have basic cyber security knowledge but were unaware of how to protect their data (Rathnabai, 2023).

In terms of specific competencies, PSTs tend to exhibit higher scores in actively avoiding the

untrusted and protecting payment information, reflecting their security priorities in common online activities(Haseski, 2020). However, competencies related to "leaving no trace," personal privacy, and precaution have been identified as relatively low (Haseski, 2020). A qualitative analysis of in-service teachers found that while they were aware of certain security aspects (e.g., safe websites), they were not applying this knowledge in their daily utility (Sridevi, 2020).

The Gap between Cybersecurity Knowledge and Actual Secure Behaviour:

A prominent finding across the literature is the significant gap between possessing cybersecurity knowledge and engaging in actual secure behaviour, sometimes referred to as cognitive dissonance (Rathnabai, 2023).

- A study examining proactive cyber security behaviour among PSTs found that they exhibited a lack of best practices in Information Assurance no different from general computer end-users (Agamba & Keengwe, 2014).
- While 69.6% of teachers in one survey knew how to create secure passwords, 37% responded that they *always* use the same password for multiple accounts, indicating a disconnect between knowledge and practice (Sridevi, 2020).
- Some research, using the KAB model, noted that male participants recorded higher knowledge scores but did not follow through with commensurately high scores in the behaviour dimension, which may be attributed to a tendency to take more risks (Benzer & Karal, 2023).

Empirical Findings on Demographics:

Studies examining demographic differences yield mixed results:

- Some research indicates that there is no significant difference in cyber security awareness between male and female teachers (Rathnabai, 2023).
- However, other studies found that males' awareness scores were significantly higher than females' when considering the overall scale (Benzer & Karal, 2023).
- Awareness levels among secondary school teachers were found to differ with respect to age, though subsequent pair-wise comparison of mean scores did not show a significant difference between individual age groups (Sridevi, 2020).
- PSTs majoring in Computer Education and Instructional Technology demonstrated a higher level of awareness compared to candidates in other disciplines, possibly due to their specialized curriculum (Benzer & Karal, 2023).

Methodology:

This study employed a descriptive survey design to examine cybersecurity knowledge and behaviour among pre-service teachers. Such a design is appropriate when the researcher intends to collect quantitative data using a structured instrument and to describe trends within a

population.Creswell (2014) notes that survey designs are useful for obtaining numeric descriptions of attitudes, opinions or behaviours of a sample and for generalizing findings to a population.

Description of the Sample:

The sample for the study consisted of 50 pre-service teachers enrolled in teacher education programmes. Of these, 33 were Bachelor of Education (B.Ed) trainees and 17 were Diploma in Elementary Education (D.El.Ed) trainees. All participants in the sample were female pre-service teachers.

Regarding prior exposure to cyber safety education, 24 participants reported that they had received some form of training in cybersecurity, while 26 participants indicated that they had not undergone any such training.

Tool:

A structured questionnaire was used to collect data for the study. The tool consisted of 28 items covering basic areas of cybersecurity knowledge and behaviour. The questionnaire was adapted from the study "A Study on the Effectiveness of Cyber Safety and Security Awareness Package for Teachers" by Dr. Angel Rathnabai, and the language of the items was simplified to suit pre-service teachers. The items were organised as knowledge and behaviour questions, and responses were recorded on a three-point scale (Yes / Sometimes / No).

Data Analysis and Interpretation:

Table 1: Findings on Knowledge of pre- teachers on Cyber security

N	Low Knowledge (< 0.50)	Medium Knowledge (0.50–0.74)	High Knowledge (≥ 0.75)
50	(5) 10%	(20) 40%	(25) 50%

Overall, the sample shows moderate-to-good cybersecurity knowledge: half of the respondents fall in the High category and a further 40% in Medium, leaving only 10% in Low.

Table 2: Findings on prevalence of safe cybersecurity behaviours and practices among pre-service teachers

N	Low Behaviour (< 0.50)	Medium Behaviour (0.50–0.74)	High Behaviour (≥ 0.75)
50	(2) 4%	(26) 52%	(22) 44%

The findings indicate that nearly half of the pre-service teachers (44%) exhibit strong and consistent cybersecurity practices, reflecting a relatively high level of behavioural preparedness. However, the fact that over half (52%) fall within the medium range suggests that many behaviours are practiced inconsistently or with uncertainty. Only 4% (2 teachers) demonstrated low levels of cybersecurity behaviour, indicating minimal adherence to recommended safety practices.

Table 3: Findings on Knowledge–Behaviour Gap

Level	Knowledge	Behaviour	Gap
High	50% (n=25)	44% (n=22)	–6%
Medium	40% (n=20)	52% (n=26)	+12%
Low	10% (n=5)	4% (n=2)	–6%

The comparison between pre-service teachers' cybersecurity knowledge levels and their actual cybersecurity behaviours reveal a clear and measurable gap. While 50% of the respondents demonstrated high knowledge, only 44% translated that understanding into high levels of safe cybersecurity behaviour. This 6% shortfall indicates that a portion of knowledgeable pre-service teachers do not consistently apply safe practices in real contexts.

