




Research Article

Development and validation of cyber security competency scale for prospective teachers

Santhosh T and Thiyagu K

Central University of Kerala, India

Correspondence should be addressed to Santhosh T  santhoshelappully@gmail.com
Received 2 May 2024; Revised 24 June 2024; Accepted 12 July 2024

The aim of this study is to develop cyber security competency scale to measure the security competency of prospective teachers in relation to the educational environment. It included 100 participants from various teacher training colleges of Kerala, a state in India. This tool development was a part of research conducted to examine the impact of a cyber-safety and security awareness program. Initially 113 items related with the security aspect of prospective teachers in the educational environment framed. Later on, 21 items were modified and 13 were deleted as per opinions of the experts. The draft scale consisting of 93 items was administered on samples and data was collected with the help of Google forms. Item analysis was carried out using t-value and r-value. Reliability of scale was determined by using Cronbach Alpha value and split-half correlation. After item analysis, the scale items were reduced to 78 items organized under 12 essential aspects of cyber security in educational environment. To obtain further validity confirmatory factor analysis also carried out. Analyses of the entire psychometric scale have demonstrated its validity and reliability, confirming its suitability for measuring the cybersecurity competency of prospective teachers.

Keywords: Confirmatory factor analysis, Cronbach alpha, cyber safety, cyber security competency

1. Introduction

In an era where digital literacy and cyber competence are integral components of modern education, the role of prospective teachers in fostering cyber security awareness among students is increasingly paramount. With the increasing integration of technology in educational settings, the dangers posed by cyber space are also on the rise, underscoring the critical importance of educators possessing the necessary skills and knowledge to tackle these issues efficiently. The implementation of a standardized metric is crucial in this regard. In order to fulfill this objective, the present study is an attempt to develop and standardize a cyber-security competency scale. The scale is tailored specifically for prospective teachers with an intend of enhancing cyber security competency in their educational environment. By offering this standardized metric, the CSS helps aspiring educators assess their ability to effectively manage cyber dangers and recognize their resilience and cyber security awareness. It also helps them in analyzing the invaluable skills they possess in the digital world.

1.1. Cyber Security Competency-An Overview

Cyber security necessitates synchronized efforts across various domains, including technology, law, organization, procedures, and society, making it an interdisciplinary concern. When it comes to the educational environment it focuses mainly on the up skilling [the] new generation with respect cyber threats. The European Union Agency for Cyber security [ENISA] emphasizes that increasing the level of skills and knowledge is an indispensable element in building society's resilience to cyberspace threats (e.g., ENISA, 2017). Enhancing skills in this field is a common goal for numerous nations and global entities. Additionally, there has been a rising focus on cyber hygiene and cyber citizenship in the past few years, aiming to prevent a multitude of security breaches (Szczeplaniuk & Szczeplaniuk, 2022). Assuming that having the necessary competences is

crucial to maintaining cyber security and that ignorance or a lack of training might increase the likelihood of cyber-attacks. Enhancing abilities is crucial in reducing the likelihood of potential hazards. Many security mishaps can be prevented by promoting cyber hygiene concepts. Therefore, understanding and assessing cyber security competency is crucial to bringing about meaningful change in any cyber-savvy culture.

Cyber security competencies are a set of skills, knowledge, and attitude that involves confident, creative, and critical use of technologies for work, leisure, and communication. These are the knowledge of individuals to protect themselves in cyberspace. In other words cyber safety and security competency involves combination of information skills, communication skills, content creation skills, safety skills, and problem solving skills (Ferrari, 2012).

US National Initiative of Cyber Security Education (NICE) defines the cyber security competency as the skills and knowledge requirements needed by individuals whose activities impact the security of the cyberspace (McDuffie, 2017). More clearly, these are the knowledge of individuals to protect themselves in cyberspace, it involves safe and responsible utilization of technology in various aspects of life, including work, leisure, and communication.

Similarly, the UNESCO ICT Competency Framework for Teachers [ICT CFT] Version 3 (2018) incorporates the need for understanding and demonstrating the basic principles and good practices of cyber security, media and information literacy for ensuring safe use of social media and mobile devices. Moreover, exploring different ways for increasing cyber security competencies among teachers and to adapt to the new challenges becomes the priority concerns of several countries.

To attain an advance level cyber maturity, measuring the level of cyber competency is essential. For this, an instrument named cyber security scale was proposed to construct.

