

A Study of Awareness of Cybersecurity Measures among the Prospective Teachers of University of Lucknow

Ravi Kumar¹, Dr. Neetu Singh²

¹Research Scholar, Department of Education, University of Lucknow, Lucknow, India,

²Associate Professor, Department of Education, University of Lucknow, Lucknow, India,

¹Email: ravi.krug@gmail.com ²Email: neetu_stp@rediffmail.com



Received 05 July 2026

Accepted 12 July 2026

Published 20 July 2026

Corresponding Author:

Ravi Kumar

Email: ravi.krug@gmail.com

DOI: <https://doi.org/10.64880/pcjaict.v1i3.01>

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sector.

Copyright: © 2026 The Author(s).



This is an open access article under the [Creative Commons Attribution-Noncommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

OPEN ACCESS

Abstract:

Cybersecurity has emerged as a significant concern in various sectors, including education, due to the vital role of digital technology in our society. With the ongoing integration of technology in the education sector, protecting the digital assets and personal information of individuals and educational institutions has become a critical issue. Cybersecurity awareness has become an essential competency for prospective teachers as digital technologies are increasingly integrated into educational practices. The present study aimed to investigate the present state of awareness of cybersecurity measures among prospective teachers of University of Lucknow. A descriptive survey method was employed for the present study. A sample of 178 prospective teachers were taken by using stratified random sampling techniques. Mean, S.D. and t-test were employed to analyze the data. mass of forthcoming teachers has average awareness of cybersecurity measures and there is a significant difference in level of awareness of cybersecurity measures between campus forthcoming teachers and forthcoming teachers of associated colleges of University of Lucknow. The study can contribution the university in recognizing areas wherever cybersecurity awareness necessities to be enhanced. Thus, supports to stand-in a culture of cybersecurity knowledge and readiness among the forthcoming teachers.

Keywords: Cybersecurity, Awareness, Prospective Teachers.

INTRODUCTION

The quick digitalization of education has basically redesigned how teaching, learning, assessment, and institutional administration are directed. Learning management systems, cloud-based alliance

tools, digital assessment programs, artificial intelligence applications, and mobile learning environs have become integral components of educational institutions. While these progresses have extended access to knowledge and reinforced pedagogical modernization, they have concurrently increased the interaction of educational institutions to cyber fears. Educational institutions nowadays accomplish huge sources of sensitive individual, academic, financial, and research facts, making them striking goals for cybercriminals. Phishing movements, ransomware attacks, identity theft, data gaps, credential cooperation, and social engineering attacks are no extended remote technological worries rather, they have become educational substances that directly impact institutional trust, teaching continuity, and learners' digital well-being (ENISA, 2023; UNESCO, 2023).

The issue mostly relates to teacher preparation. Because they are both learners and future educators, future teachers have a special place in the educational ecosystem. They mostly face institutional portals, online learning environments, digital content sources, cloud storage services, communication apps, and social networking sites during their specialized training. These future educators will be responsible for teaching pupils how to use technology in a safe and moral manner in some years. Therefore, future educators need to be more mindful of cybersecurity comparison to only their own online safety. It is a crucial professional ability that guided instruction, digital citizenship, responsible technology use, and student safety.

In the broader framework of National Education Policy (NEP) 2020, which places a strong thrust on online literacy and technology-enabled education, cyber security competency has emerged as a necessary condition for a successful and secure educational transformation. Ransomware strikes have disrupted academic activities and exposed private archives, causing a sharp rise in cyberattacks on educational institutions worldwide. The education sector continues to be one of the most frequently targeted businesses globally, experiencing thousands of cyberattacks every week, according to Check Point Research (2026). Similar to this, the European Union Agency for Cybersecurity (ENISA, 2023) notes that unequal cybersecurity preparation, vast user populations, and dispersed digital infrastructures make educational institutions increasingly weak. Such tendencies indicate that technical security measures singly would not be enough to address cyber risks; the human awareness and accountable digital behavior are also vital layers of cyber protection.

In an ideal world, teacher education programs would train their graduates to be adequate awareness of cybersecurity precautions, identify common cyber risks, practice safe online practices, comprehend data confidentiality principles, and set an example of responsible digital behavior for their future students. Thus, along with instructional expertise, technological proficiency, and ethical responsibility, cybersecurity awareness should be included in the professional competencies. Although, this goal is only partially realized. Cybersecurity education is typically not given systematic emphasis in teacher education programs, despite the fact that aspiring teachers frequently use digital technology in their courses, internships, online assessments, and collaborative learning.

