I.J. Modern Education and Computer Science, **2026, 2, 163-172**
Published Online on April 8, 2026 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2026.02.10

Cyber Security Competency and Socialization among Prospective Teachers: Effect of a Cyber Safety and Security Literacy Program

Santhosh Thangan*
Department of Education, National Institute of Technology, Calicut, Kerala, India
Email: santhoshelappully@gmail.com
ORCID iD: https://orcid.org/0000-0002-1850-0105
*Corresponding Author

Thiyagu Kaliappan
Department of Education, Central University of Karnataka, Kalaburgi, India
Email: thiyagucuk@gmail.com
ORCID iD: https://orcid.org/0000-0003-0533-597X

Received: 24 June, 2025; Revised: 10 October, 2025; Accepted: 02 February, 2026; Published: 08 April, 2026

Abstract: In the context of increasing cyber threats, digital misinformation, and online ethical dilemmas, the role of teachers in promoting safe and responsible digital behavior has become more critical than ever. This study explores the effectiveness of the Cyber Safety and Security Literacy Program (CSLP) in enhancing cyber security competency and cyber socialization among prospective teachers. The CSLP was designed as a structured educational intervention aimed at equipping future educators with the knowledge, skills, and ethical orientation necessary to navigate cyberspace confidently and responsibly. A pre-experimental one-group pre-test and post-test design was adopted, involving 50 purposively selected B.Ed. students from various teacher education institutions. The two-month intervention was delivered through Google Classroom and Google Meet, ensuring flexibility and interactive participation. The CSLP comprised 12 carefully curated modules covering critical themes such as cyber threats, digital identity protection, cyber bullying prevention, cyber ethics, safe communication, and responsible social media use. To evaluate the program's impact, data were collected using two standardized tools—the Cyber Security Competency Scale (CSC) and the Cyber Socialization Scale (CSS), both of which were developed through systematic procedures and supported by strong theoretical grounding and expert validation, providing evidence of their validity. Statistical analysis using paired-sample t-tests revealed significant improvements in participants' cyber security competency ($t(49) = 30.55$, $p < .01$, $d = 4.32$) and cyber socialization ($t(49) = 17.75$, $p < .01$, $d = 2.51$), indicating a large effect size in both domains. The findings affirm that the CSLP is an effective intervention for fostering digital responsibility, ethical awareness, and safe online behavior among future educators. The study emphasizes the urgent need to integrate comprehensive cyber security literacy programs within teacher education curricula, positioning teachers not only as informed digital citizens but also as proactive facilitators of cyber safety and ethical conduct in the learning environment.

Index Terms: Cyber Safety Literacy, Cyber Security Competency, Cyber Socialization, Teacher Education, Digital Citizenship

1. Introduction

The rapid growth of Internet usage in recent years has transformed how individuals communicate, learn, and access information [1]. According to the "We Are Social" and Hootsuite Digital Report (2022), there are 4.9 billion Internet users globally, accounting for 62.5% of the world's population. In India, Internet penetration has surged significantly, with millions of users relying on digital platforms for daily activities, highlighting the Internet's role as an indispensable part of modern life. However, with its benefits come challenges, particularly the growing threats related to cyber security and digital safety[2].

The increased reliance on the Internet has made individuals more vulnerable to risks such as cyber-attacks, phishing scams, identity theft, and misinformation. These threats highlight the critical need for robust cyber safety

This work is open access and licensed under the Creative Commons CC BY 4.0 License.

practices [3]. Prospective teachers, in particular, hold a dual responsibility: safeguarding their digital well-being and fostering responsible and ethical Internet use among future generations[4]. Despite advancements in digital literacy programs, a lack of emphasis on comprehensive cyber safety and security education has left many teachers underprepared to address the complex challenges of the digital world [5].

This issue extends beyond technical know-how to include the ability to engage in ethical and constructive online interactions, referred to as cyber socialization. Cyber socialization encompasses behaviors, attitudes, and norms that guide responsible participation in the digital sphere[6]. For prospective teachers, developing these skills is essential for navigating online environments effectively and serving as role models for their students[7].

To address these needs, this study designed and implemented a Cyber Safety and Security Literacy Program (CSLP) aimed at enhancing the cyber security competency and cyber socialization of prospective teachers. By equipping them with the knowledge and skills to identify and mitigate digital threats while promoting ethical online behavior, the CSLP seeks to empower teachers to lead by example and foster a culture of safe and responsible digital practices.

1.1 Cyber Security Competency and Cyber Socialization

Cyber security competency refers to the knowledge, skills, and attitudes necessary to identify, prevent, and respond to cyber threats effectively[8]. In an increasingly digital world, the ability to safeguard personal and professional information against risks such as hacking, phishing, malware, and identity theft has become a critical skill for educators and learners alike[9]. Research emphasizes the importance of fostering cyber security competency among prospective teachers to prepare them for addressing the challenges of digital safety and to empower them to educate future generations on secure digital practices [10]. This aligns with global efforts to integrate cyber security education into teacher training programs as a fundamental aspect of professional preparedness[11].

Cyber socialization, on the other hand, focuses on fostering ethical, responsible, and constructive interactions within digital environments. It includes the development of norms, behaviors, and practices that enable individuals to engage positively in online spaces while maintaining respect for diverse perspectives[12]. For prospective teachers, cyber socialization is a vital skill, as they are role models for students, shaping how young learners interact and communicate in the digital realm. Strong cyber socialization skills can reduce instances of cyber bullying, promote digital inclusion, and encourage collaborative learning[13].