1.2. Cyber Security Competency and Prospective Teachers

The rapid increases in cyber related crimes in the recent years and the inadequate knowledge among individuals to maintain appropriate cyber safety behavior to respond cyber-attacks become a serious concern in the present day circumstances (Yaokumah, 2019). The only solution to cure this concern is bringing a transformation among individuals who can deal with cyber-attacks (Yaokumah, 2019). This transformative change demands the determination of competency areas and their contents (Lehto, 2016). Considering the pivotal position of educational institutions especially teacher training centers in transforming society's cyber safety and security culture by providing awareness on safe internet practices, the potential responsibility of up skilling the competencies rest with future educators. Since prospective teachers can act as good source of inspiration to the masses combined with high reachability and involvement of groups or individuals towards the children and youth in society (Moreno et al., 2013). Empowering them in the understanding of cybersecurity principles is essential in cultivating a safe and secure digital learning environment Jones (2023), more specifically; the responsibility and risk assessment skills that the children and young generation need to navigate the internet effectively lie squarely on teachers' shoulders. Hence, prospective teachers should be provided more opportunity of developing skills and competencies not only for managing safe digital environment but also train them in propagating to the masses. Regrettably, in-service, and pre-service teachers are unprepared to teach students about cyber security and safety (Dambrosio, 2021). On the basis of this disclosure, the present study aims to develop a tool which measures the safety and security related competencies of the prospective teachers in line with the educational contexts.

2. Method

In order to accomplish the goal stated above, the researchers opted to create a scale, which is the most commonly utilized approach for assessing security competencies. To develop the scale of cyber security competency, we have built on previous researches that have developed lists of dimensions and indicators to measure cyber competency. The final lists of analyzed studies are summarized in Table 1.

Table 1
Details of the studies analysed

<i>Author</i>	<i>Title</i>	<i>Dimension</i>
Calvani et al. (2008)	Models and Instruments for Assessing Digital Competence at School	<ul style="list-style-type: none"> • Technological dimension • Cognitive dimension • Ethical dimension
Cartelli (2010)	Frameworks for Digital Competence Assessment: Proposals, Instruments, and Evaluation	<ul style="list-style-type: none"> • Cognitive • Affective • Social Relational
Falloon (2020)	From digital literacy to digital competence: the teacher digital competency (TDC) framework.	<ul style="list-style-type: none"> • Personal professional competencies (Operational) • Personal ethical competencies (awareness, concern, action)
Janssen et al. (2013)	Experts' views on digital competence: Commonalities and differences.	<ul style="list-style-type: none"> • Functional • Integrative • Specialized • Communication and collaboration • Information management • Privacy and security • Legal and ethical • Technology and society • 5-Learning with and about technology • Informed decision making • Coherence/self-efficacy • Dispositional
Punie and Redecker (2017)	European Framework for the Digital Competence of Educators	<ul style="list-style-type: none"> • Transversal competencies • Subject specific competencies
Skov (2016)	The Digital Competence Wheel.	<ul style="list-style-type: none"> • Health • Data protection • Identity management • Law
Tomczyk (2019)	What Do Teachers Know About Digital Safety?	<ul style="list-style-type: none"> • Ability to set privacy rules • Assessment of the credibility of information received • Knowledge about social networking • Awareness on applications
Tretinjak and Anđelić, (2016)	Digital Competences for Teachers: Classroom Practice	<ul style="list-style-type: none"> • Information • Communication safety on the internet • Problem solving • Content creation
Vuorikari et al. (2016)	The Digital Competence Framework 2.0	<ul style="list-style-type: none"> • Information and data literacy • Communication & collaboration • Digital content creation • Safety

A list of 113 items was then drafted (Yes, no, and unsure) for the 12 dimensions of cyber security. Later on 21 items were modified and 13 were deleted as per opinions of the experts. Finally, the entire items in the scale were organized under 9 dimensions of cyber security competency. After the final generation of items and its corresponding scoring procedure, the draft scale with 93 items were administered to a sample of 252 prospective teachers. For this a stratified random sampling technique was adopted for the initial sample selection. Since the online data collection methods turn into more popular and robust in the present-day context, the investigator adopted online method for response gathering. All the instructions which are necessary for collecting responses were guaranteed while administering the tool.

Table 2 shows the dimension wise break up of items for the scale. There are 93 items are comprised in the scale including 79 positive items and 14 negative items. On the basis of the generated items a 3-point scoring procedures were followed in the scale. A separate scoring procedure was adopted for negative and a positive statement in the scale.

Table 2

Dimension Wise Break Up of Items

No	Dimensions	Items	Positive	Negative
1	Social Networking Safety and Security (SNS)	10	9	1
2	Dealing with Fake Information (DWF)	10	7	3
3	Mobile Phone Security and Safety (MPS)	10	9	1
4	Email and Password Security and Safety (ELS)	10	10	0
5	Managing Digital Footprint (MDF)	10	9	1
6	Online Privacy and Wi-Fi Safety (OWS)	10	7	3
7	Application Safety and Security (APS)	10	10	0
8	Web Conferencing Safety (WCS)	10	7	3
9	Digital Learning Resource safety & Plagiarism and copyright infringement (DRS)	13	11	2
Total		93	79	14

The overall scoring pattern is as shown in Table 3.

