

Designing cyber safety and security literacy programs to enhance cyber security competency of prospective teachers

Santhosh Thangan¹, Thiyagu Kaliappan², Vrinda Vijayan³, Venukanti Sai Abhinav²,
Ashalatha Shanthipalla²

¹Department of Education, National Institute of Technology, Calicut, India

²Department of Education, School of Education and Training, Central University of Karnataka, Kalaburagi, India

³Department of Education, Central University of Kerala, Kasaragod, India

Article Info

Article history:

Received Aug 6, 2024

Revised Apr 27, 2025

Accepted May 9, 2025

Keywords:

ADDIE model

Cyber safety and security
literacy program

Cyber security competency

E safety

Online risks

ABSTRACT

This study examines the design, development, and evaluation of a cyber safety and security literacy program (CSLP) aimed at enhancing cyber security competency (CSC) among prospective teachers. Utilizing a research and development (R&D) method, the program was structured using the analysis, design, development, implementation, evaluation (ADDIE) model to create instructional modules covering key cyber safety topics. The validity of the program was ensured through expert evaluations, and its effectiveness was tested via a pre-experimental research design with a single group of 50 prospective teachers from training colleges in Kerala, India. Pre- and post-test assessments were conducted using a standardized CSC scale. Statistical analysis, including t-tests and Cohen's d, revealed a significant improvement in participants' CSC, with a large effect size (Cohen's $d=4.32$), indicating the program's substantial impact. This study emphasizes the importance of incorporating structured cyber safety education into teacher training programs to bridge the gap between digital engagement and online safety. The findings also highlight the broader need for integrating cyber security literacy in professional contexts to foster responsible digital behavior.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Santhosh Thangan

Department of Education, National Institute of Technology

Calicut, Kerala 673601, India

Email: santhoshelappully@gmail.com

1. INTRODUCTION

Cyberspace affords a wealth of services to every individual; however, it also presents significant risks and dangers. Unfortunately, many people are unaware of these risks and lack the skills needed to protect themselves. As the gap between digital use and safety grows, raising awareness becomes more critical than ever. A secure online environment demands not only awareness of potential risks but also a deep understanding of the skills and strategies required to address and mitigate these dangers [1]. Studies consistently emphasize the value of awareness programs in equipping individuals with essential cyber security skills. Well-structured programs that integrate diverse content and effective teaching methods have proven successful in addressing the challenges of the digital world, empowering individuals to guide cyberspace safely [2].

Among the key strategies for promoting cyber safety, cyber literacy plays a vital role by enhancing young people's confidence and competence in using technology safely. It extends beyond basic internet skills, encompassing information literacy, media literacy, information and communication technology (ICT) literacy, and internet literacy, all of which contribute to a broader concept of digital competence.

This competence enables individuals to use technology confidently and critically for learning, leisure, communication, and work, while also being aware of and analyzing potential risks [3], [4]. Several global frameworks, such as the UNESCO global framework of reference on digital literacy skills, the European Commission's DigComp framework, the UNESCO Media and Information Literacy (MIL) framework, and the OECD skills research framework, provide comprehensive guidelines to foster cyber safety through a range of essential digital skills. These frameworks, combined with extensive awareness materials available both online and offline, offer practical guidance on staying safe in the digital space [5].

Various organizations worldwide, including the Cyber Security Agency of Singapore, CERT India, the Central Board of Secondary Education, and the Central Institute of Education Technology in India, contribute to cyber safety education by developing interactive handbooks and booklets. Initiatives like India's Information and Security Education Awareness (ISEA) project by the Ministry of Electronics and Information Technology further support the creation of effective cyber safety and security literacy program (CSLP). These resources serve as essential tools for building a strong foundation of cyber security awareness; ensuring individuals are equipped with the knowledge and skills to navigate the online world safely.

These efforts are most impactful when integrated into formal education systems, where structured programs can be developed and implemented to ensure widespread adoption of cyber safety practices. In this context, educational institutions, especially teacher training centers, play a crucial role in shaping society's approach to cyber safety and security by promoting awareness of safe online practices. Teachers are key to this transformation, as they serve as catalysts for a broader impact of educating their students and, in turn, contributing to a safer digital environment for society as a whole. Recognizing the crucial role of teachers in promoting cyber safety, this study focuses on developing a module-based CSLP tailored specifically for prospective teachers. The central scientific questions driving this research are: i) how effective is the CSLP in enhancing cyber security competency (CSC) among future educators and ii) what specific dimensions of CSC show improvement following the implementation of the program.

These questions shape both the development and evaluation of the program, aiming to assess its validity and effectiveness in equipping teachers with the essential skills needed to foster a safer digital environment in their classrooms and beyond. The relevance of this study stems from the growing need to equip future educators with the tools and knowledge required to foster cyber safety in their classrooms. Teachers who are well-versed in cyber safety not only protect themselves but also pass on essential skills to their students, creating a multiplier effect that enhances society's overall digital resilience [6]. The study aims to address this need by developing and evaluating a tailored CSLP module for teacher education, ensuring that educators are prepared to handle the complexities of the digital world.