Efforts to enhance cyber security competency and cyber socialization among educators have gained traction in recent years[14]. Programs and initiatives have been implemented to provide educators with resources and training to build these skills. For example, some countries have introduced targeted curricula addressing online safety, ethical digital use, and interpersonal skills in virtual settings[15]. However, in many regions, including India, the systematic inclusion of cyber security and socialization topics in teacher education remains limited, leading to fragmented knowledge and inconsistent practices.

Addressing these gaps requires structured interventions, such as the CSLP which aims to equip prospective teachers with essential cyber security skills and foster their ability to navigate and facilitate ethical digital interactions. By enhancing these competencies, such programs prepare educators to create safer and more inclusive digital environments, benefitting both themselves and their future students.

2. Research Questions

The role of targeted educational programs in enhancing cyber security competency and fostering ethical online behavior has not been comprehensively explored, particularly among prospective teachers. This study aimed to address this gap by designing and implementing a CSLP to empower prospective teachers with the knowledge, skills, and attitudes necessary to navigate and promote a safe digital environment. Additionally, the study sought to investigate the impact of the CSLP on improving participants' cyber socialization, fostering responsible online interactions, and enhancing their overall preparedness as digital role models. The following research questions (RQs) guided this study:

RQ1: Do prospective teachers who participate in the CSLP demonstrate higher cyber security competency compared to those who do not?

RQ2: Does participation in the CSLP enhance prospective teachers' ability to engage in ethical and responsible cyber socialization?

RQ3: Are prospective teachers more confident and motivated in promoting cyber safety practices after participating in the CSLP?

3. Method

To address the research questions, this study is structured into two interrelated sections. The first section involves the design and development of the Cyber Safety and Security Literacy Program (CSLP), designed specifically for prospective teachers. The second section focuses on evaluating the effectiveness of the CSLP through a pre-experimental research design utilizing a one-group pre-test and post-test method.

3.1 Cyber Safety and Security Literacy Program (CSLP)

CSLP is a structured educational intervention aimed at enhancing individuals' knowledge, skills, and attitudes to navigate the digital landscape safely and responsibly. These programs address key aspects of cyber security, including identifying risks, managing online threats, protecting personal information, and fostering ethical online behavior. By integrating theoretical knowledge with practical activities, CSLPs empower participants to become proactive in safeguarding themselves and others in the digital world.

3.2 Module Design Principles

The CSLP was systematically developed using the ADDIE model (Analysis, Design, Development, Implementation, and Evaluation) to effectively address the specific cyber safety needs of prospective teachers. The program adopted a learner-centered approach by integrating real-world cyber safety challenges and encouraging active participation through case studies, group discussions, and role-playing. Content was designed to address prevalent cyber security concerns such as phishing, password protection, and digital footprints, ensuring relevance to the professional context of teacher education. The CSLP focused on two key behavioral outcomes: Cyber Security Competency (CSC) and Cyber Socialization. These outcomes were designed to build both technical skills and ethical digital behavior. Instructional strategies included interactive learning activities, scenario-based problem-solving, and reflective tasks to promote application of knowledge. Continuous assessment and immediate feedback supported concept reinforcement and addressed learning gaps. Learning objectives were structured using Bloom's Taxonomy, enabling cognitive progression from basic recall to higher-order thinking skills such as analysis and application. This structured and outcome-oriented approach aimed to equip prospective teachers with the necessary skills and awareness to foster a secure and responsible digital culture in educational settings.

3.3 Content Framework

The CSLP covered 12 key topics and 44 sub-modules, systematically addressing various aspects of cyber safety and security. Table 1 depicts the overview of CSLP contents.

Table 1. Overview of CSLP contents

No	Topics & No of Modules	Contents
1	Social Networking Safety (4)	Introduction to social networking, Platforms of social networking, Risks in social networking, Safe practices of social networking
2	Dealing with Fake Information(4)	The concept of fake information, General formats and platforms of fake information, Reasons behind creation and consumption of fake information, General tips to combat fake information
3	Mobile Phone Security and Safety(4)	Introduction to mobile phone safety and security, Major risks and threats in mobile phone usage, Areas of mobile phone safety and security, Safety concerns in mobile phone safety and security
4	Email and Password Safety(8)	Introducing Emails and Email Security, Forms of Email threats, Safe practices for email security, Introduction to password security, Characteristics of strong password, Major password cracking techniques, Safe practices for password security
5	Managing Digital Footprint(4)	Introduction to the concept of digital footprint ,Major types of digital footprint, Ways to create effective online presence, Ways to create effective online
6	Online Privacy and Wi-Fi Safety(7)	Introduction to the concept of online privacy, Online privacy related risks, General guidelines for what to share and what not to share, Safe practices for online privacy, The Conceptual Difference between Public Wi-Fi and Private Wi-Fi, Major Security Risks in Public Wi-Fi, Rules for Public Wi-Fi Safety
7	Apps Safety and Security(3)	An introductory note on apps and major kinds of apps, Major security risks in apps, Safe practices while using apps
8	Web Conferencing Safety(4)	Web Conferencing, Major Web Conferencing Platforms, Major Risks in Web Conferencing, Web Conferencing Safety
9	Digital Resource Safety, Plagiarism, and Copyright Infringement(6)	Digital Learning Resource, Major Dangers in Digital Learning Resource, Evaluation and Safe Practices for Digital Learning Resources, Plagiarism and its Examples, Safe practices for avoiding plagiarism, Copyright Infringement, Safe practices to avoid copyright infringement

This structure allowed participants to build their knowledge progressively, addressing technical, ethical, and social dimensions of cyber security.