While some organizations make reference to digital resources, they do not place as much thrust on safe digital practices.

Therefore, future teachers may possess purposeful digital literacy but lack sufficient understanding of password management, phishing detection, secure information sharing, privacy protection, multi-factor authentication, cyber ethics, or institutional security protocols.

This disconnect between technology acceptance and cybersecurity readiness creates numerous challenges. At the personal level, inadequate awareness increases vulnerability to cyber scams, identity theft, malware infections, financial fraud, and unauthorized disclosure of private information. Within educational institutions, risky user behavior may contribute to data breaches, disruption of academic activities, reputational damage, and financial losses. On a broader scale, teachers with inadequate cybersecurity awareness may inadvertently transmit insecure digital practices to students, thereby undermining efforts to promote responsible digital citizenship among youth. The consequences therefore extend beyond individual vulnerability to include institutional resilience and national educational security.

Different researchers from various countries have investigated the level of cybersecurity awareness among university students and teachers. According to Alharbi & Tassaddiq (2021), there was fluctuation regarding the level of cybersecurity awareness among university students, even though there were significant gaps in applied behaviors despite adequate theoretical knowledge. According to Bada et al. (2019), awareness programs usually increase knowledge but do not necessarily lead to sustained behavioral change. In the same way, Parsons et al. (2014) suggested that cybersecurity awareness should be studied as a multidimensional construct that includes knowledge, attitudes, perception, and purposeful behavior rather than purely information. In India, the number of new studies has emerged that acknowledge increasing worries about the privacy of data, cyber hygiene, and cybersecurity awareness among higher education students; however, studies that focus specifically on teacher education are still scarce (CERT-In, 2023).

However, there are still numerous limitations. Firstly, a large part of current literature focuses on university students in general rather than on teachers in training who have different responsibilities compared to others. Secondly, many researchers emphasize technical knowledge or high levels of cybercrimes and pay relatively little attention to practical cybersecurity measures awareness among students. Thirdly, research results obtained in developed countries cannot be simply generalized to Indian teacher education since there is a difference between technological facilities, institutional norms, curricula, and digital practices. Fourthly, only a small number of studies investigate cybersecurity awareness among state university students in India, including the University of Lucknow, where students of teachers' education are a significant part of future teaching staff. Such violations are theoretically and practically important. Digital competency frameworks have increasingly incorporated the concepts of safety, privacy, and responsible technology use as key elements of professionalism. In its DigComp 2.2, the European Digital Competence Framework considers safety and security equally important alongside information and communication skills (Vuorikari et al., 2022). Likewise, in their studies, Davis (1989) and Rogers (1975) propose the

Technology Acceptance Model and Protection Motivation Theory and argue that technology use and safety behavior depend on access, usefulness, as well as individuals' perception of risks, efficacy, and intention. In light of such perspectives, the current study will consider cybersecurity awareness as a multidimensional construct concerning knowledge about cyber threats, awareness of cybersecurity measures, harmless behavior online, privacy protection, and responsible use of digital resources by future teachers.

Taking all of the above into account, the current study will address an important gap through investigating the awareness of cybersecurity measures among prospective teachers studying at the University of Lucknow. While the present study will not concentrate on technical expertise only, it is intended to assess to what extent aspiring teachers are familiar with cybersecurity measures that are needed to ensure safe learning via digital means. The findings of the study are expected to contribute to developing curriculums and policies related to contemporary digital education.

OBJECTIVE OF THE STUDY

The study is guided by the following objectives:

1. To study the level of awareness of cybersecurity measures of university campus prospective teachers of the University of Lucknow.
2. To study the level of awareness of cybersecurity measures of prospective teachers of affiliated colleges of the University of Lucknow.
3. To compare the mean scores of awareness of cybersecurity measures of university campus prospective teachers and prospective teachers of affiliated colleges of the University of Lucknow.

HYPOTHESIS OF THE STUDY

There is no significant difference between the mean scores of awareness of cybersecurity measures of university campus prospective teachers and prospective teachers of affiliated colleges of the University of Lucknow.