In spite of the increasing emphasis on cyber safety education globally, a critical gap persists in integrating structured, research-based literacy programs into teacher education curricula, particularly in the Indian context [7]. While existing literature and global frameworks provide broad guidelines on digital competence and cyber safety, few studies have focused on contextualizing these frameworks for future educators in developing countries [8], [9]. Moreover, there is limited empirical research assessing the impact of module-based interventions tailored specifically to enhance CSC among prospective teachers [10]. This research seeks to bridge that gap by designing, implementing, and evaluating a CSLP that is pedagogically grounded, contextually relevant, and empirically tested for effectiveness [9]. The novelty of this study lies in contextualizing global digital competence frameworks into a module-based program for Indian prospective teachers and validating its effectiveness through rigorous pre-post analysis. By focusing on future educators, this study contributes to the literature by providing a scalable model that can be integrated into teacher training institutions, thereby fostering a culture of digital safety from the classroom outward.

2. METHOD

This study adopted a systematic approach to the design, development, and evaluation of a CSLP specifically aimed at prospective teachers. The program was developed using research and development (R&D) method and it further integrated analysis, design, development, implementation, evaluation (ADDIE) model in the design and development of instructional design to ensure a comprehensive, structured process [11]. Each module was crafted to address essential cyber security competencies, with the content tailored to meet the unique needs of teacher education. The validity of the program was confirmed through expert evaluation by three validators, who provided critical feedback on the accuracy, relevance, and structure of the modules. To evaluate the effectiveness of the CSLP in enhancing the CSC of prospective teachers, a pre-experimental research design was employed. A single group of 50 prospective teachers of various training colleges in Kerala, a state in India was assessed using a standardized CSC scale both before and after the intervention. The effectiveness of the program was determined by comparing the mean scores from the pre-test and post-test, highlighting the extent of improvement in participants' cyber security competencies.

The research procedure for designing and evaluating the effectiveness of the CSLP, aimed at enhancing the CSC of prospective teachers, is depicted in Figure 1.

Figure 1 outlines the key stages involved in the creation and assessment of a CSLP targeted at prospective teachers. The process begins with a thorough review of existing literature to determine suitable content. A structured program is then developed to enhance CSC. Reliable assessment tools are constructed to measure the program's impact. Expert validation ensures the content meets academic and practical standards. The final step involves pre- and post-intervention testing to evaluate the program's effectiveness through statistical analysis.

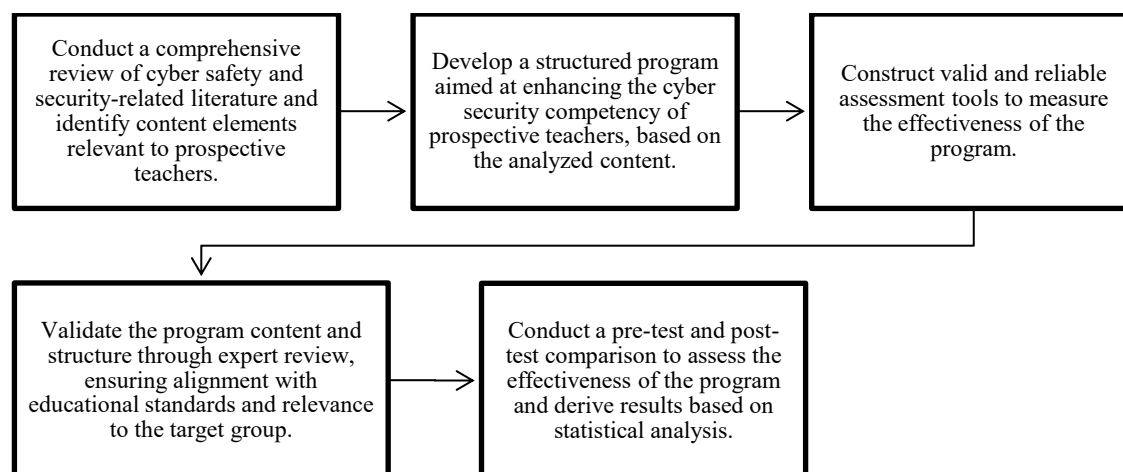


Figure 1. Research procedure adopted

2.1. Construction and development of modules

The development of the CSLP modules was carried out through a structured and phased approach. Each phase focused on aligning content with instructional goals, ensuring relevance to teacher education. Table 1 presents the general phases followed in the development process.

Table 1. General phases of the development of the program

Phases	Description
1	Identification and selection of topics of cyber safety and security literacy <ul style="list-style-type: none"> – Based on anticipated objectives and aims – Based on assumptions – Based on the core areas of cyber safety and security for teachers
2	Design and implementation <ul style="list-style-type: none"> – Theoretical considerations in terms of instructional strategy – Structuring the lesson transcript – Plan for implementation
3	Evaluation

2.1.1. Phase 1: identification and selection of cyber safety and security literacy topics

The CSLP was designed to enhance the digital preparedness of prospective teachers by raising awareness of cyber risks, linking knowledge to real life digital experiences, and fostering responsible online behavior. It also aimed to promote positive cyber socialization, etiquette and long-term technological awareness for safe digital engagement. The program was built on key assumptions to ensure its validity and relevance [12]. It was presumed that prospective teachers generally lack a clear conceptual understanding of cyber threats, and that generational differences contribute to varying perceptions of digital spaces. Furthermore, the program emphasized that active and informed participation in digital environments is essential for cultivating digital literacy, a key foundation for promoting cyber safety awareness and behavior [13].