3.4 Implementation Strategies and Resources

The CSLP was implemented online to ensure accessibility and flexibility for prospective teachers. Google Classroom was used as the Learning Management System, while Google Meet supported live interactive sessions. The program featured practical tasks such as identifying phishing emails, creating strong passwords, and managing digital footprints. Interactive quizzes, reflective discussions, and flexible module scheduling encouraged active, self-paced learning. Content was aligned with national priorities in digital literacy and cyber hygiene, drawing on relevant educational policies and ICT initiatives in India. Digital resources including concept maps, simulation exercises, and infographics were used to simplify complex topics and reinforce key concepts such as online privacy and digital

responsibility. To evaluate learning outcomes, a set of assessment tools was employed, including pre- and post-module quizzes, scenario-based evaluations, and participant feedback forms. These strategies collectively supported the program's aim of enhancing Cyber Security Competency and promoting ethical digital behavior among prospective teachers.

3.5 Validation of the Program

To ensure the content quality and instructional validity of the CSLP modules for prospective teachers, a comprehensive validation process was undertaken. Experts from three distinct domains—Computer Science education, teacher education, and cyber security—were invited to review the modules. The validation process incorporated both quantitative and qualitative descriptive methods. The qualitative analysis involved collecting expert feedback in the form of written comments and suggestions, which were thematically analyzed to inform refinements in the instructional design, content structure, and learning outcomes. The quantitative analysis utilized a structured validation questionnaire. Each expert rated the modules based on specific criteria, including: (1) conceptual clarity of cyber safety, (2) practical applicability of cyber safety practices, (3) integration of creative and critical thinking strategies, (4) learner engagement and initiation, (5) alignment with the intended learning outcomes, and (6) overall organization and structure of the program.

A systematic approach was adopted to analyze the expert ratings. The mean score for each expert group was computed by summing the ratings of individual validators and dividing by the total number of validators in that group. Since the expert validation instrument employed a five-point rating scale ranging from very poor to excellent, the midpoint of the scale (3.00) was fixed as the minimum threshold of acceptability, following standard practice in content validation studies[16].

Accordingly, components obtaining a mean score of 3.00 and above were interpreted as valid and suitable, whereas scores below 3.00 indicated the need for revision. In addition, to classify the overall quality of the program, a more stringent benchmark of 3.30 was established. Mean scores at or above 3.30 were interpreted as representing a "Good" level of quality, indicating that expert judgments were clearly above the average level of adequacy. The validation results are summarized in Table 2:

Table 2. Validation results

Experts	**Score from Validator**					**Average Scores**	**Remarks**
	I	II	III	**IV**	**V**		
Computer science teachers	3.25	3.46	3.25	3.32	3,36	3.33	Good
Cyber security professionals	3.11	3,42	3,69	3.32	3.53	3.41	Good
Training college teachers	3.44	3.22	3.43	3.25	3.67	3.40	Good

All three expert groups rated the CSLP modules above the benchmark level, indicating overall approval and recognition of the program's effectiveness. Cyber Security experts gave the highest mean score (3.41), followed closely by Teacher Educators (3.40) and Computer Science Teachers (3.33). The consistently positive ratings reflect the program's well-rounded design, relevance to contemporary cyber safety needs, and alignment with pedagogical expectations in teacher preparation. These findings suggest that the CSLP modules are both pedagogically sound and practically relevant, supporting the development of cyber security competencies among future educators.

4. Effectiveness of the Program

In this study, a pre-experimental research method was employed to evaluate the effectiveness of the CSLP in enhancing prospective teachers' cyber security competency and cyber socialization.

4.1 Participants and Implementation Procedure

The study was carried out during the 2023–2024 academic year using a purposive sampling method. A total of 50 B.Ed. students from various teacher training colleges in Kerala, a southern state in India, were selected to participate. The sample included prospective teachers with diverse academic backgrounds and varying levels of prior exposure to cyber security, ensuring a realistic representation of the target population. The intervention involved the implementation of the CSLP through an online platform using Google Classroom and Google Meet. The program comprised 12 topics and 44 sub-modules covering key cyber safety concepts. Participants engaged in interactive activities such as identifying phishing attempts, creating secure passwords, and managing digital footprints, along with discussions, case studies, and reflective exercises. Ethical guidelines were strictly adhered to in this study. Informed consent was obtained from all participants, and they were assured of the confidentiality of their responses and the voluntary nature of their participation.

At the beginning of the intervention, participants completed a 10-minute pre-assessment questionnaire to evaluate their baseline levels of cyber security competency, cyber socialization, and cyber etiquette. This was followed by a brief 10-minute introduction to the importance of cyber safety and security, highlighting the relevance of these skills in the digital age, which was delivered by the instructor. Subsequently, participants engaged in the CSLP. The experimental intervention involved interactive modules delivered through an online platform over a span of two months. Activities

included recognizing phishing attempts, creating strong passwords, managing digital footprints, and understanding safe online behaviors. At the conclusion of the program, participants completed a 10-minute post-assessment questionnaire to evaluate their progress in cyber security-related skills. The results of the pre- and post-assessments were then analyzed to measure the impact of the intervention on participants' cyber security competency and socialization.

4.2 Instrumentation

To evaluate the impact of the CSLP, two key assessment instruments were employed: the Cyber Security Competency Scale (CSC) and the Cyber Socialization Scale (CSS). Both instruments were administered as pre- and post-intervention measures.

