



ROLE OF TEACHER EDUCATION PROGRAMS IN ENHANCING CYBERSECURITY AWARENESS AMONG PROSPECTIVE TEACHERS: A SYSTEMATIC LITERATURE REVIEW

***Ved Prakash Sharma**

Research Scholar

Department of Education

Shri Venkateshwara University, Gajraula (U.P.)

****Dr. Vinita M. Chaudhary**

Associate Professor

Department of Education

Shri Venkateshwara University, Gajraula (U.P.)

1. Abstract

In the contemporary digital era, education systems across the world are undergoing a profound transformation driven by rapid advancements in information and communication technologies (ICT). This digital shift has significantly increased the dependency of educational institutions on online platforms, digital tools, and cloud-based learning environments. While this transformation has improved access to education and pedagogical efficiency, it has simultaneously exposed educators and learners to a wide range of cybersecurity threats such as phishing attacks, identity theft, ransomware, data breaches, and social engineering techniques. Teacher education programs, which are responsible for preparing prospective teachers, play a crucial role in equipping future educators with both pedagogical and digital competencies. However, cybersecurity awareness remains an underdeveloped area within most teacher training curricula. This systematic literature review (2020–2026) explores the role of teacher education programs in enhancing cybersecurity awareness among prospective teachers. The study synthesizes findings from peer-reviewed journals, international databases, and academic publications. The review reveals that while digital literacy is widely emphasized in teacher education, cybersecurity education is still inconsistently integrated. The findings indicate moderate levels of cybersecurity awareness among prospective teachers, with significant gaps in practical knowledge and behavioral application. The study also identifies that experiential learning methods such as simulations, workshops, and hands-on training significantly improve cybersecurity awareness. However, institutional limitations, lack of standardized curriculum, and insufficient policy implementation hinder effective integration. The paper concludes that cybersecurity must be embedded as a core competency within teacher education programs to ensure a digitally safe educational ecosystem.

Key Words: Education Systems, ICT, Cybersecurity & Digital Literacy



2. Introduction

The 21st century has witnessed a dramatic transformation in the field of education due to the rapid development of digital technologies. The integration of ICT tools such as online learning platforms, artificial intelligence-based educational systems, virtual classrooms, and mobile learning applications has reshaped traditional teaching-learning methodologies. This transformation has been further accelerated by global events such as the COVID-19 pandemic, which forced educational institutions to shift towards online and hybrid learning models.

Despite the numerous advantages of digital education, the increased reliance on technology has also introduced serious cybersecurity challenges. Educational institutions have become frequent targets of cyberattacks, including unauthorized data access, phishing scams, ransomware attacks, and misuse of personal information. These risks are not limited to institutions alone but extend to teachers and students who actively engage in digital platforms.

Teacher education programs are designed to prepare prospective teachers for professional roles in educational settings. In the digital age, their responsibilities extend beyond pedagogy to include safe and responsible use of technology. Teachers are expected to guide students not only in academic learning but also in digital citizenship and cybersecurity awareness.

However, existing literature suggests that cybersecurity is not yet fully integrated into teacher education curricula. Most programs focus primarily on ICT skills such as presentations, online communication, and content creation, while neglecting critical aspects of digital safety. This gap poses a serious challenge, as teachers without adequate cybersecurity knowledge may unintentionally expose themselves and their students to cyber risks.

Therefore, there is a strong need to systematically analyze existing research to understand how teacher education programs are addressing cybersecurity awareness and what improvements are necessary.

3. Objectives of the Study

The present systematic literature review is guided by the following detailed objectives:

1. To critically analyze the role of teacher education programs in developing cybersecurity awareness among prospective teachers.



- 2.To examine global and Indian research studies (2020–2026) related to cybersecurity education in teacher training institutions.
- 3.To identify the level of cybersecurity knowledge, attitudes, and practices among teacher trainees.
- 4.To explore the effectiveness of different pedagogical approaches used in cybersecurity education.
- 5.To investigate institutional, curricular, and policy-level gaps in integrating cybersecurity education.
- 6.To provide evidence-based recommendations for strengthening cybersecurity integration in teacher education programs.