Table 3

Scoring Pattern

Response	Indication	Scores	
		Positive	Negative
Yes	High Competency	2	0
No	Low Competency	0	2
Unsure	Average Competency	1	1

Table 3 shows the scoring procedure adopted for negative and a positive statement in the scale. The response 'Yes' assigned a score of 2 for a positive statement, whereas 'No' assigned a score of 0. Similarly, for a negative statement, the response 'Yes' is assigned a score of zero, whereas the response 'No' is assigned a score of 2. The response 'Unsure' assigned a score of 0 for both positive and negative statements.

The item analysis of the cyber safety and security competency scale is carried out by using Cronbach's alpha statistic. A scale is said to be consistent when its Cronbach alpha value is equal or greater than .7. High value indicates good quality items in the scale (Sansanwal, 2020). Table 4 shows the Cronbach alpha value of the cyber safety and security competency scale.

Table 4

Cronbach's Alpha before Item Wise Analysis

Name of the measure	Value	Number of Items
Cronbach's Alpha	.877	93

Table 4 depicts the Cronbach alpha value obtained before item analysis of the scale which is .877 for 93 items. The Table 5 shows the results of item wise analysis of cyber security competency scale by using Cronbach alpha value. Those items which having the lower values than computed Cronbach's alpha value (.877) were removed the scale to ensure consistency of the scale.

Table 5

Item Wise Analysis for Cyber Security Competency Scale

<i>Numbers in Draft Tool</i>	<i>Mean if Item Deleted</i>	<i>Variance if Item Deleted</i>	<i>Corrected Item-Total Correlation</i>	<i>Cronbach's Alpha if Item Deleted</i>	<i>Remarks</i>	<i>Numbers in Final Tool</i>
Social Networking Safety						
SNS1	122.60	429.181	.320	.875	Retain	SNS1
SNS2	122.69	429.811	.240	.875	Retain	SNS2
SNS3	122.99	429.356	.200	.876	Retain	SNS3
SNS4	122.87	425.601	.326	.875	Retain	SNS4
SNS5	122.59	432.122	.199	.876	Retain	SNS5
SNS6	123.23	426.525	.265	.875	Retain	SNS6
SNS7	122.80	429.020	.236	.876	Retain	SNS7
SNS8	123.03	439.583	-.084	.879	Reject	-
SNS9	122.85	427.347	.307	.875	Retain	SNS8
SNS10	123.16	423.384	.360	.874	Retain	SNS9
Dealing with Fake Information						
DWF1	123.09	422.684	.472	.873	Retain	DWF1
DWF2	122.95	438.829	-.063	.879	Reject	-
DWF3	122.94	425.063	.352	.874	Retain	DWF2
DWF4	123.10	422.386	.402	.874	Retain	DWF3
DWF5	123.54	429.928	.182	.876	Retain	DWF4
DWF6	122.77	425.183	.398	.874	Retain	DWF5
DWF7	123.34	428.414	.236	.876	Retain	DWF6
DWF8	123.13	432.049	.119	.877	Retain	DWF7
DWF9	122.95	435.675	.027	.878	Reject	-
DWF10	123.01	428.470	.251	.875	Retain	DWF8
Mobile Phone Safety						
MPS1	122.55	431.095	.254	.875	Retain	MPS1
MPS2	123.21	427.672	.226	.876	Retain	MPS2
MPS3	123.61	428.536	.210	.876	Retain	MPS3
MPS4	123.20	422.711	.346	.874	Retain	MPS4
MPS5	122.89	428.598	.234	.876	Retain	MPS5
MPS6	122.81	432.864	.124	.877	Retain	MPS6
MPS7	122.89	430.638	.168	.876	Retain	MPS7
MPS8	122.78	423.421	.453	.874	Retain	MPS8
MPS9	123.51	427.701	.240	.876	Retain	MPS9
MPS10	123.33	425.472	.299	.875	Retain	MPS10
Managing Digital Footprint						
MDF1	123.11	423.927	.339	.874	Retain	MDF1
MDF2	122.56	428.087	.398	.874	Retain	MDF2
MDF3	123.73	438.116	-.044	.879	Reject	-
MDF4	123.87	433.459	.101	.877	Retain	MDF3
MDF5	122.62	436.586	.013	.877	Retain	MDF4
MDF6	123.67	433.754	.067	.878	Reject	-
MDF7	123.84	431.504	.167	.876	Retain	MDF5
MDF8	123.72	431.854	.123	.877	Retain	MDF6
MDF9	123.43	427.414	.241	.876	Retain	MDF7
MDF10	122.81	424.251	.385	.874	Retain	MDF8