The Cyber Security Competency Scale (CSC) was developed by drawing upon established digital literacy and cybersecurity frameworks, including the DigComp Framework and the UNESCO ICT Competency Framework for Teachers. The scale comprises 78 items rated on a three-point scale (2 = Yes, 1 = No, 0 = Unsure). It covers nine domains, namely: 1. Social Networking Safety and Security (SNS), 2. Dealing with Fake Information (DWF), 3. Mobile Phone Security and Safety (MPS), 4. Email and Password Security and Safety (ELS),5. Managing Digital Footprint (MDF), 6. Online Privacy and Wi-Fi Safety (OWS), 7. Application Safety and Security (APS), 8. Web Conferencing Safety (WCS), 9. Digital Learning Resource Safety, Plagiarism, and Copyright Infringement (DRS). The scale demonstrated strong internal consistency, with Cronbach's alpha values of 0.87 (pre-test) and 0.90 (post-test). To ensure the scale's validity, the investigators employed construct validity using Confirmatory Factor Analysis (CFA). The CFA results demonstrated excellent validity, with a Chi-square value of 145.72 ($p = .196$), indicating statistical significance. Fit indices further supported the model: the Comparative Fit Index (CFI) was 0.945, the Tucker–Lewis Index (TLI) was 0.927, and the Root Mean Square Error of Approximation (RMSEA) was 0.067, collectively indicating a very good fit to the hypothesized model.

The Cyber Socialization Scale (CSS) was designed to evaluate participants' ability to engage ethically, responsibly, and constructively within digital environments. The scale originally consisted of 30 items and was refined to a 24-item instrument, emphasizing adherence to norms, rules, and expectations that guide behavior in cyberspace. Responses were recorded on a four-point Likert scale, and the scale showed good reliability, with Cronbach's alpha values of 0.78 (pre-test) and 0.89 (post-test). Within the scope of the present study, the construct validity of the CSS was supported through rigorous theoretical grounding and expert review. Further studies with broader samples are encouraged to strengthen the validity evidence of the scale.

Both instruments underwent expert validation by specialists in cybersecurity education and teacher training. A pilot study involving 257 B.Ed. students, who were not part of the main research sample, was conducted to assess the tools' clarity, relevance, and reliability. Feedback from this pilot led to minor revisions in item wording and structure to improve comprehensibility and cultural appropriateness.

4.3 Data Collection and Analysis Procedure

The instruments, namely the Cyber Security Competency Scale (CSC) and the Cyber Socialization Scale (CSS), were administered both before and after the intervention to assess the effectiveness of the CSLP. The survey was conducted online using Google Forms to ensure ease of access and wider reach among participants. Prior to data collection, participants were informed about the purpose of the study, assured of confidentiality and voluntary participation, and encouraged to respond honestly.

All responses were initially recorded in Microsoft Excel and subsequently imported into SPSS (Statistical Package for the Social Sciences) for analysis. To examine the impact of the intervention, a paired-sample t-test was conducted to compare pre- and post-test scores on both the CSC and CSS, thereby measuring changes in participants' cyber security competency and socialization behavior. In addition, descriptive statistics were used to analyze mean scores and standard deviations for each domain within the scales. Effect sizes were calculated to determine the magnitude of change resulting from the intervention.

5. Experimentation Results

To address RQ1, i.e., to find out whether the CSLP has a significant effect in augmenting cyber security competency among prospective teachers, a comparison of the total pretest and post-test scores of the total sample was tested for the significance of difference of the scores.

The data and results of the test of significance of difference between the mean pre-test scores and post test scores of cyber security competency and its components among the total sample are given in Table 3.

Table 3 reveals the mean comparison of pre- and post-test scores of cyber security competency (CSC) and its components. The analysis revealed a significant difference between the pre-test and post-test scores of cyber security competency (CSC), $t(49) = 30.55$, $p < .01$. The mean CSC score improved from $M = 91.22$, $SD = 13.55$ in the pre-test to $M = 127.66$, $SD = 8.07$ in the post-test. A strong positive correlation was observed between the two sets of scores ($r = .81$, $p < .01$). The calculated effect size was large, with Cohen's $d = 4.32$.

Table 3. Mean comparison of cyber security competency (CSC) and its components among the total sample

Component	Pre-test		Post-test		t(49)	p	r	Cohen's d
	M_1	SD_1	M_2	SD_2				
CSC Total	91.22	13.55	127.66	8.07	30.55	.00	.81**	4.32
SNS	11.68	1.67	15.70	1.47	18.88	.00	.54**	2.67
DWF	9.36	2.45	13.02	1.56	13.45	.00	.62**	1.90
MPS	11.50	2.63	15.60	1.89	12.92	.00	.55**	1.83
MDF	8.48	2.30	13.08	1.66	19.81	.00	.70**	2.80
OWS	11.44	1.76	14.36	.74	13.55	.00	.51**	1.92
APS	11.66	1.85	16.00	1.94	22.49	.00	.74**	3.18
WCS	7.58	2.36	11.74	1.33	15.668	.00	.61**	2.22
DRS	10.56	2.95	15.22	2.17	18.75	.00	.80**	2.65
ELS	8.96	2.50	13.06	1.63	13.79	.00	.55**	1.95

*N=50; **Significant at 0.01 level*

For the component Social Networking Safety (SNS), there was a significant increase in scores, $t(49) = 18.88$, $p < .01$, with the pre-test mean at $M = 11.68$, $SD = 1.67$ and the post-test mean at $M = 15.70$, $SD = 1.47$. A moderate correlation was found between the scores ($r = .54$, $p < .01$), and the effect size was large ($d = 2.67$). The component Dealing with Fake Information (DWF) also showed significant improvement, $t(49) = 13.45$, $p < .01$. The pre-test mean score was $M = 9.36$, $SD = 2.45$, which increased to $M = 13.02$, $SD = 1.59$ in the post-test. The correlation between the two scores was significant ($r = .62$, $p < .01$), and the effect size was large ($d = 1.90$).