METHODOLOGY

4.1 Research Design

The present study is based on a Systematic Literature Review (SLR) design, which is widely recognized as one of the most structured and reliable methods for synthesizing existing research. This design focuses on collecting, analyzing, and interpreting previously published studies to derive meaningful conclusions. Unlike primary research, this approach does not involve direct data collection from respondents but relies on secondary sources of information. The SLR method is particularly useful in identifying trends, patterns, and research gaps in a specific field. In this study, the SLR approach helps in understanding how cybersecurity awareness has been addressed in teacher education programs between 2020 and 2026. It also allows for a comprehensive comparison of findings from different geographical and institutional contexts. The systematic nature of this design ensures transparency, replicability, and academic rigor.

4.2 Data Sources

The data for this study was collected from multiple reputed academic databases to ensure reliability and authenticity of information. Major sources include Google Scholar, ResearchGate, IEEE Xplore, SpringerLink, and ERIC (Education Resources Information Center). These databases were selected because they provide access to peer-reviewed journals, conference papers, and academic publications related to education and cybersecurity. In addition, Scopus-indexed journals were also referred to wherever accessible. The selection of multiple databases ensures a broad and diverse range of studies covering both Indian and international contexts. This helps in achieving a balanced understanding of cybersecurity awareness in teacher education programs. Only those studies that met academic quality standards were included in the review process.



4.3 Time Frame of the Study

The time frame selected for this systematic review is from 2020 to 2026. This period is considered highly relevant because it represents the post-pandemic digital education era, during which the use of online learning platforms increased significantly. The COVID-19 pandemic acted as a catalyst for digital transformation in education, making cybersecurity an essential concern. By selecting this time frame, the study ensures that only recent and updated research findings are included. This helps in understanding current trends, challenges, and developments in cybersecurity awareness among teacher trainees. Studies prior to 2020 were excluded to maintain relevance to modern digital learning environments. The selected period also reflects the latest policy changes and technological advancements in education.

4.4 Inclusion Criteria

The inclusion criteria were carefully defined to ensure that only relevant and high-quality studies were selected for analysis. First, only studies focusing on teacher education, teacher trainees, or prospective teachers were included. Second, research papers related to cybersecurity awareness, cyber hygiene, digital safety, and cybercrime education were considered. Third, only peer-reviewed journal articles and conference papers published between 2020 and 2026 were selected. Fourth, studies written in the English language were included to maintain consistency in analysis. Additionally, studies that provided empirical findings, literature reviews, or systematic reviews were prioritized. This strict inclusion process ensured that the data used in the study was academically valid, reliable, and relevant to the research objectives.

4.5 Exclusion Criteria

To maintain the quality and focus of the study, certain exclusion criteria were applied. Studies that were not related to education or teacher training were excluded from the review. Opinion-based articles, blog posts, and non-peer-reviewed sources were also excluded due to lack of academic reliability. Duplicate publications across multiple databases were removed to avoid redundancy. Studies that did not specifically address cybersecurity awareness or digital safety were not considered. Additionally, research papers published before 2020 were excluded to ensure that only recent and updated literature was analyzed. Articles that lacked full-text availability or sufficient methodological clarity were also omitted. This exclusion process helped in refining the dataset and improving the accuracy of findings.



4.6 Data Analysis Technique

The collected data was analyzed using thematic analysis, which is a widely used qualitative method for identifying patterns and themes within textual data. In this study, the selected research papers were carefully reviewed and categorized into different themes such as cybersecurity awareness levels, training effectiveness, institutional role, digital behavior, and curriculum integration. Each theme was analyzed in detail to understand recurring patterns and differences across studies. Thematic analysis helps in organizing large volumes of qualitative data into meaningful categories, making interpretation easier and more structured. This method also allows comparison between different studies and identification of common research gaps. The findings derived through thematic analysis provide a comprehensive understanding of the current state of cybersecurity awareness in teacher education programs.

5. REVIEW OF LITERATURE

5.1 Cybersecurity Awareness among Prospective Teachers

Cybersecurity awareness refers to the understanding of digital threats, safe online behavior, and preventive measures against cyber risks. Recent studies (2020–2026) indicate that prospective teachers generally possess a moderate level of awareness regarding basic cyber issues such as password protection, safe browsing, and identification of suspicious links. However, their understanding of advanced threats like ransomware attacks, phishing techniques, identity theft, and social engineering remains limited. Research further suggests that awareness is often theoretical rather than practical. Many teacher trainees are aware of cyber risks but do not consistently apply safety measures in real-life digital environments. This gap between knowledge and behavior highlights the need for structured cybersecurity training in teacher education programs. Scholars also emphasize that awareness increases significantly when learners are exposed to real-life case studies and interactive learning environments. Therefore, cybersecurity awareness is not only a knowledge issue but also a behavioral competency that needs continuous development.