Table 5 continued

<i>Numbers in Draft Tool</i>	<i>Mean if Item Deleted</i>	<i>Variance if Item Deleted</i>	<i>Corrected Item-Total Correlation</i>	<i>Cronbach's Alpha if Item Deleted</i>	<i>Remarks</i>	<i>Numbers in Final Tool</i>
Online Privacy and Wi-Fi Safety						
OWS1	122.89	427.827	.257	.875	Retain	OWS1
OWS2	122.84	428.270	.262	.875	Retain	OWS2
OWS3	123.12	436.388	.007	.878	Reject	-
OWS4	122.57	427.240	.420	.874	Retain	OWS3
OWS5	122.71	437.940	-.040	.878	Reject	-
OWS6	122.63	435.283	.059	.877	Retain	OWS4
OWS7	122.54	430.223	.309	.875	Retain	OWS5
OWS8	123.52	424.386	.321	.875	Retain	OWS6
OWS9	122.62	425.767	.422	.874	Retain	OWS7
OWS10	122.52	429.862	.365	.875	Retain	OWS8
Apps Safety						
APS1	122.65	424.684	.455	.874	Retain	APS1
APS2	122.65	427.170	.376	.874	Retain	APS2
APS3	122.88	423.838	.397	.874	Retain	APS3
APS4	122.97	424.475	.348	.874	Retain	APS4
APS5	122.71	426.665	.359	.874	Retain	APS5
APS6	122.57	430.475	.288	.875	Retain	APS6
APS7	122.66	429.367	.272	.875	Retain	APS7
APS8	123.01	419.866	.447	.873	Retain	APS8
APS9	122.64	428.312	.339	.875	Retain	APS9
APS10	123.62	423.566	.359	.874	Retain	APS10
Web Conferencing Safety						
WCS1	123.39	425.621	.286	.875	Retain	WCS1
WCS2	123.33	444.638	-.207	.881	Reject	-
WCS3	123.15	423.298	.365	.874	Retain	WCS2
WCS4	122.77	427.358	.301	.875	Retain	WCS3
WCS5	123.37	424.502	.333	.874	Retain	WCS4
WCS6	122.95	438.233	-.048	.879	Reject	-
WCS7	122.96	441.180	-.142	.879	Reject	-
WCS8	122.86	423.544	.416	.874	Retain	WCS5
WCS9	123.89	432.485	.134	.877	Retain	WCS6
WCS10	122.77	425.626	.362	.874	Retain	WCS7
Digital Learning Resource Safety						
DRS1	122.69	423.395	.458	.873	Retain	DRS1
DRS2	122.99	422.483	.416	.874	Retain	DRS2
DRS3	123.03	420.730	.445	.873	Retain	DRS3
DRS4	122.82	422.592	.448	.873	Retain	DRS4
DRS5	123.03	419.771	.502	.873	Retain	DRS5
DRS6	122.94	420.298	.494	.873	Retain	DRS6
DRS7	122.96	435.327	.038	.878	Reject	-
DRS8	122.68	422.890	.544	.873	Retain	DRS7
DRS9	123.02	436.986	-.012	.878	Reject	-
DRS10	123.69	435.237	.037	.878	Reject	-
DRS11	123.41	425.276	.315	.875	Retain	DRS8
DRS12	123.46	419.485	.469	.873	Retain	DRS9
DRS13	123.47	422.532	.401	.874	Retain	DRS10

Table 5 continued

Numbers in Draft Tool	Mean if Item Deleted	Variance if Item Deleted	Corrected Item-Total Correlation	Cronbach's Alpha if Item Deleted	Remarks	Numbers in Final Tool
E-Mail Safety and Security						
ELS1	122.59	429.170	.356	.875	Retain	ELS1
ELS2	123.37	421.793	.389	.874	Retain	ELS2
ELS3	123.73	433.069	.100	.877	Retain	ELS3
ELS4	122.87	429.485	.221	.876	Retain	ELS4
ELS5	122.93	435.478	.036	.878	Reject	-
ELS6	123.01	425.671	.305	.875	Retain	ELS5
ELS7	122.93	425.069	.343	.874	Retain	ELS6
ELS8	122.76	436.506	.008	.878	Reject	-
ELS9	122.94	424.003	.376	.874	Retain	ELS7
ELS10	122.90	425.809	.332	.875	Retain	ELS8

The topic wise break up of retained and removed items in the scale as shown in Table 6.

Table 6

Dimension wise break up of retained and removed items

No	Topics	Final Items	Positive	Negative	Items Deleted
1	Social Networking Safety and Security (SNS)	9	9	0	SNS 8
2	Dealing with Fake Information (DWF)	8	6	2	DWF 2 and DWF 9
3	Mobile Phone Security and Safety (MPS)	10	9	1	-
4	Email and Password Security and Safety (ELS)	8	8	0	ELS 5 and ELS 8
5	Managing Digital Footprint (MDF)	8	7	1	MDF 3 and MDF 6
6	Online Privacy and Wi-Fi Safety (OWS)	8	7	1	OWS 3 and OWS 5
7	Apps Safety and Security (APS)	10	10	0	-
8	Web Conferencing Safety (WCS)	7	6	1	WCS 2, WCS 6 and WCS 7
9	Digital Learning Resource safety & Plagiarism and copyright infringement (DRS)	10	10	0	DRS 7, DRS 9 and DRS 10
Total		78	72	6	15

Table 6 indicates the topic wise retained and removed items in the cyber safety and security competency scale. After removing 15 items in the scale 78 items were retained for final validation process.