In Mobile Phone Safety (MPS), a significant mean difference was observed, $t(49) = 12.92$, $p < .01$. The mean score improved from $M = 11.50$, $SD = 2.63$ to $M = 15.60$, $SD = 1.89$. A significant correlation was found ($r = .55$, $p < .01$), and the effect size was large ($d = 1.83$). For Managing Digital Footprint (MDF), the mean difference was significant, $t(49) = 19.81$, $p < .01$. The pre-test mean of $M = 8.48$, $SD = 2.30$ increased to $M = 13.08$, $SD = 1.66$ post-test. The correlation was strong ($r = .70$, $p < .01$), and the effect size was large ($d = 2.80$). The component Online Privacy and Wi-Fi Safety (OWS) also showed a significant difference in scores, $t(49) = 13.55$, $p < .01$. Pre-test scores averaged $M = 11.44$, $SD = 1.76$, rising to $M = 14.36$, $SD = 0.74$ in the post-test. The correlation was moderate ($r = .51$, $p < .01$), and the effect size was large ($d = 1.92$). In Application Safety (APS), the results indicated a significant improvement, $t(49) = 22.49$, $p < .01$. The pre-test mean score was $M = 11.66$, $SD = 1.76$, increasing to $M = 16.00$, $SD = 1.94$ post-test. The scores were strongly correlated ($r = .74$, $p < .01$), and the effect size was large ($d = 3.18$). For Web Conferencing Safety (WCS), the results showed a significant mean difference, $t(49) = 15.66$, $p < .01$. The mean score increased from $M = 7.58$, $SD = 2.36$ in the pre-test to $M = 11.74$, $SD = 1.33$ in the post-test. A significant correlation was observed ($r = .61$, $p < .01$), and the effect size was large ($d = 2.22$). Regarding Digital Learning Resources Safety (DRS), a significant improvement was found, $t(49) = 18.75$, $p < .01$, with pre-test scores at $M = 10.56$, $SD = 2.95$ and post-test scores at $M = 15.22$, $SD = 2.17$. The correlation was strong ($r = .80$, $p < .01$), and the effect size was large ($d = 2.65$).

Finally, in Email Safety (ELS), the results revealed a significant mean difference, $t(49) = 13.79$, $p < .01$. The average score rose from $M = 8.96$, $SD = 2.50$ to $M = 13.06$, $SD = 1.63$. The correlation between the scores was significant ($r = .55$, $p < .01$), and the effect size was large ($d = 1.95$).

To address RQ2, i.e., to find out whether the cyber safety and security literacy program has a significant effect in augmenting cyber socialization among prospective teachers, a comparison of the total pretest and post-test scores of the total sample was tested for the significance of difference of the scores.

The data and results of the test of significance of difference between the mean pre-test scores and post test scores of cyber socialization and its components among the total sample are given in Table 4.

Table 4. Mean comparison of CSS among the total sample

Variable	Pre-test		Post-test		t(49)	p	r	Cohen's d
	M_1	SD_1	M_2	SD_2				
CSS Total	62.02	5.84	78.76	4.70	17.75	.00	.21**	2.51

*N=50; **Significant at 0.01 level*

Table 4 reveals the mean comparison of pre- and post-test scores of cyber socialization (CS). The finding indicated a significant mean difference in CS with $t(49) = 17.75$, $p < .01$. Results show that the mean pre-test score of CS ($M1 = 62.02$, $SD1 = 5.84$) subsequently augmented in the post test scores of CS ($M_2 = 78.76$, $SD_2 = 4.70$). Two sets of scores were significantly correlated ($r = .21$, $p < .01$). The value of Cohen's d for pre and post test scores of CS was 2.51 (>.80), which indicates a large effect size.

To address RQ3, participants' confidence, motivation, and readiness to promote cyber safety practices were explored through informal interviews and structured discussion-based sessions. These qualitative interactions revealed

consistent perceptions of increased confidence, heightened awareness, and stronger motivation to advocate responsible cyber behavior. When considered alongside the significant improvement in cyber security competency (RQ1) and the enhancement of cyber socialization (RQ2), these findings provide convergent and supportive evidence of a positive shift in participants' readiness and willingness to promote cyber safety practices[17].

6. Discussion

The findings of this study demonstrate that the CSLP had a significant and positive effect on augmenting cyber security competency and cyber socialization among prospective teachers. The statistical evidence strongly supports the program's efficacy, as seen in the substantial improvement in mean post-test scores compared to pre-test scores across all measured components of cyber security competency[18–21]. The significant correlation observed between pre- and post-test scores in this intervention study primarily signifies consistency in participants' relative standing over time, reflecting the stability of the measurement rather than direct evidence of intervention impact; therefore, these correlations should be viewed as supplementary to the mean change and effect size results.

Specifically, the overall cyber security competency (CSC) showed a highly significant increase ($t(49) = 30.55$, $p < .01$) with a large effect size (Cohen's $d = 4.32$), indicating that the program was effective in enhancing participants' knowledge and skills. This improvement was consistent across all subcomponents, including social networking safety, dealing with fake information, mobile phone safety, managing digital footprints, online privacy and Wi-Fi safety, application safety, web conferencing safety, digital learning resource safety, and email safety. Each component demonstrated statistically significant gains with large effect sizes, confirming the comprehensive impact of the CSLP [22–25]. At the same time the extremely large effect sizes observed (e.g., Cohen's $d > 4$) are uncommon in educational research and warrant cautious interpretation. Although these values indicate strong pre–post sensitivity to the intervention, they may partly reflect design- and measurement-related factors, including the one-group pre–post design, strong alignment between the intervention content and assessment instruments, and the use of self-report measures. Such magnitudes may also indicate potential measurement artifacts, ceiling effects, or response bias. Furthermore, although the CSLP was associated with statistically significant gains across several outcome dimensions, the multiple paired comparisons conducted without formal adjustment procedures suggest that subscale-level significances may reflect chance effects. Accordingly, these findings should be interpreted sensibly.

