Advances in Consumer Research
https://acr-journal.com/
Volume-3 | Issue-2 | Feb 2026
Original Researcher Article

Development And Validation of a Cyber Security Questionnaire for Knowledge, Critical Thinking and Skills Assessment

Dr. Dolly Rani [1]*, Dr. Ajay Dubey [2], Ms. Rekha Dixit [3], Mrs. Sapna Verma[4], Dr. Priyanka Singh[5]
[1]Assistant Professor, Home Science, P. R. Government Girls Degree College, Etawah, Uttar Pradesh, India
[2]Associate Professor, Physical Education, P. R. Government Girls Degree College, Etawah, Uttar Pradesh, India
[3]Assistant Professor, English, P. R. Government Girls Degree College, Etawah, Uttar Pradesh, India
[4]Assistant Professor, Commerce, P. R. Government Girls Degree College, Etawah, Uttar Pradesh, India
[5]Assistant Professor, Physical Education, A.N.D. College, Kanpur, Uttar Pradesh, India
*Corresponding author: Dr. Dolly Rani (ORCID: 0000-0001-5966-044X)

ABSTRACT
The rapid expansion of digital technologies has heightened exposure to cyber threats, underscoring the urgent need for comprehensive cyber security literacy. This study develops and validates a questionnaire designed to assess three critical domains of cyber security literacy: knowledge, critical thinking, and skills. A survey was administered to 60 higher education students, and the instrument underwent rigorous psychometric evaluation. Reliability testing showed strong internal consistency (Cronbach's $\alpha = 0.815$ for knowledge, 0.714 for critical thinking, and 0.956 for skills) and high test–retest stability (0.945 and 0.970 for knowledge and critical thinking, respectively). Item analysis revealed that while most items demonstrated satisfactory difficulty, discrimination, and item–total correlations, a few required refinements. Validity testing confirmed strong construct and convergent validity, with high inter-domain correlations ($r = 0.849$ between knowledge and critical thinking, $r = 0.769$ between knowledge and skills, and $r = 0.654$ between critical thinking and skills). These results indicate that the questionnaire is a reliable and valid tool for measuring cyber security literacy in educational contexts. The study highlights its utility for identifying learners' strengths and weaknesses, informing curriculum development, and guiding future interventions. Recommendations are provided for item improvement and validation across broader populations to strengthen its generalizability..
Keywords: Cyber Security, Knowledge, Critical Thinking, Skills, Reliability, Validity, Digital Literacy, Higher Education

INTRODUCTION:

The increasing integration of digital technologies into everyday life has transformed the way individuals learn, communicate, work, and engage with society. However, this digital transformation has simultaneously introduced unprecedented vulnerabilities. Cyberattacks such as phishing, ransomware, malware infections, identity theft, and data breaches are now pervasive across personal, organizational, and national levels. These incidents not only impose significant financial costs but also jeopardize reputations, trust, and security.

Given the magnitude of these risks, **cyber security literacy** has emerged as a global educational priority. Cyber literacy extends beyond simple awareness—it encompasses factual knowledge of cyber threats, the ability to think critically when confronted with suspicious digital scenarios, and the practical skill to implement preventive and protective strategies. Collectively, these domains empower individuals to engage with technology safely and responsibly.

Despite its importance, measuring cyber security literacy remains challenging. Most existing assessments emphasize factual knowledge, overlooking whether learners can reason critically or translate knowledge into effective action. Such one-dimensional measures risk producing misleading conclusions, as knowledge without skills or critical thinking does not guarantee secure behavior.

To address this gap, the present study develops and tests a questionnaire that captures all three dimensions of cyber security literacy: **knowledge, critical thinking, and skills**. The instrument undergoes psychometric evaluation to establish its reliability and validity, ensuring its suitability for educational and training contexts.