METHODOLOGY

A descriptive survey method was used in the present study. A sample of 178 pupil teachers was selected by using stratified random sampling. Cybersecurity Awareness Scale (a researcher-made tool) was used to collect data. In the present study, mean, SD, percentage, and t-test were used to assess the level of awareness of cybersecurity measures of prospective teachers.

DATA ANALYSIS AND INTERPRETATION

The current study has been examined as follows with reference to the objective of the study.

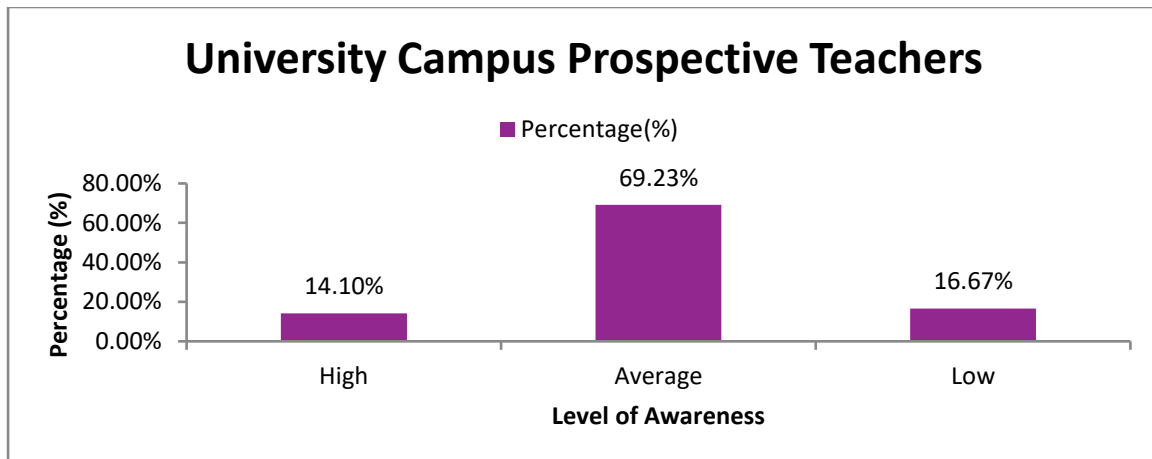
Objective 1: To study the level of awareness of cybersecurity measures of university campus prospective teachers of the University of Lucknow.

For this objective data were analyzed with the help of percentage and the result are given in the following tables:

Table 1: Percentage wise awareness of cybersecurity measures of university campus prospective teachers

Level of Awareness	Score	No. of Students	Percentage
High Awareness	Above 134	11	14.10%
Average Awareness	108-134	54	69.23%
Low Awareness	Below 108	13	16.67%

Figure 1: Percentage wise awareness of cybersecurity measures of university campus prospective teachers



From the above table 1 and graph in figure 1, it can be seen that 14.10% university campus prospective teachers have scored above 134 marks and have high level of awareness of cybersecurity measures while 16.23% university campus prospective teachers have scored below 108 marks and have low level of awareness of cybersecurity measures and 69.23% university campus prospective teachers have average level of awareness of cybersecurity measures.

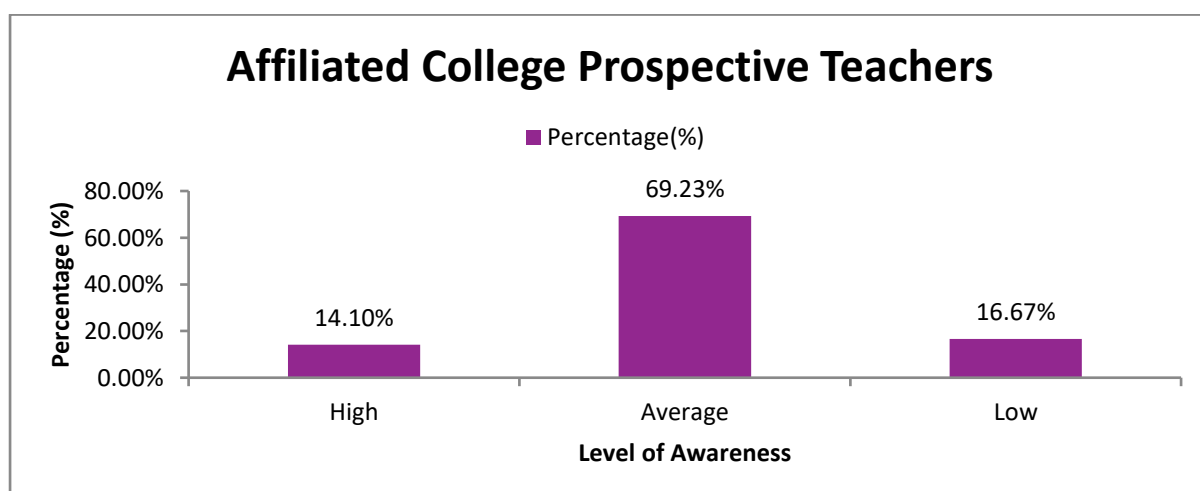
Objective 2: To study the level of awareness of cybersecurity measures of prospective teachers of affiliated colleges of the University of Lucknow.