These results align well with prior research on digital education interventions that emphasize experiential and practical learning approaches, such as role-playing and game-based learning, which have been shown to improve awareness, behavioral tendencies, and motivation in digital literacy contexts [24,26,27]. The strong correlations observed between pre- and post-test scores (r values ranging from .51 to .81) further reinforce the reliability of the observed scores of improvements.

Similarly, cyber socialization scores also significantly improved post-intervention ($t(49) = 17.75$, $p < .01$), with a large effect size (Cohen's $d = 2.51$). This suggests that the program effectively facilitated not only knowledge acquisition but also the social dimensions of cyber safety, which is crucial for fostering responsible digital citizenship and peer advocacy among future educators[26,29]. The observed enhancements in cyber security competency and socialization likely contributed to an increased sense of responsibility and motivation to promote cyber safety practices, which is critical for prospective teachers who are expected to serve as role models in digital environment [30–35]. This interpretation is further supported by studies on digital game-based learning (DGBL), which emphasize the role of immersive and interactive educational tools in strengthening intrinsic motivation and engagement with cyber wellness topics[35].

Furthermore, the qualitative findings revealed a positive shift in participants' perceived confidence, motivation, and readiness to promote cyber safety practices, which converged with the quantitative gains observed in RQ1 and RQ2. This pattern aligns with the concept of mastery experiences, wherein successfully completing hands-on tasks enhances perceived self-efficacy. Experiential engagement in cyber security activities not only strengthened participants' confidence in their personal skills but also fostered a growing sense of professional responsibility and advocacy orientation among prospective teachers to promote safe and ethical online practices[36,37].

7. Conclusion and Limitations

This study highlights the significant impact of the CSLP in enhancing both cyber security competency and cyber socialization among prospective teachers in Kerala. The results demonstrated statistically significant improvements across all key components of cyber safety following the intervention. The large effect size further indicated the practical effectiveness of the CSLP, suggesting that the program not only improved participants' knowledge and awareness but also positively influenced their attitudes and behaviors related to digital engagement. These findings emphasize the critical importance of integrating structured digital literacy and cyber safety programs into teacher education curricula. Equipping future educators with robust cyber safety knowledge prepares them to model and promote responsible online behavior, thereby cultivating digital citizenship among their students. In particular, CSLP modules focusing on online privacy, identifying and managing fake information, digital learning resource safety, and the role of prospective teachers in applying cyber safety practices within educational settings were instrumental in translating knowledge into

practice. By engaging participants with realistic digital scenarios and classroom-relevant tasks, these modules strengthened their confidence, motivation, and readiness to implement cyber safety strategies in educational contexts.

However, the study provides useful preliminary insights; it is not without methodological limitations. First, the research adopted a one-group pre-test–post-test pre-experimental design without a control or comparison group. Even while the CSLP intervention resulted in statistically significant improvements, the absence of a control group restricts the ability to attribute these gains exclusively to the program, because maturation effects, testing effects, or external influences cannot be ruled out. Second, the study was conducted with a relatively small sample of 50 prospective teachers selected through purposive sampling from teacher education institutions in Kerala. The non-random sampling technique and the focus on a single geographic region substantially limit the generalizability of the findings.

Therefore, future research should aim to include larger and more diverse populations and adopt longitudinal, observational, and objective behavioral assessment methods to examine the long-term retention and real-world application of the competencies gained. Despite these limitations, the study offers promising preliminary evidence supporting the potential value of integrating cyber wellness education within teacher preparation. At a policy level, the findings may inform pilot initiatives, curriculum development discussions, and capacity-building programs in teacher education institutions, rather than immediate large-scale mandates. Such exploratory evidence can support policymakers and curriculum planners in considering cyber wellness and cyber security literacy as emerging priority areas, while emphasizing the need for further rigorous research before formal curricular standardization. This approach may contribute to the gradual development of safer, more secure and ethically responsible digital learning environments across educational institutions.

Author Contributions Statement

Santhosh Thangan – Constructed the overall framework, Writing – Drafted the initial manuscript, contributed to the literature survey, and documented the technical background of the study.

Thiyagu Kaliappan – Conceptualization, Methodology, and Supervision: Proposed research ideas, Visualization, and Statistical analysis, and supervised project execution.

All authors have read and agreed to the published version of the manuscript.

Conflict of Interest Statement

The authors declare no conflicts of interest.

Funding Declaration

This research received no external funding.

Data Availability Statement

The data used to support the findings of this study are available from the corresponding author upon reasonable request.

Ethical Declarations

Authors have obtained informed consent from all individuals included in this study.

Acknowledgments

The authors thank the domain experts for their valuable feedback, which improved the quality of this study, and acknowledge all who supported this research.

Declaration of Generative AI in Scholarly Writing

During the preparation of this manuscript, the authors used AI-assisted tools to improve language clarity, grammar, and readability. The authors reviewed and edited the content as necessary and take full responsibility for the accuracy, originality, and integrity of the work.