With these guiding objectives and clear assumptions, a thorough literature review was conducted to identify the essential areas of cyber safety and security relevant to teachers. This review focused on communication security, information decency, online interpersonal safety, and safe computer/internet usage

[14]. Based on these insights, the final topics for the CSLP were determined, encompassing the major aspect CSC. Table 2 shows the summary of topics and its corresponding modules.

Table 2. Topics and its corresponding modules

No	Topics selected	Modules
1	Social networking safety and security (SNS)	4
2	Dealing with fake information (DWF)	4
3	Mobile phone security and safety (MPS)	4
4	Email and password security and safety (ELS)	8
5	Managing digital footprint (MDF)	4
6	Online privacy and Wi-Fi safety (OWS)	7
7	Apps safety and security (APS)	3
8	Web conferencing safety (WCS)	4
9	Digital learning resource safety and plagiarism and copyright infringement (DRS)	6

2.1.2. Phase 2: design and implementation of the program

An effective literacy plan ensures the active participation of all its target audience. For this extensive step by step plan is created it is for design and implementation. This phase includes three sub phases, namely: i) integration ADDIE model strategy in the module development; ii) structuring the lesson transcript; and iii) plan for implementation.

a. Integration ADDIE model strategy in the module development

The fundamental tenet of ADDIE is that all activities are designed to assist learners in gaining knowledge within a specific learning environment [15]. In creating CSLP for prospective teachers, the main phases of the ADDIE were meticulously integrated. The detailed descriptions are shown in Table 3.

Table 3. Utilization of ADDIE model in the program

Stages	Concerns addressed
Analysis	Background of the target audience and the existing competency in relation to the topics of cyber safety and security. Goals to be achieved at the end of the program.
Design	Preparations of the learning materials. The methodology and strategy of the program for its smooth delivery.
Developing	The approaches for testing the outcome of the program. Contents and resources for integrating with the program. Validating those contents with learning outcomes.
Implementation	Revising and updating the contents for implementation. The learning experience to the targeted audience.
Evaluation	Preparing the learners participation and gathering constant feedback from the learners. The quality of the whole instruction (including learning resources and accomplishment of learning outcome) through different summative and formative evaluation.

b. Structuring the lesson transcript

On the basis of this key components and concerns addressed by each aspect in the ADDIE model a lesson transcript template was designed with a sequence of activities and with required materials [16]. Blooms taxonomy of lesson planning is followed for the design of the lesson transcript. The whole lesson plan templates were operating under three sequential stages: preparatory, delivery, and evaluation. It was shown in Figure 2. In the preparatory stage, educational objectives were formulated, providing a foundation for the program. The delivery stage created a dynamic learning experience through activities such as discussions, demonstrations, and problem-solving, supported by various communication channels (emails, videos, and social media) and learning resources (concept notes, posters). Finally, the evaluation stage assessed behavioral changes in participants using online quizzes, measuring their CSC and the overall effectiveness of the program. These phases are represented in the lesson transcript to guide structured and effective implementation.

On the basis of the sequential stages the investigators prepared the design for the cyber safety and security literacy module lesson transcripts. Each lesson transcript has similar sections, and the contents are presented in specific manner based on the objectives. All lesson transcripts consist of discussion and activity as a core section because all kinds of cyber dangers deserve broad debate. To guarantee objectivity of the program a few additional resources were prepared by the investigators. It includes a google site (<https://sites.google.com/view/cyberspacesafety/about>) and a textbook comprising the topics which are closely related to the cyber safety and security concepts. These additional resources acted as an information repository

of the CSLP program. Moreover, for the ease of convenience the nine topics of cyber safety and security were further separated into 12 topics. Figure 3 presents the sample templates of the lesson transcripts.

c. Plan for implementation

The program considers itself as an awareness initiative. After designing the lesson transcripts, a specific plan for implementation was created focusing on actual delivery of the program to the targeted audience. The plan for implementation was based on two fundamental pillars: prior approval from academic stakeholders and an adequate institutional climate.

2.1.3. Phase 3: evaluation of the program

To evaluate the efficacy of CSLP modules for prospective teachers a validity analysis carried out from the various stakeholders of this area. Computer science teachers, training college teacher's cyber-security professionals were in the expert group. For this two data analysis techniques were used: quantitative and qualitative descriptive. Qualitative data was analyzed by collecting comments and suggestions from expert validators. Quantitative data was analyzed by calculating the percentage score from filling out the validation questionnaire sheet [17]. Further to evaluate validity response of the different expert groups, a systematic approach is used involving the calculation of average scores and setting a benchmark for comparison. First, the scores from each validator for a particular group of experts are collected. These scores are then summed up and divided by the number of scores to calculate the average score for each group. A benchmark score of 3.30 is established to categorize the performance: if the average score meets or exceeds this benchmark, the validity is deemed "good"; otherwise, it would be considered "needs improvement." The validation criteria include: i) understanding of cyber safety concepts; ii) application of cyber safety practices; iii) creative thinking strategies; iv) learners initiation; v) orientation towards expected outcome of CSLP; and vi) organization and structure of the program.