5.2 Role of Teacher Education Programs in Cybersecurity Development

Teacher education programs are designed to prepare future educators with essential pedagogical, psychological, and professional competencies. In the context of digital education, these programs are expected to include ICT-based training. However, studies show that cybersecurity is still not a core component of most curricula. Instead, emphasis is placed on basic computer skills such as MS Office, presentation tools, and online communication platforms. Recent literature highlights that when cybersecurity modules



are included, they are often optional or theoretical in nature. This reduces their effectiveness in developing practical skills among trainees. Researchers argue that teacher education programs must evolve to include structured cybersecurity training modules that focus on real-world digital threats and preventive strategies. Without this integration, future teachers may remain digitally skilled but not digitally safe, which can have serious implications for classroom environments.

5.3 Impact of Digital Transformation and Post-COVID Education Shift

The COVID-19 pandemic played a major role in accelerating digital transformation in education systems worldwide. Schools and colleges rapidly adopted online teaching platforms such as Zoom, Google Classroom, and Microsoft Teams. While this shift ensured continuity of education, it also exposed teachers and students to various cybersecurity vulnerabilities. Many educators had to adopt digital tools without adequate training in cyber safety practices. Studies conducted after 2020 reveal that cyber incidents such as phishing emails, fake links, and data misuse increased significantly during this period. Teacher trainees, in particular, faced challenges in managing digital platforms securely. The sudden transition highlighted the lack of preparedness in teacher education programs regarding cybersecurity awareness. Researchers conclude that post-COVID education has made cybersecurity an essential component of teacher training rather than an optional skill.

5.4 Digital Competency Frameworks and Cybersecurity Integration

Digital competency frameworks such as DigCompEdu and similar international models aim to define the essential digital skills required for educators. These frameworks typically include areas such as professional engagement, digital resources, teaching and learning, assessment, and learner empowerment. However, cybersecurity is often included as a minor sub-component rather than a standalone competency. Recent studies suggest that this limited inclusion leads to insufficient attention to digital safety in teacher education. Scholars argue that cybersecurity should be treated as a core digital competency because it directly affects all other areas of digital education. Without strong cybersecurity awareness, teachers may unknowingly compromise personal and institutional data. Therefore, researchers recommend restructuring digital competency frameworks to give equal importance to cybersecurity alongside other digital skills.

5.5 Effectiveness of Training Methods in Cybersecurity Education

The effectiveness of cybersecurity education largely depends on the teaching methods used in teacher education programs. Traditional lecture-based approaches have been found to be less effective in developing practical cybersecurity skills. In contrast,



experiential learning methods such as simulations, role-playing exercises, cyber-attack demonstrations, and interactive workshops have shown significantly better outcomes. Studies indicate that when trainees are exposed to real-life scenarios, they develop stronger understanding and better decision-making abilities in digital environments. Simulation-based training helps learners recognize phishing attempts, unsafe websites, and suspicious digital behavior more effectively. Additionally, group discussions and case-study analysis enhance critical thinking skills. Researchers emphasize that cybersecurity education should be practice-oriented rather than theory-heavy to ensure meaningful learning outcomes.

5.6 Institutional Support and Policy Implementation

Institutional support plays a critical role in integrating cybersecurity education into teacher training programs. However, many teacher education institutions lack dedicated cybersecurity policies, trained faculty members, and structured curriculum frameworks. Studies reveal that in most institutions, cybersecurity topics are either briefly mentioned or completely absent from the syllabus. Even where ICT labs exist, they are primarily used for technical training rather than safety education. Policy-level frameworks such as NEP 2020 emphasize digital education but do not provide detailed guidelines for cybersecurity training implementation. Researchers highlight that without institutional commitment, cybersecurity awareness cannot be effectively developed among prospective teachers. Continuous professional development programs, faculty training, and curriculum reforms are essential for strengthening institutional capacity in this area.

6. DISCUSSION OF FINDINGS

The findings of this systematic literature review highlight several important aspects of cybersecurity awareness among prospective teachers and the role of teacher education programs. The discussion is based on studies conducted between 2020 and 2026, which collectively provide an understanding of current trends, gaps, and challenges in this area. Prospective teachers generally show a moderate level of cybersecurity awareness. They are familiar with basic concepts such as passwords, safe browsing, and avoiding suspicious links, but their understanding of advanced threats like phishing, ransomware, and identity theft is limited. Their awareness is mostly superficial and depends more on personal digital exposure than formal training provided in teacher education programs. There is also a clear gap between theoretical knowledge and practical application. Although trainees understand cybersecurity concepts in theory, they often fail to apply them in real-life digital situations. Safe practices such as using strong passwords and maintaining cautious online behavior are not consistently followed, indicating that current training focuses more on theory than practical skill development.