Abbreviations

The following abbreviations are used in this manuscript:

APS -Application Safety and Security
CSC - Cyber Security Competency
CSLP -Cyber Security and Safety Literacy Program
CSS - Cyber Socialization Scale
DRS - Digital Learning Resource Safety, Plagiarism, and Copyright Infringement
DWF -Dealing with Fake Information
ELS -Email and Password Security and Safety
M - Mean
MDF - Managing Digital Footprint
MPS -Mobile Phone Security and Safety
OWS- Online Privacy and Wi-Fi Safety
SD - Standard Deviation
SNS - Social Networking Safety and Security
WCS - Web Conferencing Safety

References

[1] K. Mouratidis and A. Papagiannakis, "COVID-19, internet, and mobility: The rise of telework, telehealth, e-learning, and e-shopping," *Sustain. Cities Soc.*, vol. 74, no. July, p. 103182, 2021, doi: 10.1016/j.scs.2021.103182.
[2] A. Djenna, S. Harous, and D. E. Saidouni, "Internet of things meet internet of threats: New concern cyber security issues of critical cyber infrastructure," *Appl. Sci.*, vol. 11, no. 10, 2021, doi: 10.3390/app11104580.
[3] Adebimpe, Eseoghene Kupa, and Oluwatosin Ilori, "Best practices in cybersecurity for green building management systems: Protecting sustainable infrastructure from cyber threats," *Int. J. Sci. Res. Arch.*, vol. 12, no. 1, pp. 2960–2977, 2024, doi: 10.30574/ijsra.2024.12.1.1185.
[4] W. Zhao, J. Zhang, X. Liu, and Z. Jiang, "Application of ISO 26000 in digital education during COVID-19," *Ain Shams Eng. J.*, vol. 13, no. 3, p. 101630, 2022, doi: 10.1016/j.asej.2021.10.025.
[5] H. Holmarsdottir, I. Seland, and C. Hyggen, "How can we understand the everyday digital lives of children and young people?," in Understanding The Everyday Digital Lives of Children and Young People. Cham, Switzerland: Palgrave Macmillan, 2024, pp. 3–26, doi: 10.1007/978-3-031-46929-9_1.
[6] E. F. Saleh, *Adolescent Socialization in the Digital Age: The Role of Internet Usage and Social Networks*, no. April. 2024.
[7] P. Onu, A. Pradhan, and C. Mbohwa, *Potential to use metaverse for future teaching and learning*, vol. 29, no. 7. 2024.
[8] D. Bendler and M. Felderer, "Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model," *ACM Trans. Comput. Educ.*, vol. 23, no. 2, 2023, doi: 10.1145/3573205.
[9] R. K. Barbhuiya, "Cyber-Safety : Concepts , Threats , and Essential Measures," pp. 361–376, 2024.
[10] W. J. Triplett, "Addressing Cybersecurity Challenges in Education," *Int. J. STEM Educ. Sustain.*, vol. 3, no. 1, pp. 47–67, 2023, doi: 10.53889/ijses.v3i1.132.
[11] S. Thangan, T. Kaliappan, V. Vijayan, V. S. Abhinav, and A. Shanthipalla, "Designing cyber safety and security literacy programs to enhance cyber security competency of prospective teachers," *Int. J. Eval. Res. Educ.*, vol. 14, no. 5, pp. 4088–4098, 2025, doi: 10.11591/ijere.v14i5.32359.
[12] E. Gagrčin, P. Porten-Cheé, L. Leißner, M. Emmer, and L. Jørring, "What Makes a Good Citizen Online? The Emergence of Discursive Citizenship Norms in Social Media Environments," *Soc. Media Soc.*, vol. 8, no. 1, 2022, doi: 10.1177/20563051221084297.
[13] S. R. Fajri, N. Fajri, F. Sarnita, H. Fitriani, A. S. Bago, and P. Kerti, "Digital Literacy Dan Cyber Socialization In The Context Of 21st Century Education : A Systematic Review," vol. 6, no. 2, pp. 76–91, 2024, doi: 10.36733/ijassd.v6i2.9078.
[14] Y. Liu, N. Zeng, E. Papadonikolaki, K. Maritshane, and P. W. Chan, "The future of digitalized project practices through data-savvy talent: A digital competence formation perspective," *Proj. Leadersh. Soc.*, vol. 5, no. March, p. 100120, 2024, doi: 10.1016/j.plas.2024.100120.
[15] S. Hamedani, S. Aslam, B. A. Mundher Oraibi, Y. B. Wah, and S. Shahidi Hamedani, "Transitioning towards Tomorrow's Workforce: Education 5.0 in the Landscape of Society 5.0: A Systematic Literature Review," *Educ. Sci.*, vol. 14, no. 10, 2024, doi: 10.3390/educsci14101041.
[16] Y. Dragostinov *et al.*, "Preliminary psychometric scale development using the mixed methods Delphi technique," *Methods Psychol.*, vol. 7, no. November, pp. 1–10, 2022, doi: 10.1016/j.metip.2022.100103.
[17] H. D. Surdjono *et al.*, "Effectiveness of Cybersecurity Awareness Program Based on Mobile Learning to Improve Cyber Hygiene," *Int. J. Inf. Educ. Technol.*, vol. 15, no. 2, pp. 220–229, 2025, doi: 10.18178/ijiet.2025.15.2.2235.
[18] A. Prakash, "the Effectiveness of Using Social Media To Raise Cyber Safety Awareness Among the Public," no. June, 2024.
[19] M. Lan, N. Law, and Q. Pan, "Effectiveness of anti-cyberbullying educational programs: A socio-ecologically grounded systematic review and meta-analysis," *Comput. Human Behav.*, vol. 130, no. July 2021, p. 107200, 2022, doi: 10.1016/j.chb.2022.107200.
[20] N. Gcaza and K. L. Thomson, "Factors contributing to the successful development of cyber safety education for foundation phase children: a systematic literature review," *Inf. Comput. Secur.*, 2025, doi: 10.1108/ICS-07-2024-0175.