2.1. The Reliability of the Scale

The reliability of the scale was determined by calculating the value of Cronbach's alpha and split-half correlation coefficient of the revised scale. The following table depicts the values of Cronbach's alpha and split-half correlation coefficient.

Table 7

Cronbach's alpha and Split half correlation coefficient for the Cyber Security Competency Scale

Name of the Measure	Values	Number of Items
Cronbach's Alpha	.906	78
Split Half Correlation	.851	

Table 7 furnishes the details about the calculated Cronbach's alpha value (.906) and split-half correlation coefficient value (.851) of 78 items in the cyber security competency scale. Both these values indicate the sound reliability of the scale.

2.2. Validity of the Scale

To ensure the validity of the scale the investigators depended on the construct validity procedure. For this Confirmatory Factor Analysis (CFA) was carried out. This analysis further helped to complement the results obtained with the reliability analysis. To carry out this analysis, the scale was administered again to prospective teachers, in this case to a sample of 100 participants. The analysis was carried out using the Jasp software.

The CFA aimed to assess the fit of the proposed factor model compared to a baseline model. The model fit was evaluated using the Chi-square test (see Table 8) with the baseline model yielding a Chi-square value of 145.727 with 36 degrees of freedom, while the factor model produced a Chi-square value of 33.034 with 27 degrees of freedom, resulting in a non-significant p -value of .196, indicating acceptable model fit.

Table 8

Model fit- Chi-square test

<i>Model</i>	χ^2	<i>df</i>	<i>p</i>
Baseline model	145.727	36	
Factor model	33.034	27	.196

In addition to the Chi-square test, various fit indices were computed, including the Comparative Fit Index [CFI], Tucker-Lewis Index [TLI], Bentler-Bonett Non-normed Fit Index [NNFI], Bentler-Bonett Normed Fit Index [NFI], and others. These indices provided a comprehensive assessment of the model fit, with values ranging from 0.773 to 0.949, indicating a reasonably good fit of the factor model (see Table 9).

Table 9

Additional fit measures - Fit indices

<i>Index</i>	<i>Value</i>
Comparative Fit Index	0.945
Tucker-Lewis Index	0.927
Bentler-Bonett Non-normed Fit Index	0.927
Bentler-Bonett Normed Fit Index	0.773
Parsimony Normed Fit Index	0.580
Bollen's Relative Fit Index	0.698
Bollen's Incremental Fit Index	0.949
Relative Noncentrality Index	0.945

Furthermore, the results of parameter estimates, factor loadings, and factor variances showed relationships between the latent factors and their observed indicators, were all statistically significant with p -values less than .001, indicating a strong association between the factors and their respective indicators.

Table 10 shows the results of CFA. From this it is evident that all factor loadings are statistically significant ($p < .001$), indicating a strong relationship between the indicators and their respective factors.

Table 10
Factor loadings

Factor	Indicator	Estimate	SE	z	p	95% Confidence Interval	
						Lower	Upper
CSS	D1 SNS	0.850	0.245	3.467	< .001	0.369	1.330
	D2 DWF	1.302	0.352	3.698	< .001	0.612	1.992
	D3 MPS	1.556	0.365	4.262	< .001	0.841	2.272
	D4 MDF	1.406	0.317	4.429	< .001	0.784	2.028
	D5 OWS	0.901	0.253	3.561	< .001	0.405	1.397
	D6 APS	1.248	0.289	4.313	< .001	0.681	1.815
	D7 WCS	1.652	0.315	5.248	< .001	1.035	2.269
	D8 DRS	1.998	0.397	5.029	< .001	1.219	2.777
	D9 ELS	1.522	0.345	4.407	< .001	0.845	2.199

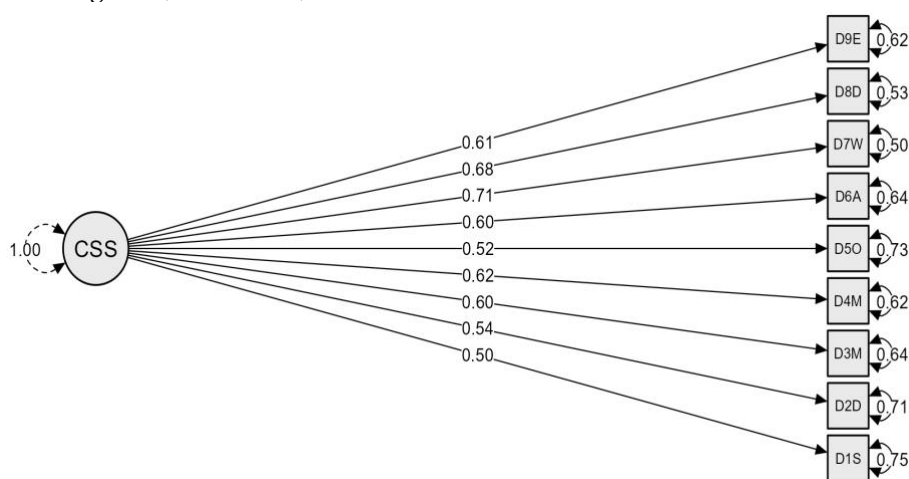
In Table 11, the estimated factor variance for the CSS factor is 1.000, indicating that the factor explains all of the variance in the indicator variables associated with it. The standard error for the factor variance estimate is 0.000, indicating a precise estimation of the factor variance.