Similarly, the proportion of pre-service teachers in the medium category shows a notable shift: 40% had medium knowledge, but 52% exhibited medium behaviour. This 12% increase suggests that some individuals with partial or limited knowledge are still engaging in moderately safe behaviours, possibly due to habitual digital routines, device defaults, or external guidance rather than conscious application of cybersecurity principles.

At the lower end, 10% of participants had low cybersecurity knowledge, whereas only 4% displayed low-level behaviour. This indicates that low knowledge does not necessarily lead to unsafe behaviour, as many basic security practices may be followed unintentionally or automatically (e.g., built-in security settings, common-sense precautions).

Overall, the results show that knowledge does not correspond perfectly with behaviour. In general, pre-service teachers' cybersecurity knowledge is higher than their demonstrated behavioural practices. This mismatch reflects a knowledge–behaviour gap, where understanding cybersecurity concepts does not consistently translate into action. These findings highlight the need for more practice-oriented training, behavioural reinforcement, and experiential learning to help pre-service teachers convert their cybersecurity knowledge into stable, everyday digital practices.

Findings and Discussion:

The findings show that pre-service teachers in this study demonstrated moderate to high levels of cybersecurity knowledge, which aligns with earlier research reporting similar awareness patterns among teacher trainees (Rathnabai, 2023; Benzer & Karal, 2023). However, as consistently noted in previous studies, knowledge did not fully translate into practice. Although 50% of participants had high knowledge, only 44% showed high cybersecurity behaviour, confirming the knowledge–behaviour gap highlighted by Rathnabai (2023) and Sridevi (2020).

The majority of participants fell into the medium behaviour category, indicating that safe online practices are followed inconsistently. This supports the observations of Agamba and Keengwe

(2014) and Haseski (2020), who found that teachers and pre-service teachers often perform certain behaviours unintentionally or rely on built-in digital safeguards rather than deliberate action.

The pattern also reflects the KAB model (Knowledge–Attitude–Behaviour), where behaviour is influenced by multiple factors beyond knowledge alone (Benzer & Karal, 2023). Even participants with medium knowledge displayed moderate behaviour, suggesting that environmental factors or general caution may influence their practices..

Overall, the findings reinforce what earlier research has emphasized: teacher education programmes must move beyond theoretical awareness and provide more practical, hands-on cybersecurity training (Navarrete, 2023; Tiwari & Dhiman, 2025). Strengthening behavioural competencies is essential if future teachers are expected not only to understand cybersecurity but to model safe digital habits for their students.

Limitations:

- The study had a small sample of 50 pre-service teachers, all female, limiting generalisability and preventing gender comparisons.
- Convenience sampling was used, which may have introduced selection bias.
- Data were self-reported, so participants might have misjudged their own knowledge or behaviour.
- The adapted questionnaire might not fully capture the complete range of cybersecurity competence.
- The study examined only knowledge and behaviour, ignoring attitudes, motivation, and other influencing factors

Conclusion

The study showed that pre-service teachers possess moderate to high levels of cybersecurity knowledge, but their actual online behaviour does not fully match what they know. This confirms a clear knowledge–behaviour gap, similar to patterns reported in earlier research. While trainees understand key cyber safety concepts, their practices are often inconsistent. These findings highlight the need for teacher education programmes to strengthen practical, hands-on cybersecurity training so that future teachers not only understand digital safety but can also model safe behaviour for their students.

References:

1. Agamba, J., & Keengwe, J. (2014). Pre-service teachers' perceptions of information assurance and cyber security. *International Journal of Information and Communication Technology Education, 8*(2), 94–101. https://doi.org/10.4018/jicte.2012040108
2. Benzer, A. İ., & Karal, Y. (2023). Pre-service teachers' information security awareness: An analysis based on the knowledge–attitude–behavior model. *Educational Academic Research,*

(49), 10–22. https://doi.org/10.5152/AUJKKEF.2023.1034562

3. Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance: Issues and Practice, 47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6
4. Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Sage.
5. Damenu, T., Gökbay, İ., Covaci, A., & Li, S. (2025). Cyber security educational games for children: A systematic literature review. *arXiv*. https://doi.org/10.48550/arXiv.2508.17414
6. Haseski, H. İ. (2020). Cyber security skills of pre-service teachers as a factor in computer-assisted education. *International Journal of Research in Education and Science, 6*(3), 484–500.
7. Navarrete, C. (2023). Preparing preservice teachers to teach cyber security education: Examining theoretical approaches. In *ICERI2023 Proceedings* (pp. 2215–2221). IATED. https://doi.org/10.21125/iceri.2023.0616
8. Rathnabai, A. (2023). *A study on the effectiveness of cyber safety and security awareness package for teachers* (Research report). Central Institute of Educational Technology, National Council of Educational Research and Training.
9. Santhosh, T., & Thiyagu, K. (2024). Development and validation of cyber security competency scale for prospective teachers. *Journal of Pedagogical Sociology and Psychology, 6*(3). https://doi.org/10.33902/jpsp.202428783
10. Sridevi, K. V. (2020). *Cyber security awareness among in-service secondary school teachers of Karnataka*. Department of Curriculum Studies, NCERT.
11. Tiwari, P. K., & Dhiman, V. (2025). Integrating cybersecurity awareness into teacher training programs: A new frontier in educational policy. *International Journal of Research Publication and Reviews, 6*(5), 6246–6253. https://doi.org/10.55248/gengpi.6.0525.1781