The expert validation results of CSLP module, as presented in Table 4, reveal a commendable level of agreement among various experts. Computer science teachers, cyber security professionals, and training college teachers all contributed their evaluations, resulting in an overall positive assessment. Computer science teachers provided an average score of 3.33, while cyber security professionals offered a slightly higher average of 3.41. Notably, training college teachers rated the module the highest, with an average score of 3.40. Each group's scores were categorized as 'good,' reflecting a high degree of satisfaction. These results not only affirm the module's efficacy but also demonstrate its broad applicability in providing awareness on cyber security competencies.

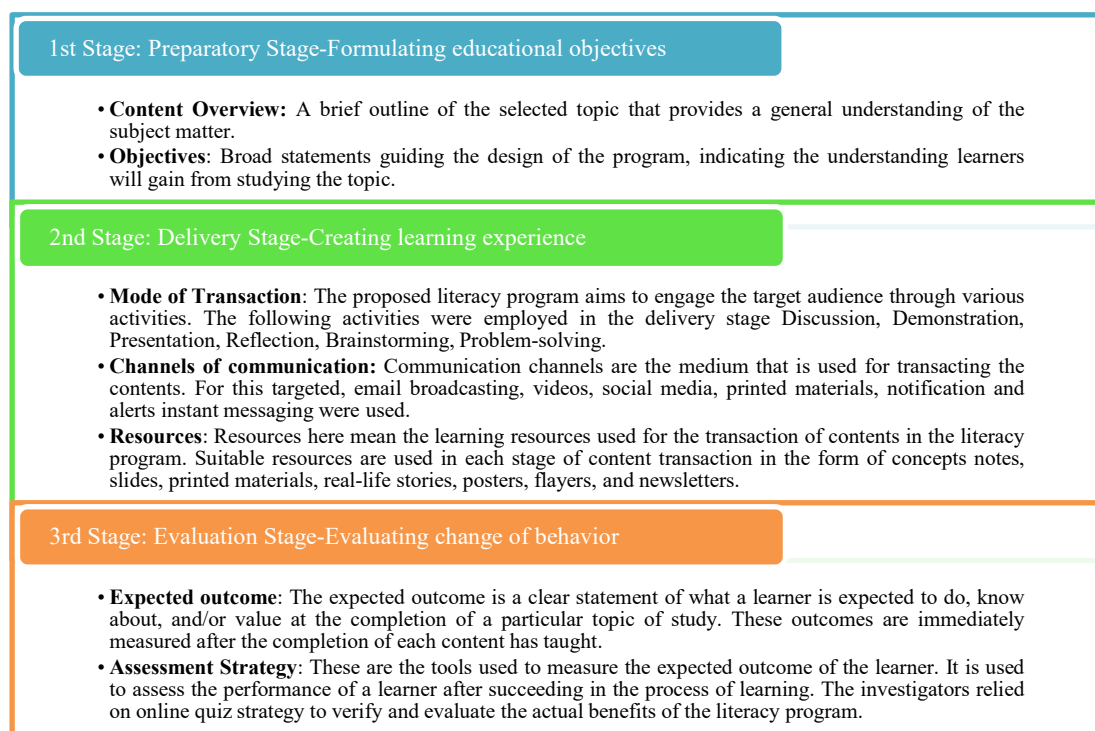


Figure 2. Stages in the lesson transcript


Password Safety and Security		
Topic 1: Introduction to Password Safety and Security	Targeted Audience	Duration
	B Ed Trainees	40 minutes
Learning Objectives		
<ul style="list-style-type: none">• Cognize the concept of password security.• Understand the need of password security.		
Resources	Content Overview	
<ul style="list-style-type: none">• Concept note on Password Security.	<p>A password is a basic security mechanism which is made up of a secret pass phrase that can be generated by combining alphabetic, numeric, alphanumeric, and symbolic elements. A password is used to restrict access to a system, application or service to only those users who have memorized or stored and/or are authorized to use it. A password may also be called an access code, PIN or secret code.</p>	
References		
<p>https://www.techopedia.com/definition/8797/password-protection</p> <p>https://www.computerhope.com/jargon/p/password.html</p>		
Let's Discuss		
<ul style="list-style-type: none">• Did you create passwords for any of your accounts in cyber space?• Discuss the functions of password?• Why password security is essential?		
Activity (Online/Offline)		
<ul style="list-style-type: none">• Directions: Read and reflect the concept note on password security.		
Summary		
<ul style="list-style-type: none">• A password may also be called an access code, PIN or secret code.• Online activities provide rooms for creating passwords and pin.• Password security is an important concern in the present day context.		
Self-Reflection / Evaluation		
<ul style="list-style-type: none">• Will be able to cognize the concept of password safety and security.• Attempt a quiz on password safety.		

Figure 3. Sample lesson transcript

Table 4. Results of validation

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

2.2. Effectiveness of module based CSLP in augmenting cyber security competency

To evaluate the effectiveness of the module-based CSLP, the experimental group was assessed twice: once prior to the intervention and again post-intervention, with no control group for comparison. A CSC scale, consisting of 93 items (79 positive and 14 negative statements), was used for this purpose. A 3-point scoring system was applied, with separate scoring methods for positive and negative items. Following a pilot study, the scale was refined to 78 items (72 positive and 6 negative), covering nine dimensions of CSC. It was retained for final validation process. The topic wise break up of number items in the scale as shown in Table 5.