2. REVIEW OF LITERATURE

2.1 Cyber security knowledge: Cyber security knowledge typically encompasses familiarity with key terms and practices such as malware, phishing, password management, firewalls, and ransomware. Siponen and Oinas-Kukkonen (2007) emphasize that knowledge serves as a foundation for secure digital practices. Empirical studies show that greater awareness often correlates with safer behavior; however, Hadlington (2017) notes that knowledge alone is insufficient, as individuals may still engage in risky digital activities despite being informed.

2.2 Critical thinking in cyber security: Critical thinking refers to the capacity to analyze, evaluate, and respond effectively to novel or suspicious situations (Facione, 2011). Within cyber security, this skillset allows individuals to identify fraudulent emails, question unexpected online requests, and evaluate the legitimacy of websites. Pfleeger and Caputo (2012) argue that decision-making skills are crucial in mitigating risks that cannot be resolved by knowledge alone. Without critical reasoning, individuals may fall prey to increasingly sophisticated attacks despite their awareness of cyber threats.

2.3 Skill development in cyber security: Practical skills involve applying knowledge and reasoning to real-world behaviors. These include implementing two-factor authentication, managing secure backups, regularly updating software, and using tools like VPNs. Chen and Zahedi (2016) highlight that such competencies are best cultivated through experiential learning or guided training programs. Self-reported skill assessments, such as those described by Kraemer and Carayon (2007), are frequently used to gauge learners' confidence and ability in applying secure practices.

2.4 Reliability and validity of assessment tools: For any educational intervention to be evaluated effectively, the instruments used must demonstrate psychometric soundness. Reliability ensures consistency of results, while validity ensures accuracy in measuring the intended construct (DeVellis, 2016). Cronbach's alpha is widely employed to test internal consistency, with thresholds above 0.7 considered acceptable and above 0.9 excellent (Tavakol & Dennick, 2011). In cyber security education, tools often assess attitudes and awareness but seldom integrate knowledge, reasoning, and skills.

2.5 Research gap: Prior studies emphasize the necessity of holistic frameworks integrating cognitive (knowledge), affective (attitudes), and behavioral (skills) dimensions (Anderson & Agarwal, 2010). However, validated instruments that comprehensively assess cyber security literacy remain scarce. This study contributes to the literature by developing and evaluating such a tool.

3. OBJECTIVES OF THE STUDY

To evaluate the internal consistency reliability of the questionnaire across its three domains.

To conduct item analysis for knowledge and critical thinking items to determine difficulty and discriminatory power.

To establish construct validity through correlations among knowledge, critical thinking, and skills.

To ensure content validity through expert review and alignment with cyber security frameworks.

To recommend improvements for future refinement and use of the questionnaire.

4. METHODOLOGY

4.1 Research Design: This study follows a **quantitative, survey-based research design** with a focus on psychometric evaluation. The approach is exploratory in nature, aiming to establish the reliability and validity of the cyber security questionnaire before its wider use in academic and organizational training contexts.

4.2 Respondents: A total of **60 respondents** participated in this study. Participants were drawn from higher education institutions (college students across science, commerce, and arts streams). This sample size was deemed adequate for preliminary psychometric testing, particularly for reliability analysis using Cronbach's Alpha, which performs well with 50–100 respondents.

Respondents varied in their socio-economic and educational backgrounds, as captured in **Section 1 of the questionnaire** (personal and family characteristics). However, the present report focuses exclusively on **Section 2** (knowledge, critical thinking, and skill development in cyber security). The demographic information was collected primarily to contextualize responses and enable potential future subgroup analyses.

4.3 Instrument: The instrument titled **"Questionnaire for Cyber Security"** was designed with three main subsections:

Section	No. of Items	Nature of Items	Score
Knowledge: Items measured factual knowledge of cyber security concepts such as strong passwords, phishing, malware, firewalls, ransomware, and safe online practices.	10	multiple-choice	1 for correct and 0 for incorrect responses
Critical Thinking: Items presented **scenario-based questions** requiring judgment in realistic cyber security situations (e.g., handling suspicious emails, USB drives, or public Wi-Fi use)	10	multiple-choice	scored dichotomous (1 for correct and 0 for incorrect responses)
Skill Development: Items measured respondents' **self-rated ability and confidence** in cyber security practices (e.g., using 2FA, VPNs, backups, and safe online behaviors).	10	5-point Likert scale	1 = very poor to 5 = excellent

4.4 Data Collection Procedure: Data were collected through a supervised administration of the questionnaire in academic institutions. Respondents were briefed on the purpose of the study and assured of confidentiality. Each participant completed the questionnaire individually, without external help, in approximately 25–30 minutes. Completed responses were entered into Microsoft Excel and subsequently imported into Python for statistical analysis.