The findings further show that increased digital exposure slightly improves awareness but also increases vulnerability. Trainees who frequently use smartphones and online platforms are more exposed to cyber threats, but this does not necessarily mean they are better prepared to handle them. Thus, digital usage alone is not sufficient for cybersecurity competence.

Another important finding is the presence of regional and institutional differences. Urban institutions generally show higher levels of cybersecurity awareness compared to rural institutions due to better infrastructure, resources, and training facilities. Rural institutions face limitations such as lack of ICT infrastructure and trained faculty, which leads to unequal learning outcomes.

The review also highlights that experiential learning methods such as simulations, workshops, and case studies are more effective than traditional lecture-based teaching. These methods help improve understanding, retention, and practical application of cybersecurity concepts among trainees.

Finally, significant institutional and policy gaps are observed. Many teacher education institutions lack structured cybersecurity modules and trained faculty. Although NEP 2020 promotes digital education, it does not provide detailed cybersecurity guidelines, resulting in inconsistent implementation across institutions.

7. FINDINGS

7.1 Level of Cybersecurity Awareness

- Prospective teachers generally show a moderate level of cybersecurity awareness.
- Basic concepts like passwords, safe browsing, and suspicious links are known.
- Awareness about advanced threats like phishing, ransomware, and identity theft is limited.
- Switch Understanding is mostly theoretical rather than practical.
- Awareness depends more on personal digital exposure than formal training.

7.2 Absence of Structured Curriculum

- Mostly teacher education programs do not have a separate cybersecurity curriculum.
- ICT courses mainly focus on tools and software usage.
- Cyber safety and digital protection are not given sufficient importance.
- Lack of structured syllabus leads to uneven learning outcomes.
- Cybersecurity is treated as a secondary or optional topic.

7.3 Gap between Theory and Practice

- Trainees understand cybersecurity concepts but fail to apply them in real life.



- Safe practices like strong passwords are not consistently followed.
- Awareness of cyber threats does not always lead to safe behavior.
- There is a clear gap between knowledge and application.
- Behavioral change is weak despite theoretical understanding.

7.4 Effectiveness of Practical Training Methods

- Experiential learning methods are more effective than traditional lectures.
- Simulations, workshops, and real-life examples improve understanding.
- Practical training helps in better retention of concepts.
- Learners show improved cyber safety behavior after hands-on training.
- Interactive methods increase engagement and awareness.

7.5 Institutional and Regional Differences

- Urban institutions show higher awareness levels than rural institutions.
- Better ICT infrastructure supports improved learning in cities.
- Rural institutions face lack of resources and trained faculty.
- This creates unequal learning opportunities among trainees.
- Institutional support strongly influences cybersecurity awareness.

7.6 Digital Exposure vs Awareness

- High digital usage does not guarantee high cybersecurity awareness.
- Students frequently use smartphones and online platforms.
- However, they often ignore privacy and security risks.
- Increased exposure sometimes increases vulnerability.
- Proper training is missing despite high technology usage.

7.7 Need for Policy Integration

- NEP 2020 promotes digital education but lacks detailed cyber safety guidelines.
- Cybersecurity is not mandatory in most teacher education programs.
- There is no uniform implementation across institutions.
- Policy-level integration is necessary for consistency.
- Cybersecurity should be a core part of curriculum.

8. RESEARCH GAP

The systematic review of literature reveals several important research gaps in the area of cybersecurity awareness among prospective teachers. One of the most significant gaps is the lack of a standardized curriculum for cybersecurity education in teacher training programs. At present, most institutions include cybersecurity only as a small part of ICT



courses, without a structured framework. This leads to inconsistency in learning outcomes across different universities. As a result, teacher trainees do not receive uniform exposure to essential cybersecurity concepts such as phishing, ransomware, data privacy, and safe online behavior.

Another important gap is the limited availability of India-specific empirical studies. Most existing research is international, while Indian teacher education institutions remain under-researched, especially in rural and semi-urban areas. There is a lack of large-scale studies focusing on regional differences and infrastructural challenges. This makes it difficult to apply global findings directly to the Indian education system.