The reliability of the scale was determined by calculating the value of Cronbach's alpha and split-half correlation coefficient of the revised scale. Reliability analysis demonstrated strong results, with a Cronbach's alpha of .906 and a split-half correlation coefficient of .851, indicating high internal consistency and reliability. To further validate the scale, the investigators conducted confirmatory factor analysis (CFA) to assess its construct validity. The results showed a strong model fit, with a Chi-square test (χ^2) value of 145.72 ($p=.196$), indicating statistical significance. Additionally, key fit indices, including a comparative fit index (CFI) of .945, a Tucker–Lewis Index (TLI) of .927, and a root mean square error of approximation (RMSEA) of .067, confirmed the scale's validity. These metrics collectively indicate that the scale is both reliable and highly effective in measuring CSC among prospective teachers.

Table 5. Dimension wise break up of items in the scale

No	Topics	Final number of items	Positive	Negative
1	Social networking safety and security	9	9	0
2	Dealing with fake information	8	6	2
3	Mobile phone security and safety	10	9	1
4	Email and password security and safety	8	8	0
5	Managing digital footprint	8	7	1
6	Online privacy and Wi-Fi safety	8	7	1
7	Apps safety and security	10	10	0
8	Web conferencing safety	7	6	1
9	Digital learning resource safety and plagiarism and copyright infringement	10	10	0
	Total	78	72	6

3. RESULTS AND DISCUSSION

The results of the pre-test and post-test were analyzed using both independent sample t-tests and paired-sample t-tests to examine the effect of CSLP on CSC of prospective teachers. Additionally, Cohen's d was calculated to measure the effect size of the program's impact. All statistical analyses were performed using SPSS 23.0 software. The data from the pre-test and post-test scores are summarized in Table 6, which shows a substantial increase in the participants' competency levels following the intervention.

Table 6. Mean comparison CSC

Component	Pre-test		Post-test		t(49)	p	r	Cohen's d
	M ₁	SD ₁	M ₂	SD ₂				
CSC	91.22	13.55	127.66	8.07	30.55	.00	.81**	4.32

N=50; **Significant at 0.01 level

Table 6 highlights the significant difference between the mean scores of CSC before and after the intervention. The pre-test mean score (M₁=91.22, SD₁=13.55) significantly increased to a post-test mean score (M₂=127.66, SD₂=8.07) after the CSLP intervention. The results of the t-test [t(49)=30.55, p<.01] confirm that this increase is statistically significant, indicating that the CSLP had a strong positive impact on the participants' CSC. Moreover, the high correlation (r=.81, p<.01) between the pre- and post-test scores suggests a consistent pattern of improvement across participants. The Cohen's d value of 4.32, which is well above the threshold of .80, demonstrates a very large effect size, confirming that the CSLP modules had a substantial and meaningful impact on improving the cyber security skills of prospective teachers.

Table 7 reveals the mean comparison of pre and post test scores of CSC components. All nine components of CSC showed statistically significant improvement from pre-test to post-test scores, indicating the effectiveness of the CSLP in enhancing the cyber security awareness and practices of prospective teachers. For social networking safety (SNS), the mean score increased from 11.68 (SD=1.67) to 15.70 (SD=1.47), with t(49)=18.88, r=.54, and Cohen's d=2.67. Dealing with fake information (DWF) also showed a rise from 9.36 (SD=2.45) to 13.02 (SD=1.59), t(49)=13.45, r=.62, d=1.90. Mobile phone security (MPS) scores improved from 11.50 (SD=2.63) to 15.60 (SD=1.89), with t(49)=12.92, r=.55, and d=1.83. In the case of managing digital footprint (MDF), the scores rose significantly from 8.48 (SD=2.30) to 13.08 (SD=1.66), t(49)=19.81, r=.70, d=2.80. Online privacy and Wi-Fi safety (OWS) increased from 11.44 (SD=1.76) to 14.36 (SD=.74), t(49)=13.55, r=.51, d=1.92. Application safety (APS) showed marked improvement from 11.66 (SD=1.76) to 16.00 (SD=1.94), with t(49)=22.49, r=.74, d=3.18. Web conferencing safety (WCS) rose from 7.58 (SD=2.36) to 11.74 (SD=1.33), t(49)=15.66, r=.61, d=2.22. Digital learning resources safety (DRS) scores increased from 10.56 (SD=2.95) to 15.22 (SD=2.17), t(49)=18.75, r=.80, d=2.65. Finally, email safety (ELS) improved from 8.96 (SD=2.50) to 13.06 (SD=1.63), with t(49)=13.79, r=.55, and d=1.95. All the results were statistically significant at p<.01, and the large effect sizes across all domains reflect the substantial impact of the program on enhancing the CSC of prospective teachers.