4.5 Data Analysis: The data analysis comprised the following steps:

Reliability Analysis (Internal Consistency):

Test - retest method was applied to dichotomous scales (Knowledge and Critical Thinking).

Cronbach's Alpha was calculated separately for the knowledge, critical thinking, and skill sections. Items with zero variance (all respondents answering identically) were excluded, as they do not contribute to reliability. Interpretation was based on conventional thresholds:

≥ 0.9 = Excellent

0.8–0.9 = Good

0.7–0.8 = Acceptable

0.6–0.7 = Questionable

< 0.6 = Poor

Item Analysis:

For evaluating the quality of the questionnaire items, **item analysis** was conducted. Three statistical measures (difficulty index, discrimination index, and item-total correlations) were computed for each item

Validity Testing:

Content Validity: Evaluated through expert review (alignment with established cyber security frameworks and prior research).

Construct Validity: In the present study, construct validity was supported by a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy, indicating that the data are suitable for Factor Analysis.

Convergent Validity: In the present study, convergent validity was confirmed through high Pearson's correlations between domain total scores (Knowledge, Critical Thinking, Skills), showing these domains are related as expected.

Use of Artificial Intelligence (AI): A Large Language Model (LLM), ChatGPT (OpenAI, GPT-5, 2025), was used to assist in language refinement of this manuscript. The LLM was not involved in study conception, questionnaire design, data collection, statistical analysis, or interpretation. All analyses, interpretations, and accountability for the content remain solely with the author.

5. RESULTS

After the tabulation and analyzing the data, result has been presented under the following heads:

Reliability of the questionnaire

Item analysis of the questionnaire

Validity of the questionnaire

5.1 Reliability of the questionnaire: For accessing the reliability of the questionnaire test - retest method was applied to dichotomous scales (Knowledge and Critical Thinking about Cyber Security) and Cronbach's Alpha was calculated separately for the knowledge, critical thinking, and skill sections about cyber security

Table. 1. Reliability coefficients for Cyber Security questionnaire domains

Method	Scale	No. of Items	Reliability Coefficient
Test-retest method	Knowledge	10	0.945
	Critical Thinking	10	0.97
Cronbach's Alpha	Knowledge	10	**0.815** (good reliability)
	Critical Thinking	10	**0.714** (acceptable reliability).
	Skill Development	10	**0.956** (excellent reliability).

Table 1. indicates that the instrument is internally consistent, with the skill section performing particularly strongly. The knowledge and critical thinking sections also demonstrated satisfactory reliability, suggesting that the items measure their respective constructs consistently. The **test–retest reliability coefficients** (0.945 and 0.970) indicate very strong stability of responses over time. This shows that your instrument is both **stable** and **internally consistent**, making it suitable for reliable data collection.

5.2 Item Analysis of the questionnaire: For evaluating the quality of the questionnaire items, **item analysis** was conducted. Three statistical measures (difficulty index, discrimination index, and item-total correlations) were computed for each item:

Table. 2. Item Analysis – Knowledge about Cyber Security

Item no.	Item	Difficulty Index (Proportion	Discrimination Index (Upper 27% -	Item-Total Correlation (r)