Table 11
Factor Variances

Factor	Estimate	SE	z	p	95% Confidence Interval	
					Lower	Upper
CSS	1.000	0	-	-	1.000	1.000

Lastly, the results of the route diagram (see Figure 1) showed acceptable factor loads (standardized values) for all the items, ranging from 0.50 to 0.71, these values being acceptable if they are above 0.10.

Figure 1
CFA Diagram (Model Plot)



Overall, the results of the CFA suggest that the proposed factor model adequately fits the observed data, as indicated by the various fit measures and statistical significance of the parameter estimates and factor loadings. In summary, the CFA results demonstrate the adequacy of the factor model in representing the relationships between latent constructs and their indicators. The combination of statistical tests, fit indices, parameter estimates, and modification indices provides a comprehensive evaluation of the model fit and potential areas for model refinement, contributing to a thorough understanding of the underlying factor structure within the data.

3. Conclusion

The objective of this study was to develop an instrument to assess the cyber security competency of prospective teachers. The initial reliability analysis showed the calculated Cronbach's alpha value (.906) and split-half correlation coefficient value (.851) of 78 items in the cyber security competency scale. Both these values indicate the sound reliability of the scale (Final version of the Cyber Security Competency Scale [CSC-TSKT] was presented in Appendix 1).

With respect to the validation constructs the CFA indicated an excellent validity of the scale. The measured value of Chi-square test (χ^2) was 145.72 with $p = .196$, being statistically significant (Wong et al., 2017). Further the he index of comparative adjustment, the Tucker-Lewis index, and the root mean square error of approximation are the most relevant. The CFI and the TLI have a range of 0 to 1 considering these values more valid when they are closer to the unit; in addition, the value of RMSEA is considered to indicate a good fit to the model if it is less than 0.06. In the study, the CFI was $n = 0.945$, the TLI was $n = 0.927$ and the RMSEA that was obtained were 0.067, data that show a very good fit to the hypothetical model (Tomé-Fernández et al., 2020).

In conclusion, the development and standardization of a cyber-security competency scale tailored for prospective teachers represents a crucial step in enhancing cyber security awareness and preparedness within educational environments. The scale, based on extensive analysis and refinement, provides a comprehensive assessment of nine dimensions of cyber security competency, offering a reliable and valid method for measuring prospective educators' abilities to manage cyber threats effectively. The reliability of the scale is demonstrated by a high Cronbach's alpha value and its robustness and effectiveness are further confirmed by extensive Confirmatory Factor Analysis (CFA) results. The findings of the study underscore the growing urgency for educators to possess the necessary skills and competencies to navigate the digital landscape safely, thus highlighting the instrumental role of teachers in fostering cyber security awareness among students. Furthermore, this scale not only serves as a tool for self-assessment but also as a roadmap for educational institutions to craft targeted interventions to empower prospective teachers with the necessary skills and knowledge. Ultimately, the scale contributes to the larger goal of creating a cyber-savvy culture, ensuring a safe and secure digital learning environment for present and future generations.

Acknowledgements: This study is part of a doctoral thesis titled "The Impact of a Cyber Safety and Security Literacy Program on Cyber Security Competency, Cyber Socialization, and Etiquette among Prospective Teachers in Kerala".

Author contributions: The first author was responsible for all aspects of the manuscript, while the second author served as the research supervisor.

Declaration of interest: The authors declare that no competing interests exist.

Funding: No funding source is reported for this study.

References

- Calvani, A., Cartelli, A., Fini, A. & Ranieri, M. (2008). Models and instruments for assessing digital competence at school. *Journal of E-Learning and Knowledge Society*, 4, 183-193. <https://doi.org/10.20368/1971-8829/288>
- Cartelli, A. (2010). Frameworks for digital competence assessment: proposals, instruments and evaluation. In F. Tommasi, & E. Cohen (Eds.), *Proceedings of Informing Science & IT Education Conference* (pp. 561-574). Informing Science Institute. <https://doi.org/10.28945/1274>
- Dambrosio, R. (2021). *Student online safety and security: middle school teacher perspectives concerning safe internet use in the classroom* [Unpublished master's thesis]. California State University, Stanislaus.
- European Union Agency for Cyber security [ENISA]. (2018, January). *Threat Landscape Report 2017*. Author.