The findings of this study offer compelling evidence on the efficacy of module-CSLPs in significantly enhancing the cyber security competencies of prospective teachers. The statistically significant improvement in mean scores, coupled with large effect sizes, highlights the transformative potential of structured and pedagogically sound literacy programs in bridging the gap between digital engagement and responsible online behavior. These results affirm and extend previous research suggesting that comprehensive, well-targeted training interventions can meaningfully elevate awareness, understanding, and practice of cyber safety [18], [19]. A critical differentiating strength of this study lies in its component-wise analysis, which provides a deeper and more nuanced insight into the specific domains of cyber security competence impacted by the

CSLP. Unlike many existing studies that offer only aggregated measures of program effectiveness, this research identifies distinct gains across various components: SNS (Cohen's $d=2.67$), DWF (1.90), MPS (1.83), MDF (2.80), OWS (1.92), APS (3.18), WCS (2.22), DRS (2.65), and ELS (1.95). These substantial effect sizes provide concrete evidence of the program's holistic impact. Additionally, the strong correlations between pre- and post-test scores ($r=.51$ to $.81$) further establish the reliability and internal consistency of the results [20].

Table 7. Mean comparison of CSC components

CSC components	Pre-test		Post-test		t (49)	p	r	Cohen's d
	M ₁	SD ₁	M ₂	SD ₂				
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

Another unique contribution of this study is its application of the ADDIE instructional design model in the development of the CSLP. While many earlier interventions lack a systematic instructional design framework, this study's adherence to the ADDIE model ensures that the program is both structured and learner-centered. The use of this validated model contributes to creating engaging, responsive, and outcome-oriented learning experiences, which directly influence learners' competency development. This approach aligns with instructional design research advocating for structured planning to optimize learning outcomes [21], [22].

Meanwhile, the breadth and relevance of content covered in the CSLP is another defining feature that amplifies its practical utility. Addressing a wide spectrum of themes from password safety and digital footprints to application and email security, the CSLP reflects a holistic understanding of cyber safety as a multifaceted competence. This comprehensive approach empowers prospective teachers not just to protect themselves in digital environments but also to effectively educate and influence their future students toward safer digital practices. Such integration of cyber ethics and safety into teacher education holds transformative potential, as it instills a culture of cyber responsibility from the classroom outward [23], [24]. Furthermore, this study emphasizes the critical role of teachers as digital role models and catalysts for behavioral change. The improved competencies observed among participants suggest that empowering future educators with digital literacy is essential in cultivating cyber-aware learning environments. It also emphasizes the need for continuous professional development and recurrent interventions to keep pace with the evolving nature of cyber threats and technologies. This proactive stance supports the development of lifelong learning mindsets among educators, a crucial requirement in the context of 21st-century education [25], [26].

On a broader level, the implications of this research extend beyond teacher education. The findings reaffirm the growing need for context-specific cyber security education across diverse professional settings. As digital tools become ubiquitous, embedding CSLPs within educational and workplace curricula becomes not just relevant but essential. Such initiatives help mitigate vulnerabilities, reduce risks, and promote a culture of cyber resilience and responsible digital citizenship [27]–[30].

4. CONCLUSION

This study highlights the transformative impact of the CSLP in equipping prospective teachers with essential competencies to navigate and thrive in an increasingly digital world. Grounded in the ADDIE instructional design model and validated through a rigorous pre-experimental research design, the CSLP proved to be both pedagogically robust and practically impactful. The statistically significant improvements observed across all measured domain ranging from mobile safety and email security to digital footprint management and web conferencing protocols targets the program's holistic approach and learner-centered focus. By enhancing the CSC of prospective teachers, the CSLP not only prepares them to act as digitally responsible educators but also empowers them to serve as role models for promoting safer digital practices among students. These ripple effects have the potential to foster a culture of cyber awareness and resilience across educational institutions and communities.

The study advocates for the integration of structured, context-specific cyber safety education into teacher preparation programs not as an optional addition, but as a foundational element of professional

training. Furthermore, mainstreaming such programs across diverse sectors can address the growing digital skill gap and contribute to building a safer, more informed digital society. In an era of rapidly evolving cyber threats, continuous, scalable, and adaptive interventions like the CSLP are essential. Introducing such initiatives within broader professional development frameworks will be crucial for safeguarding individuals and institutions, ensuring that education remain a key force in cultivating cyber-aware, ethically sound, and digitally resilient citizens for the 21st century.

FUNDING INFORMATION

No funding source is involved in this study.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Santhosh Thangan	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				
Thiyagu Kaliappan	✓	✓	✓	✓	✓			✓	✓	✓	✓	✓	✓	
Vrinda Vijayan		✓			✓		✓		✓	✓		✓	✓	
Venukanti Sai Abhinav		✓			✓				✓	✓				
Ashalatha Shanthipalla		✓			✓		✓		✓	✓				

C : Conceptualization

M : Methodology

So : Software

Va : Validation

Fo : Formal analysis

I : Investigation

R : Resources

D : Data Curation

O : Writing - Original Draft

E : Writing - Review & Editing

Vi : Visualization

Su : Supervision

P : Project administration

Fu : Funding acquisition

CONFLICT OF INTEREST STATEMENT

Authors have no conflict of interest

INFORMED CONSENT

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

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author [ST], upon reasonable request.