		Correct)	Lower 27%)	
ITEM 1	What is cyber security?	1.0	0.0	nan
ITEM 2	Which of the following is a strong password ?	0.867	0.364	0.709
ITEM 3	What is phishing?	0.617	0.902	0.636
ITEM 4	What does a firewall do?	0.217	0.342	0.772
ITEM 5	Which one is a cyber crime?	0.867	0.364	0.709
ITEM 6	What is Two-Factor Authentication (2FA)?	0.867	0.364	0.709
ITEM 7	What is malware?	0.25	0.395	0.758
ITEM 8	What should you do if you receive a suspicious email?	1.0	0.0	nan
ITEM 9	What is ransomware?	0.233	0.153	0.504
ITEM 10	What is the safest way to store passwords?	1.0	0.0	nan

Table 2. indicates the item analysis related to Knowledge about Cyber Security. The result reported that the difficulty index showed that items **2, 5, 6** were too easy (≥0.80), while items **4, 7, and 9** were too difficult (<0.30). Only **item 3** was within the ideal range (0.30–0.70). The discrimination index indicated that items **2, 3, 4, 5, 6, and 7** had good to excellent discrimination (≥0.30), with **item 3** being the best (0.902). Items **1, 8, and 10** had zero discrimination, making them ineffective. Item–total correlations were strong for most items (0.504–0.772), except for **items 1, 8, and 10**, which showed undefined correlations due to lack of variance.

In summary: Items **2, 3, 4, 5, 6, and 7** are good; item **9** is acceptable; and items **1, 8, and 10** should be revised or discarded.

Table. 3. Item Analysis – Critical Thinking about Cyber Security

Item no.	Item	Difficulty Index (Proportion Correct)	Discrimination Index (Upper 27% - Lower 27%)	Item-Total Correlation (r)
ITEM 1	A university receives an email that looks like it is from the IT department, asking all students to reset their passwords using a given link. The link redirects to a page asking for personal and banking details. What should be the first step for a cautious student?	1.0	0.0	Nan
ITEM 2	An employee receives a USB drive labeled "Company Salary Data" in the office parking lot. What is the safest action?	1.0	0.0	Nan
ITEM 3	A hospital's system suddenly locks and displays a message demanding payment in cryptocurrency to restore access to patient records. This is an example of:	0.317	0.9	0.471
ITEM 4	While shopping online, you notice the website URL starts with "http://" instead of "https://". What does this imply?	0.6	1.0	0.833

ITEM 5	A company wants to protect employees working remotely from phishing attacks. Which of the following would be the **most effective preventive measure**?	0.867	0.4	0.804
ITEM 6	A student downloads free software from an unverified website. Later, their laptop becomes very slow and shows unwanted ads. Which cybersecurity risk is most likely involved?	0.117	0.25	0.277
ITEM 7	A bank notices unusual login attempts from multiple countries on a customer's account. To mitigate such risks, what is the best solution?	0.867	0.4	0.804
ITEM 8	During a video call, an employee unknowingly shares their screen with sensitive financial data visible. This scenario is an example of:	0.6	1.0	0.833
ITEM 9	A college student is asked to join a free public Wi-Fi to download study material. Which action would be **most secure**?	0.3	0.062	0.296
ITEM 10	A company wants to ensure that even if data is stolen, hackers cannot read it. Which cybersecurity approach is best suited?	0.567	0.338	0.278

The item analysis results (Table 3.) related to critical thinking about cyber security reveal that Items 1 and 2 were answered correctly by all respondents (difficulty index = 1.0) and showed no discrimination or correlation with total scores, indicating that they are too easy and fail to differentiate between high- and low-performing individuals. Items 3, 4, 5, 7, and 8 demonstrated strong psychometric qualities, with moderate to acceptable difficulty levels, high discrimination indices, and strong item–total correlations, making them the most effective items in assessing knowledge. In contrast, Item 6 had a very low difficulty index (0.117), suggesting it was too difficult for most respondents, and both its discrimination and correlation values were weak, reducing its usefulness. Item 9 also showed poor discrimination (0.062) and a low correlation, despite being a difficult item, making it less reliable. Item 10 fell into a moderate range of difficulty but displayed only fair discrimination and weak correlation, indicating limited effectiveness. Overall, the analysis suggests that Items 3, 4, 5, 7, and 8 are strong and should be retained, while Items 1, 2, 6, and 9 need revision or replacement, and Item 10 may require minor improvement.