A further gap is the weak focus on behavioral aspects. Most studies focus on awareness and theoretical knowledge rather than actual digital behavior. Very few studies examine whether trainees apply cybersecurity practices in real life. This creates a gap between knowing and doing, which is a major limitation in current research.

In addition, there is an absence of continuous training programs. Cybersecurity education is mostly limited to one-time workshops, which are not enough for long-term awareness. Since cyber threats constantly evolve, continuous training is necessary but largely missing.

Finally, there is a lack of longitudinal studies that track awareness over time. Most research is cross-sectional and does not measure long-term impact, making it difficult to evaluate effectiveness properly.

9. CONCLUSION

The systematic literature review shows that cybersecurity awareness has become an essential requirement in modern education due to increasing digitalization. Teacher education programs play a crucial role in preparing future educators, but current programs focus mainly on basic digital literacy rather than cybersecurity.

Findings show that prospective teachers have moderate awareness of cybersecurity. They understand basic concepts like passwords and safe browsing but lack knowledge of advanced threats such as phishing, ransomware, and identity theft. Their awareness is mostly theoretical and not strongly reflected in practical behavior.

There is a clear gap between knowledge and practice. Even when trainees know about cyber safety, they do not consistently apply it in real-life situations. This shows that current teacher education programs do not adequately focus on practical training.

Institutional and curricular limitations also contribute to this issue. Cybersecurity is not systematically included in most programs, and there is a lack of trained faculty and structured modules. Urban institutions perform better than rural ones due to better infrastructure.



It can be concluded that cybersecurity must be integrated as a core part of teacher education programs to ensure digitally safe and responsible educators.

10. RECOMMENDATIONS

Cybersecurity should be made a compulsory part of the teacher education curriculum. It should not be optional or a small part of ICT courses but a structured subject with proper syllabus coverage.

Institutions should adopt practical teaching methods such as simulations, workshops, and real-life case studies. These methods are more effective than traditional lecture-based teaching.

Faculty training programs should be introduced so that teacher educators can properly teach cybersecurity concepts. Without trained teachers, effective implementation is not possible.

Continuous professional development programs should also be introduced because cyber threats change rapidly. One-time training is not enough for long-term awareness.

National policies like NEP 2020 should include detailed cybersecurity guidelines to ensure uniform implementation across all institutions.

REFERENCES

- Almohammad, A., & Abulibdeh, A. (2022). Cyber hygiene practices among educators. *Computers & Education Journal*, 176, 104–112.
- Beltrán, A., Jiménez, M., & López, S. (2023). Cybersecurity education methods: A systematic review. *International Journal of Digital Learning*, 12(1), 101–115.
- Gupta, V., & Agarwal, S. (2021). Online learning and cyber risks in education. *Education and Technology Studies*, 10(2), 56–70.
- Khan, M. A. (2020). Cybersecurity awareness in developing countries. *International Journal of Information Security*, 19(4), 233–245.
- Kumar, S., Gupta, R., & Sharma, P. (2021). Cybersecurity awareness among teacher trainees in higher education institutions. *Journal of Educational Technology Research*, 18(2), 45–58.
- National Education Policy. (2020). Ministry of Education, Government of India.
- OECD. (2021). Digital education and security frameworks. OECD Publishing.
- Patel, R., & Sharma, N. (2022). ICT and cybersecurity integration in education. *Journal of Modern Education Review*, 12(3), 120–130.
- Recent Google Scholar studies (2020–2026) on cybersecurity awareness in teacher education programs.
- Reddy, P., & Mishra, S. (2023). Digital literacy and cyber awareness in teacher education. *Indian Journal of Educational Research*, 44(1), 15–28.
- Sarker, I. H. (2021). Cybersecurity threats in educational environments. *Journal of Cybersecurity Studies*, 9(2), 77–89.



- Singh, A., &Verma, R. (2020). ICT integration in teacher education: Challenges and perspectives. *Journal of Teacher Education Research*, 15(3), 23–34.
- Torres-Hernández, N., &Gallego-Arrufat, M. J. (2022). Digital competence and cybersecurity in teacher education. *Education and Information Technologies*, 27(5), 6789–6805.
- UNESCO. (2021). Digital safety and cybersecurity in education systems. UNESCO Publishing.
- World Economic Forum. (2022). Global cybersecurity outlook in education sector. WEF Report.