For this objective data were analyzed with the help of percentage and the result are given in the following tables:

Table 2: Percentage wise awareness of cybersecurity measures of prospective teachers of affiliated colleges

Level of Awareness	Score	No. of Students	Percentage
High Awareness	Above 139	8	8.00%
Average Awareness	118-139	84	84.00%
Low Awareness	Below 118	8	8.00%

Figure 2: Percentage wise Awareness of Cybersecurity measures of prospective teachers of affiliated colleges



From the above table 2 and graph in figure 2, it can be seen that 8.00% affiliated college prospective teachers have scored above 139 marks and have high level of awareness of cybersecurity measures while 8.00% affiliated college prospective teachers have scored below 118 marks and have low level of awareness of cybersecurity measures and 84.00% affiliated college prospective teachers have average level of awareness of cybersecurity measures.

This means that the majority of prospective teachers have average or moderate understanding of the cybersecurity measures, which is a positive sign but, it also indicates that there is still room for improvement in their overall awareness and knowledge.

Objective 3: To compare the mean scores of awareness of cybersecurity measures of university campus prospective teachers and prospective teachers of affiliated colleges of the University of Lucknow.

H₀: There is no significant difference between the mean scores of awareness of cybersecurity measures of university campus prospective teachers and prospective teachers of affiliated colleges of University of Lucknow.

For the verification of the H₀ the data was analyzed with the help of t-test and results are given in table 3.

Table 3: Institute type wise comparison of mean scores of awareness of cybersecurity measures of prospective teachers

S. No.	Institute	N	Mean	S.D.	t-value	Remark
1	University Campus	78	120.8077	13.0208	3.98	Significant at 0.05 level
2	Affiliated College	100	128.02	10.446		

From table 3, It can be seen that t-value is 3.98, which is significant at 0.05 level with d.f. = 176. It indicates that mean scores of awareness of cybersecurity measures among university campus prospective teachers and prospective teachers of affiliated colleges of University of Lucknow differ significantly. Thus, the null hypothesis that there is no significant difference between the mean scores of awareness of cybersecurity measures among university campus prospective teachers and prospective teachers of affiliated colleges of University of Lucknow is rejected. Further, the mean scores of awareness of cybersecurity measures among prospective teachers of affiliated colleges of University of Lucknow is 128.02, which is significantly higher than those of university campus prospective teachers whose mean scores of awareness of cybersecurity measures is 120.8077.

It may therefore be said that " **prospective teachers of affiliated colleges of University of Lucknow were found to have significantly better awareness of cybersecurity measures as compared to university campus prospective teachers.**"

FINDINGS AND DISCUSSION

The findings indicate that awareness was predominantly at the average level in both institutional settings, although a statistically significant difference emerged between the two groups. Specifically, 69.23% of university campus prospective teachers and 84.00% of affiliated college prospective teachers demonstrated average awareness, while only a small proportion in either group exhibited high awareness. Moreover, allied college prospective teachers got a significantly higher mean

awareness score ($M = 128.02$, $SD = 10.40$) than their university campus equals ($M = 120.81$, $SD = 13.02$), with the alteration reaching statistical significance ($t = 3.98$, $p < .05$). This evidence suggests that the level of cybersecurity awareness amongst future teachers is not unduly low but also not adequately high enough to satisfy the growing security needs of modern-day teaching situations.

The predominance of average cybersecurity awareness can be traced back to an important element of teacher training in India. Given the rising use of digital technology in teaching, testing, learning, and management, upcoming teachers are likely to become more exposed to cyber-attacks. However, the training of upcoming teachers regarding cybersecurity continues to be inadequate even in the best curriculums of teacher education. This is why many students gain cybersecurity awareness informally.