Table. 4. Item Analysis – Skill about Cyber security

Item no.	Item	Mean Rating (1–5)	Discrimination Index (Upper 27% - Lower 27%)	Item-Total Correlation (r)
ITEM 1	The learner demonstrates the ability to create and use strong, unique passwords.	3.767	1.857	0.993
ITEM 2	The learner identifies phishing emails, suspicious links, or fake websites accurately.	3.2	2.0	0.875
ITEM 3	The learner updates software, applications, and security patches in a timely manner.	3.2	2.214	0.919
ITEM 4	The learner applies two-factor authentication (2FA) effectively to secure accounts.	4.067	2.5	0.861
ITEM 5	The learner uses safe practices while connecting to public Wi-Fi (e.g., VPN, hotspot).	2.467	1.0	0.646

ITEM 6	The learner avoids downloading files or software from untrusted sources.	3.333	1.5	0.864
ITEM 7	The learner demonstrates secure data backup and recovery practices.	3.2	2.0	0.894
ITEM 8	The learner protects sensitive information when using online platforms and social media.	3.467	1.214	0.696
ITEM 9	The learner reports cybersecurity incidents (e.g., phishing, malware, data breach) appropriately.	3.2	2.214	0.829
ITEM 10	The learner applies cybersecurity practices consistently in simulated or real-life scenarios.	3.767	1.857	0.864

The item analysis related to skill about cyber security in Table 4. indicates that most items performed well, with mean ratings ranging from 3.2 to 4.0, showing positive responses overall. The discrimination indices were generally strong, particularly for Items 3, 4, and 9, suggesting that these items effectively differentiate between high and low scorers. Item-total correlations were also high across items, confirming good internal consistency of the scale. However, Items 5 and 8 showed comparatively lower mean ratings, weaker discrimination, and lower item-total correlations, indicating the need for further review or refinement. Overall, the scale demonstrates good reliability and validity.

5.4 Validity of the questionnaire: To validate the questionnaire related to knowledge, critical thinking and skill development about cyber security content validity, construct validity and convergent validity were assessed.

Construct Validity: In the present study, construct validity was supported by a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy, indicate that the data is suitable for Factor Analysis. The Skill Development scale showed acceptable sampling adequacy (KMO = 0.709) with evidence of strong inter-item correlations.

Convergent Validity: In the present study, convergent validity was confirmed through high Pearson's correlations between domain total scores (Knowledge, Critical Thinking, Skills about Cyber Security), showing these domains are related as expected.

Table. 5. Inter-scale correlations (Pearson's r)

Pairwise Correlation	r-value	Interpretation
Knowledge vs Critical Thinking	0.849	Strong positive correlation
Knowledge vs Skill	0.769	Strong positive correlation
Critical Thinking vs Skill	0.654	Moderate-to-strong correlation

Table 5. clearly indicate a strong positive relationship between **knowledge and critical thinking** indicates that individuals with better factual knowledge tend to perform better in reasoning-based scenarios.

Knowledge also correlated strongly with skills, showing that factual awareness contributes to greater confidence in applying practices.

The correlation between critical thinking and skills was moderate-to-strong, suggesting that while related, practical skill adoption may also depend on factors beyond reasoning (such as training or experience).

6. DISCUSSION

The present study examined the reliability and validity of a newly developed questionnaire designed to assess knowledge, critical thinking, and skill development in cyber security. The findings demonstrate that the instrument is psychometrically sound, with strong evidence of reliability, acceptable item performance, and adequate construct validity.

6.1 Reliability: The test–retest reliability coefficients for knowledge (0.945) and critical thinking (0.970) domains indicated high stability of responses across time. Similarly, Cronbach's Alpha values were strong, particularly for the skill section (0.956, excellent), followed by knowledge (0.815, good) and critical thinking (0.714, acceptable). These results align with the recommendations of Tavakol and Dennick (2011), who suggest that coefficients above 0.70 indicate acceptable internal consistency. Thus, the questionnaire can be considered a consistent tool for measuring the three targeted domains of cyber security literacy.