REFERENCES

- [1] R. A. M. Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, pp. 1–18, 2020, doi: 10.1186/s42400-020-00050-w.
- [2] S. Sudarman and A. Ardian, "The Development of Interactive Module To Support Student Centered Learning," *Akademika*, vol. 10, no. 1, pp. 77–92, 2021, doi: 10.34005/akademika.v10i01.1344.
- [3] L. Kajee, "Digital Literacy: a Critical Framework for Digital Literacy Practices in Classrooms," in *EDULEARN16 Proceedings*, 2016, pp. 6380–6385, doi: 10.21125/edulearn.2016.0374.
- [4] L. Pan, S. ul Haq, X. Shi, and M. Nadeem, "The Impact of Digital Competence and Personal Innovativeness on the Learning Behavior of Students: Exploring the Moderating Role of Digitalization in Higher Education Quality," *SAGE Open*, vol. 14, no. 3, pp. 1–19, 2024, doi: 10.1177/21582440241265919.
- [5] K. Walsh *et al.*, "Best Practice Framework for Online Safety Education: Results from a rapid review of the international literature, expert review, and stakeholder consultation," *International Journal of Child-Computer Interaction*, vol. 33, p. 100474, 2022, doi: 10.1016/j.ijcci.2022.100474.
- [6] O. S. Ahmed, S. A. Nasef, A. Z. Al Rawashdeh, and M. E. Eltahir, "Teacher's awareness to develop student cyber security: A Case Study," *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, vol. 12, no. 10, pp. 5148–5156, 2021, doi: 10.17762/turcomat.v12i10.5297.
- [7] S. S. Bajwa, "Need of Media Information Literacy in Cyber Crime," *International Journal of Science and Research (IJSR)*, vol. 12, no. 6, pp. 2605–2608, 2023, doi: 10.21275/sr23625205508.





- [8] H. Tinmaz, Y. T. Lee, M. F. Ivanovici, and H. Baber, "A systematic review on digital literacy," *Smart Learning Environments*, vol. 9, no. 21, pp. 2–18, 2022, doi: 10.1186/s40561-022-00204-y.
- [9] D. Bendler and M. Felderer, "Competency Models for Information Security and Cybersecurity Professionals: Analysis of Existing Work and a New Model," *ACM Transactions on Computing Education*, vol. 23, no. 2, pp. 1–33, 2023, doi: 10.1145/3573205.
- [10] M. Mukherjee, N. T. Le, Y. W. Chow, and W. Susilo, "Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes," *Information*, vol. 15, no. 2, p. 117, 2024, doi: 10.3390/info15020117.
- [11] R. Luo, J. Li, X. Zhang, D. Tian, and Y. Zhang, "Effects of applying blended learning based on the ADDIE model in nursing staff training on improving theoretical and practical operational aspects," *Frontiers in Medicine*, vol. 11, p. 1413032, Jun, 2024, doi: 10.3389/fmed.2024.1413032.
- [12] V. A. Kolupaev, "Conditions and assumptions of strength criteria," *Advanced Structured Materials*, vol. 86, pp. 151–158, 2018, doi: 10.1007/978-3-319-73049-3_8.
- [13] H. Jo and H. Y. Ahn, "Understanding digital engagement: factors influencing awareness and satisfaction of digital transformation," *Discover Computing*, vol. 27, no. 1, p. 23, 2024, doi: 10.1007/s10791-024-09455-4.
- [14] A. Kaban, "Secure Internet Use in Information Technologies and Software Course Textbooks at Primary and Secondary Schools," *Athens Journal of Education*, vol. 8, no. 1, pp. 37–52, Jan. 2020, doi: 10.30958/aje.8-1-3.
- [15] N. A. Khairunnisa, M. A. Rahman, and C. Handrianto, "English Digital Literacy Practices Inside and Outside Class to Develop Students' Speaking Skills," *Pedagogy: Journal of English Language Teaching*, vol. 10, no. 1, 2022, doi: 10.32332/joelt.v10i1.3790.
- [16] A. G. Spatioti and I. Kazanidis, "A Comparative Study of the ADDIE Instructional Design Model in Distance Education," *Information*, vol. 13, no. 9, p. 402, 2022, doi: 10.3390/info13090402.
- [17] A. Aithal and P. S. Aithal, "Development and Validation of Survey Questionnaire & Experimental Data – A Systematical Review-based Statistical Approach," *International Journal of Management, Technology, and Social Sciences (IJMTS)*, vol. 5, no. 2, pp. 233–251, 2020, doi: 10.47992/ijmts.2581.6012.0116.
- [18] L. Tomczyk and L. Eger, "Online safety as a new component of digital literacy for young people," *Integration of Education*, vol. 24, no. 2, pp. 172–184, 2020, doi: 10.15507/1991-9468.099.024.202002.172-184.
- [19] M. Elrayah and S. Jamil, "Impact of Digital Literacy and Online Privacy Concerns on Cybersecurity Behaviour: The Moderating Role of Cybersecurity Awareness," *International Journal of Cyber Criminology*, vol. 17, no. 2, pp. 166–187, 2023, doi: 10.5281/zenodo.4766711.
- [20] H. Gaffney, M. M. Tfofi, and D. P. Farrington, "Effectiveness of school-based programs to reduce bullying perpetration and victimization: An updated systematic review and meta-analysis," *Campbell Systematic Reviews*, vol. 17, no. 2, p. e1143, 2021, doi: 10.1002/c12.1143.
- [21] S. Boateng, G. K. Gilbert, and C. Duedu, "Augmenting Academic Efficiency: The Integration of Assessments Within the Addie Model for Pedagogical Development," in *Proceedings of The International Conference on Advanced Research in Education, Teaching, and Learning*, 2024, pp. 1–12, doi: 10.33422/aretl.v1i1.186.
- [22] S. Chaudhary, V. Gkioulos, and S. Katsikas, "Developing metrics to assess the effectiveness of cybersecurity awareness program," *Journal of Cybersecurity*, vol. 8, no. 1, pp. 1–19, 2022, doi: 10.1093/cybsec/tyac006.
- [23] B. T. Zahed, G. White, and J. Quarles, "Play it safe: An educational cyber safety game for children in elementary school," in *2019 11th International Conference on Virtual Worlds and Games for Serious Applications (VS-Games)*, 2019, pp. 1–4, doi: 10.1109/VS-Games.2019.8864594.
- [24] I. M. Venter, R. J. Blignaut, K. Renaud, and M. A. Venter, "Cyber security education is as essential as 'the three R's'," *Heliyon*, vol. 5, no. 12, p. e02855, Dec. 2019, doi: 10.1016/J.HELIYON.2019.E02855.
- [25] S. N. S. Nasir, "Exploring the Effectiveness of Cybersecurity Training Programs: Factors, Best Practices, and Future Directions," *Advances in Multidisciplinary and Scientific Research Journal Publication*, vol. 2, no. 1, pp. 151–160, 2023, doi: 10.22624/aims/csean-smart2023p18.
- [26] H. AbdulRab, "Teacher Professional Development in the 21st Century," *African Journal of Education and Practice*, vol. 9, no. 4, pp. 39–50, 2023, doi: 10.47604/ajep.2237.
- [27] S. R. Fajri, N. Fajri, F. Sarnita, H. Fitriani, A. S. Bago, and P. Kerti, "Digital Literacy and Cyber Socialization In The Context Of 21st Century Education: A Systematic Review," *International Journal of Applied Science and Sustainable Development (IJASSD)*, vol. 6, no. 2, pp. 76–91, 2024, doi: 10.36733/ijassd.v6i2.9078.
- [28] E. Kovatcheva, W. Dimitrov, M. Koleva, I. Kostadinova, and I. Getova, "Competency in Nuggets for Cyber Security Trainings," in *EDULEARN19 Proceedings*, 2019, pp. 4311–4318, doi: 10.21125/edulearn.2019.1086.
- [29] R. V. R. Hernández and C. M. J. Ibarra, "Awareness and Training to Increase Cyber-Security in University Students," *PAAKAT: Revista de Tecnología y Sociedad*, vol. 8, no. 14, pp. 1–13, 2018, doi: 10.32870/pk.a8n14.318.
- [30] N. Kurniasih, "Digital Literacy: Education for Safe Internet Usage," *Engagement: Jurnal Pengabdian Kepada Masyarakat*, vol. 7, no. 1, pp. 139–150, 2023, doi: 10.29062/engagement.v7i1.1534.