[21] M. Mukherjee, N. T. Le, Y. W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Inf.*, vol. 15, no. 2, pp. 1–23, 2024, doi: 10.3390/info15020117.
[22] A. M. Alnajim, S. Habib, M. Islam, H. S. AlRawashdeh, and M. Wasim, "Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches," *Symmetry (Basel).*, vol. 15, no. 12, 2023, doi: 10.3390/sym15122175.
[23] F. Alqurashi and I. Ahmad, "A data-driven multi-perspective approach to cybersecurity knowledge discovery through topic modelling," *Alexandria Eng. J.*, vol. 107, no. June, pp. 374–389, 2024, doi: 10.1016/j.aej.2024.07.044.
[24] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, no. September 2023, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.
[25] J. Jung, S. Choi, and M. Fanguy, "Exploring Teachers' Digital Literacy Experiences," *Int. Rev. Res. Open Distrib. Learn.*, vol. 25, no. 2, pp. 41–59, 2024, doi: 10.19173/irrodl.v25i2.7572.
[26] Ł. Tomczyk, "Digital literacy and e-learning experiences among the pre-service teachers data," *Data Br.*, vol. 32, 2020, doi: 10.1016/j.dib.2020.106052.
[27] J. Zhong and Y. Zheng, "'What It Means to be a Digital Citizen': Using concept mapping and an educational game to explore children's conceptualization of digital citizenship," *Heliyon*, vol. 9, no. 9, p. e19291, 2023, doi: 10.1016/j.heliyon.2023.e19291.
[28] M. Estellés and A. Doyle, "From safeguarding to critical digital citizenship? A systematic review of approaches to online safety education," *Rev. Educ.*, vol. 13, no. 1, 2025, doi: 10.1002/rev3.70056.
[29] C. Behera and J. P. Deb, "An Overview of Digital Literacy and Cyber Socialization in the Educational Scenario of 21st Century," Asian J. Multidiscip. Res. Rev., vol. 4, no. 2, pp. 70–79, 2023.
[30] M. Cowling, K. Nui, S. Joanne, and O. Jafar, "activities for 10 to 13 Year Old Students," pp. 941–958, 2025.
[31] J. Zhong *et al.*, "To Be Ethical and Responsible Digital Citizens or Not: A Linguistic Analysis of Cyberbullying on Social Media," *Front. Psychol.*, vol. 13, no. April, 2022, doi: 10.3389/fpsyg.2022.861823.
[32] N. F. Khan, N. Ikram, H. Murtaza, and M. Javed, "Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model," *Comput. Secur.*, vol. 125, 2023, doi: 10.1016/j.cose.2022.103049.
[33] V. B. Hinsz, "Motivating cybersecurity behaviors : a beyond reasoned action conceptualization," 2023, doi: 10.1108/OCJ-08-2023-0015.
[34] N. S. Sulaiman, M. A. Fauzi, S. Hussain, and W. Wider, "Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks," *Inf.*, vol. 13, no. 9, 2022, doi: 10.3390/info13090413.
[35] S. Chen, P. Huang, S. Deng, Y. Xie, P. Liu, and Y. Zheng, "Effects of digital game-based learning on students' digital commerce literacy and learning engagement," *Proc. - 2024 Int. Symp. Educ. Technol. ISET 2024*, pp. 463–467, 2024, doi: 10.1109/ISET61814.2024.00097.
[36] G. Towhidi and J. Pridmore, "Increasing cybersecurity interest and self-efficacy through experiential labs," *Issues Inf. Syst.*, vol. 23, no. 2, pp. 119–131, 2022, doi: 10.48009/2_iis_2022_110.
[37] N. Alsaleh, "The Effectiveness Of An Instructional Design Training Program To Enhance Teachers' Perceived Skills In Solving Educational Problems," *Educ. Res. Rev.*, vol. 15, no. 12, pp. 751–763, 2020, doi: 10.5897/ERR2020.4082.

Authors' Profiles



Santhosh Thangan presently serving as an ad-hoc faculty in the Department of Education, National Institute of Technology, Calicut, Kerala, India. He has obtained his PhD in Education from Department of Education, Central University of Kerala. He holds Master's degree in both Economics and Education. He was a recipient of University Grants Commission (UGC) Junior Research Fellowship (JRF) in education and has qualified UGC National Eligibility Test (NET) for lectureship in economics. His areas of interest are education technology, teacher training, cyber safety and security, and economics of education. He has attended several workshops and conferences in the field of education and also presented and published articles in reputed journals. He has authored two books and two manuals in the field of cyber safety and security.



Thiyagu Kaliappan is an associate professor in the Department of Education, School of Education and Training, Central University of Karnataka, Kalaburagi, India. His research interests include educational technology, pedagogy of mathematics, and research methods in education, with specializations in digital pedagogy, cyber safety, AI-powered Education, and augmented reality in education. He has authored four books and published more than fifty-five research papers in reputed journals and conference proceedings. His academic work focuses on integrating emerging technologies to enhance teaching and learning, fostering innovation in education, and promoting digital competence among educators. He actively engages in academic collaborations, seminars, and workshops.

How to cite this paper: Santhosh Thangan, Thiyagu Kaliappan, "Cyber Security Competency and Socialization among Prospective Teachers: Effect of a Cyber Safety and Security Literacy Program", International Journal of Modern Education and Computer Science(IJMECS), Vol.18, No.2, pp. 163-172, 2026. DOI:10.5815/ijmecs.2026.02.10