6.2 Item analysis: Item-level evaluation provided further insights into the functioning of the instrument. In the knowledge section, some items (e.g., Items 1, 8, and 10) showed zero discrimination and undefined item-total correlations, indicating their inability to differentiate between high and low performers. Conversely, Items 3, 4, and 7 demonstrated good discrimination and correlation values, making them effective for measuring cyber knowledge. The critical thinking section revealed that

while most items (3, 4, 5, 7, and 8) were strong, certain items were either too easy (Items 1 and 2) or too difficult (Item 6), thereby reducing their discriminative capacity. This pattern resonates with findings in other educational assessment studies, where extremely easy or difficult items tend to contribute little to overall test reliability (DeVellis, 2016). The skill development section performed particularly well, with most items showing positive mean ratings and strong correlations. Nonetheless, Items 5 and 8 were weaker compared to others, suggesting a need for revision. Overall, the item analysis confirmed that the majority of items are functioning as intended, while a few require refinement.

6.3 Validity: Evidence from construct and convergent validity further strengthened confidence in the tool. The KMO measure (0.709) indicated sampling adequacy for factor analysis, supporting the multidimensional construct of the questionnaire. High positive correlations between knowledge and critical thinking (r = 0.849) suggest that factual understanding strongly influences reasoning in cyber security contexts, which is consistent with prior studies (Pfleeger & Caputo, 2012). The correlation between knowledge and skills (r = 0.769) confirms that awareness of cyber concepts translates into confidence in secure practices, echoing Hadlington (2017). Meanwhile, the moderate-to-strong correlation between critical thinking and skills (r = 0.654) highlights that while reasoning ability is linked to practical skills, real-world application may also depend on hands-on training and experiential learning (Chen & Zahedi, 2016).

6.4 Implications: These findings underscore the importance of a holistic framework for cyber security education, combining factual knowledge, critical reasoning, and applied skills. The questionnaire provides educators, trainers, and researchers with a reliable tool to assess learners' competencies across these domains. Its application can help diagnose strengths and weaknesses in cyber security literacy, guide curriculum development, and evaluate the effectiveness of interventions.

6.5 Limitations and future directions: While the results are encouraging, some limitations must be acknowledged. The study relied on a relatively small sample (N = 60), drawn from higher education students, which may limit generalizability to other populations such as professionals or school learners. Some items showed weak discrimination or correlation, necessitating refinement and re-testing in larger and more diverse samples. Future research should also explore predictive validity by examining whether scores on this questionnaire correlate with actual cyber security behavior in real-world or simulated environments.

7. CONCLUSION

Overall, the developed questionnaire demonstrated strong reliability and validity in assessing knowledge, critical thinking, and skills related to cyber security. With minor item revisions and validation across broader samples, the tool holds promise as a comprehensive measure for advancing cyber security literacy in educational and organizational settings

REFERENCES

1. Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS Quarterly, 34(3), 613–643.
2. Chen, Y., & Zahedi, F. M. (2016). Individuals' Internet security perceptions and behaviors: Polycontextual contrasts. Information & Management, 53(2), 225–236.
3. DeVellis, R. F. (2016). Scale development: Theory and applications (4th ed.). Sage Publications.
4. Facione, P. A. (2011). Critical thinking: What it is and why it counts. Insight Assessment.
5. Hadlington, L. (2017). Human factors in cyber security: Examining the role of psychological traits, Internet addiction and attitudes toward cyber security. Heliyon, 3(7), e00346.
6. Kraemer, S., & Carayon, P. (2007). Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists. Applied Ergonomics, 38(2), 143–154.
7. Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815–825.
8. Pfleeger, S. L., & Caputo, D. D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), 597–611.
9. Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database, 38(1), 60–80.
10. Tavakol, M., & Dennick, R. (2011). Making sense of Cronbach's alpha. International Journal of Medical Education, 2, 53–55.

.