BIOGRAPHIES OF AUTHORS







Santhosh Thangan    is presently serving as an ad-hoc faculty in the Department of Education, National Institute of Technology, Calicut Kerala, India. He obtained his Ph.D. in Education from the Central University of Kerala. He holds master's degrees in both Economics and Education. He is a recipient of the UGC Junior Research Fellowship (JRF) in Education and has qualified the UGC National Eligibility Test (NET) for Lectureship in Economics in India. 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 several journals. He has authored 4 books in the field of cyber safety and security. He can be contacted at email: santhoshelappully@gmail.com.







Thiyaagu Kaliappan     is currently working as an associate professor in the Department of Education, School of Education and Training, Central University of Karnataka, Kalaburagi, India. He holds qualifications of M.Sc., M.Ed., M.Phil., and Ph.D. His primary research interests include educational technology, mathematics teaching methodologies, and research methods in education. Relating to his research areas, he has authored and published four books and more than 55 research articles in reputed journals and conference proceedings. He can be contacted at email: thiyagusuri@gmail.com.







Vrinda Vijayan     is assistant professor (Mathematics) and former ICSSR post-doctoral fellow as well as UGC research scholar in the Department of Education, Central University of Kerala. She has master's degree in both Education and Mathematics. She has published articles in peer-reviewed, UGC-CARE listed and Scopus-indexed journals. She has presented papers in the National and International Seminars. Her areas of expertise include mathematics education, instructional technology, and research statistics. She can be contacted at email: drvindarun@gmail.com.



Venukanti Sai Abhinav     is working as an assistant professor in Department of Education, School of Education and Training Central University of Karnataka, India. He has Ph.D. in Physical Education and M.PEd. He has 7 years of experience in teaching and coaching, proficient in sports sciences and physical education. He has published articles in many peer reviewed journals. His areas of expertise are innovative teaching methods, research in sports training and health education, fitness and wellbeing, and sports sciences. He can be contacted at email: saiabhinav@cuk.ac.in.



Ashalatha Shanthipalla     is currently working as an assistant professor in the Department of Education, Central University of Karnataka. She has a Ph.D. in Education. She has postgraduate degrees in education, psychology, history, and social work. Her contributions are primarily in the areas of open educational resources and teacher education. She has published multiple peer review articles and book chapters on educational technology, pedagogy, and Indian education system. She can be contacted at email: sashalatha@cuk.ac.in.