This trend can help to explain why the level of awareness is moderate rather than high. Such observations were reported in the study by Bada and Nurse (2019), which claimed that awareness programs increase the awareness about cyber threats but do not foster safe behavior. In addition, Alharbi and Tassaddiq (2021) revealed that the awareness of university students was adequate concerning cybersecurity issues, but important deficiencies existed in password management, phishing awareness, and personal information protection. Thus, the current findings reinforce the growing body of international research proving the inadequacy of cybersecurity awareness of university students in dealing with advanced cyber threats.

It is important to pay attention to the relatively low number of respondents who had high awareness levels. Just 14.10% of prospective teachers from university campuses and 8.00% of those from colleges reached high awareness levels. Considering the fact that these prospective teachers will soon start working as teachers, the issue mentioned above may raise certain concerns about their capability of ensuring safe digital behavior of school students. In addition, teachers should play the role of facilitators of digital citizenship, which means that they should protect personal information of learners, teach them good behavior in the digital environment, and react appropriately to any cybersecurity issues. This is the reason why relatively low awareness levels may indicate the readiness gap in the teacher education program. It was pointed out by UNESCO (2023) as well.

The proportion of highly aware prospective teachers was slightly higher on the university campus; however, the college prospective teachers had a significantly higher total average awareness score. The apparent anomaly means that awareness scores were relatively more evenly spread for associated college prospective teachers while university campus prospective teachers scored higher with relatively greater variation, shown by the higher standard deviation. One plausible explanation has to do with the level of institutional exposure to digital practices. Several associated colleges have increasingly embraced the use of blended learning approaches, learning management system, presence online, digital assessment, and institutional cybersecurity strategies after the emergence of online learning after the COVID-19 pandemic. Consistent interaction with the digital world can have strengthened cybersecurity awareness despite the few high-scoring people.

In addition to the statistically significant institutional differences, this result also adds value to ongoing debate about contextual factors of cybersecurity awareness. It has already been proven that

cybersecurity awareness is influenced by individual characteristics along with institutional context, access to digital information, prior training and technology usage. Parsons et al. (2014) pointed out that the working environment has a strong influence on people's secure behavior through increased awareness due to constant interaction with other people in this institution. Furthermore, Hadlington (2017) proved that digital experience and technology experience predict the level of cybersecurity awareness among adults. This study confirms these statements, indicating that the institutional context can have a stronger influence on awareness than individual demographics.

However, the current findings differ from previous studies which found consistently low levels of cybersecurity awareness among college students from developing countries. Some studies from South Asia and Africa have revealed consistent gaps in terms of awareness about phishing, malware, identity theft, and privacy protection. The comparatively higher awareness level in this current study might be attributed to the rising importance that is being placed on cybersecurity issues in India. Government programs such as Digital India, National Cyber Security Policy, various awareness campaigns by CERT-In, and extensive use of e-learning sites have significantly increased the awareness levels regarding cybersecurity. Even if these governmental programs might not have offered any kind of training to people, it seems as though they help gain some basic knowledge among future teachers.

EDUCATIONAL IMPLICATIONS

These findings can have vital implications for policies concerning educational technologies and curriculum in teacher training institutions. According to the National Education Policy (2020), there should be an extensive incorporation of digital technologies into educational systems, yet the importance of digital literacy and safe utilization of technology is highlighted. Yet the curriculum in teacher training institutes provides no emphasis on cybersecurity skills development. These findings indicate that it should be an integral part of preservice teacher training program rather than an additional part of the educational technology curriculum. Cybersecurity training may involve such aspects as password management, phishing detection, privacy protection, cybernetics, safe use of educational technologies, handling of student data, and incident reporting. Furthermore, such training techniques as simulations, case studies, cyber drills, and scenarios may provide more benefits for students than just informative presentations.

In addition to curriculum revisions, the higher education institutions should introduce cybersecurity awareness ecosystems. Workshops, cybersecurity policies within educational institutions, alignment programs, awareness campaigns, and collaboration with cybersecurity professionals will ensure secure behavior of trainees during their preparation. Continuous assessment of cybersecurity skills of future teachers will also help institutions find out what aspects require further studying before teachers go into practice.