- Falloon, G. (2020) From digital literacy to digital competence: the teacher digital competency (TDC) framework. *Education Technology Research Development*, 68, 2449–2472. <https://doi.org/10.1007/s11423-020-09767-4>
- Ferrari, A. (2012). *Digital competence in practice : an analysis of frameworks*. European Union. <https://doi.org/10.2791/82116>
- Jansen, J., & van Schaik, P. (2019). The design and evaluation of a theory-based intervention to promote security behaviour against phishing. *International Journal of Human-Computer Studies*, 123, 40-55. <https://doi.org/10.1016/j.ijhcs.2018.10.004>
- Jones, M. A. (2023). "It was everywhere all at once": Exploring digital coercive control in the context of intimate partner violence through mix-method research. [Doctoral dissertation, The University of New Brunswick]. Scholarly Research Repository. <https://unbscholar.lib.unb.ca/handle/1882/37567>
- Lehto, M. (2015). Cyber security competencies: cyber security education and research in Finnish universities. In N. Abouzakhar (Ed.), *ECCWS-Proceedings of the 14th European conference on cyber warfare & security* (pp. 179-88). ACPI.
- McDuffie, E. (2011). NICE: National initiative for cybersecurity education. In F. T. Sheldon, R. Abercrombie, & A. Krings (Eds.), *Proceedings of the seventh annual workshop on cyber security and information intelligence research (CSIIRW '11)* (pp. 1-7). ACM. <http://doi.acm.org/10.1145/2179298.2179311>
- Moreno, M. A., Egan, K. G., Bare, K., Young, H. N., & Cox, E. D. (2013). Internet safety education for youth: stakeholder perspectives. *BMC Public Health*, 13, 543. <https://doi.org/10.1186/1471-2458-13-543>
- Punie, Y., & Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. Publications Office of the European Union.
- Sansanwal, D. N. (2020) *Research methodology and applied statistics*. Shipra Publications.
- Skov, A. (2016). *The digital competence wheel*. Center for Digital Dannelsø.
- Szczepaniuk, E. K., & Szczepaniuk, H. (2022). Analysis of cybersecurity competencies: Recommendations for telecommunications policy. *Telecommunications Policy*, 46(3), 102282. <https://doi.org/10.1016/j.telpol.2021.102282>
- Tomczyk, L. (2019). What do teachers know about digital safety? *Computers in the Schools*, 36(3), 167-187. <https://doi.org/10.1080/07380569.2019.1642728>
- Tomé-Fernández, M., Fernández-Leyva, C., & Olmedo-Moreno, E. M. (2020). Exploratory and confirmatory factor analysis of the social skills scale for young immigrants. *Sustainability*, 12(17), 6897. <https://doi.org/10.3390/su12176897>
- Tretinjak M. F. & Anđelić, V. (2016). Digital competences for teachers: classroom practice. In P. Biljanovic, Z. Butkovic, K. Skala, T. G. Grbac, M. Cicin-Sain, V. Sruk, S. Ribaric, S. Gros, B. Vrdoljak, M. Mauher, E. Tijan, & D. Lukman (Eds.), *39th international convention on information and communication technology, electronics and microelectronics (MIPRO)* (pp. 807-811). <https://doi.org/10.1109/MIPRO.2016.7522250>
- UNESCO. (2018). *UNESCO ICT Competency framework for teachers*. Author.
- Vuorikari, R., Punie, Y., Carretero, G. S., & Van Den Brande, G. (2016). *DigComp 2.0: The digital competence framework for citizens. update phase 1: the conceptual reference model*. Publications Office of the European Union.
- Wong, P. K. S., Wong, D. F. K., Zhuang, X. Y., & Liu, Y. (2017). Psychometric properties of the AIR Self-Determination Scale: the Chinese version (AIR SDS-C) for Chinese people with intellectual disabilities. *Journal of Intellectual Disability Research*, 61(3), 233-244. <https://doi.org/10.1111/jir.12343>
- Yaokumah, W. (2019). Cyber security competency model based on learning theories and learning continuum hierarchy. In B. Christiansen, & A. Piekarczyk (Eds.), *Global cyber security labor shortage and international business risk* (pp. 94-110). IGI Global. <https://doi.org/10.4018/978-1-5225-5927-6.ch006>

Appendix 1. Cyber Security Competency Scale (CSC-TSKT) (Final Version)**Dear Student Teacher,**

You are requested to express your degree of agreement for each statement by marking the corresponding column of response. Your participation in this study is voluntary and you are free to withdraw your participation from this study at any time. The process of filling form may take 20 to 30 minutes. There are no risks associated with participating in this study. The scale collects no identifying information of any respondent. All the responses in the form will be recorded anonymously.