CONCLUSION

This study explored the extent of cybersecurity measures' awareness amongst prospective teachers enrolled at University of Lucknow and its affiliated colleges. Specifically, this study aimed to examine the extent of cybersecurity awareness amongst prospective teachers in general and compare

awareness levels in different institutional settings. As the world is moving towards digitalization and technology plays a vital role in transforming educational practices; the preparedness of prospective teachers to detect and address any cyber threat has become important. The findings indicated that the vast majority of prospective teachers have an average level of cybersecurity awareness, whereas only few prospective teachers had high cybersecurity awareness level. In addition, there was a statistically significant difference between the two institutions with regard to their awareness levels with prospective teachers at the affiliated colleges having higher mean cybersecurity awareness scores compared to the prospective teachers of the university campus. While the findings show that prospective teachers have some awareness about cybersecurity measures, they also highlight that there is still plenty of room to enhance their cybersecurity skills before entering the profession of teaching.

In light of the ongoing digital revolution within the field of education in the post-pandemic era, equipping future teachers with broad knowledge about cybersecurity and cybersecurity competencies will become a necessity to ensure that educational institutions become safe learning environments and nurture responsible digital citizenship. The findings confirm the assertion that cybersecurity awareness develops through educational processes, institutional support, and consistent exposure to digital technology, as opposed to mere secondary exposure. Moreover, based on the findings, it can be asserted that institutional contexts influence cybersecurity readiness of future teachers, and hence there is a need to integrate cybersecurity education in teacher preparation programs. In disseminating cybersecurity research to the domain of pre-service teacher education, this paper contributes to the existing body of literature on digital competency and regards cybersecurity awareness as an essential element of professional willingness in the modern educational sector.

REFERENCES

- Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Journal of King Saud University – Computer and Information Sciences*. <https://www.researchgate.net/publication/351459566>
- Ayanwale, M. A., Sanusi, I. T., Molefi, R. R., & Otunla, A. O. (2024). A structural equation approach and modelling of pre-service teachers' perspectives of cybersecurity education. *Education and Information Technologies*, 29, 3699–3727. <https://doi.org/10.1007/s10639-023-11973-5>
- Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv*. <https://doi.org/10.48550/arXiv.1901.02672>
- Chawla, V., Kapoor, Y., & Chawla, T. (2023). Cybersecurity awareness amongst youth: A survey in Delhi/NCR. *Indian Journal of Computer Science*, 8(2), 42–52. <https://doi.org/10.17010/ijcs/2023/v8/i2/172777>
- Check Point Research. (2026). The state of global cyber security 2026. <https://research.checkpoint.com/2026/cyber-security-report-2026/>

- Computer Emergency Response Team–India. (2023). Annual report 2022–2023. Ministry of Electronics and Information Technology, Government of India. <https://www.cert-in.org.in/s2cMainServlet?pageid=PUBANULREPRT>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340. <https://doi.org/10.2307/249008>
- European Union Agency for Cybersecurity. (2023). ENISA threat landscape 2023. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf>
- Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, 3(7), e00346. <https://doi.org/10.1016/j.heliyon.2017.e00346>
- National Education Policy 2020. https://static.pib.gov.in/WriteReadData/userfiles/NEP_Final_English_0.pdf
- National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST CSWP 29). <https://doi.org/10.6028/NIST.CSWP.29>
- Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
- 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>
- Sridevi, K. V. (2020). Cyber security awareness among in-service secondary school teachers of Karnataka. *Indian Journal of Educational Technology*, 2(II), 82–94. <https://journals.ncert.gov.in/IJET/article/view/366>
- Torres-Hernández, N., & Gallego-Arrufat, M. J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies*, 27(6), 8583–8602. <https://doi.org/10.1007/s10639-022-10978-w>
- UNESCO. (2023). Global Education Monitoring Report 2023: Technology in education—A tool on whose terms? UNESCO. <https://www.unesco.org/gem-report/en/publication/technology>
- Vuorikari, R., Kluzer, S. and Punie, Y., DigComp 2.2: The Digital Competence Framework for Citizens - With new examples of knowledge, skills and attitudes, EUR 31006 EN, Publications Office of the European Union, Luxembourg, 2022, ISBN 978-92-76-48882-8, <https://doi.org/10.2760/115376>, JRC128415.

Disclaimer/Publisher's Note: The views, findings, and opinions expressed in this publication are solely those of the author(s). The publisher and editorial team are not responsible for any errors, claims, or consequences arising from the use of the published content.