No	Components/ Statements	Degree of Agreement		
		Yes	No	Unsure
	Social Networking Safety and Security			
1.	Are you selective in joining diverse social networking sites?			
2.	Do you limit your messaging options in your social networking sites?			
3.	Do you restrict the visibility of the active users in social networking?			
4.	Did you set login alerts for your social networking platforms?			
5.	Do you block spam users in social networking sites?			
6.	Do you update your antivirus software regularly?			
7.	Are you selective in tagging photos of others and yours in social networking?			
8.	Do you use extensively the privacy settings of all social networks?			
9.	Do you know how to report illegal activities in social networking platforms?			
	Dealing with Fake Information			
10.	Do you easily differentiate facts (accurate) and opinion (a person's view) in digital platforms?			
11.	Do you verify the facts of the information over online?			
12.	Do you seek the help of experts for validating the information?			
13.	Do you know about any fact checking websites?			
14.	Are you concerned about the credibility and reliability of the information online?			
15.	Do you set aside your personal bias while assessing any online information?			
16.	Are you easily attracted to the design and makeup of information online?			
17.	Do you introspect and think about the context of information that you receive online?			
	Mobile Phone Safety			
18.	Did you use to lock your phone with password?			
19.	Do you back up your data in phone regularly?			
20.	Did you enable mobile tracking feature in your phone?			
21.	Have you installed antivirus software in your phone?			
22.	Do you update your mobile device frequently?			
23.	Does your phone carry unwanted applications?			
24.	Do you disconnect internet when your mobile device is not in use?			
25.	Are you cautious about knowing the reviews and features of apps before downloading it in your mobile device?			

No	Components/ Statements	Degree of Agreement		
		Yes	No	Unsure
26.	Have you noted IMEI (International Mobile Equipment Identity) number of your device?			
27.	Do you check reset to factory settings when the phone was given to others?			
	Managing Digital Footprint			
28.	Do you explore privacy settings of all your online browsing platforms?			
29.	Are you alert in deleting unwanted social media accounts?			
30.	Do you use online audit tools for creating better digital footprint?			
31.	Did you like to advertise your personal emotions online?			
32.	Did you check your digital footprint regularly?			
33.	Do you have a password keeper file as your own?			
34.	Did you ever try to know about the audience of your online engagements?			
35.	Do you restrict yourself in engaging in online activities?			
	Online Privacy and Wifi Safety			
36.	Do you edit your privacy settings in all the online platforms that you engage?			
37.	Is your messaging app is end to end encrypted?			
38.	Are you aware of the consequences of postings and sharing in various social networking platforms?			
39.	Do you store private information in public storage?			
40.	Are you selective in choosing friends request online?			
41.	Have you installed privacy protection software in your device?			
42.	Are you alert in removing personal information from unwanted online platforms?			
43.	Are you serious in protecting and securing your privacy online?			
	Application Safety			
44.	Are you very cautious in downloading apps?			
45.	Do you read the reviews of the apps before installing?			
46.	Do you read and reflect the privacy policy of app before downloading?			
47.	Do you review the privacy settings of the installed app?			
48.	Are you cautious in downloading the apps from trusted app store?			
49.	Are you careful in deleting unused apps?			
50.	Are you concerned about not to disclose personal information through apps?			
51.	Do you know some apps track and shared location?			
52.	Do you check the usefulness of apps before its installation?			
53.	Do you install any technology safety apps in your device?			
	Web Conferencing Safety			
54.	Do you update your web conferencing software regularly?			
55.	Are you cautious in disabling other applications and programs when you are			

No	Components/ Statements	Degree of Agreement		
		Yes	No	Unsure
	in web conference?			
56.	Do you turn off audio and video sharing options in web conferencing?			
57.	Have you tried to explore all the privacy setting features of web conferencing platform?			
58.	Do you follow the rules and provisions issued by web conferencing host?			
59.	Do you know about bombing in web conferencing?			
60.	Are you vigilant in giving out personal information over web conferencing platform?			
Digital Learning Resource Safety				
61.	Are you alert in accessing digital learning resources from trusted sites?			
62.	Do you pay attention to the domains or URL of the educational resources that you access?			
63.	Do you discuss with the experts about the educational resources to ensure authenticity of the resources before using it for further study?			
64.	Are you concerned about the language and grammar used in educational resource that you access?			
65.	Do you check the author and their affiliation details of the digital learning resources that you access?			
66.	Do you try to verify certain statement in the resources with other sources?			
67.	Do you follow good online behaviour (Think before Share) while accessing digital online resources?			
68.	Do you cite the exact source while using the ideas of other person?			
69.	Did you ever read and learn about user agreement and IP address before using the online content?			
70.	Do you check creative commons license of online contents?			
Email and Password Safety				
71.	Have you created a strong password for your email accounts?			
72.	Do you know how to activate Two Factor Authentication (2FA) of email?			
73.	Do you change your email passwords frequently?			
74.	Do you have different password for your different accounts?			
75.	Has your password included short codes and characters?			
76.	Are you cautious in clicking unwanted email links?			
77.	Are you cautious in entering password in public Wi- fi and public places?			
78.	Are you very alert in logging off accounts after each and every internet activity?			