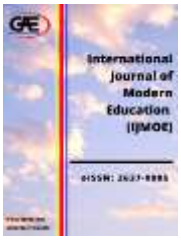
International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718



INTERNATIONAL JOURNAL OF MODERN EDUCATION (IJMOE)
www.gaexcellence.com/ijmoe

ADAPTING CYBERSECURITY KNOWLEDGE MEASURES FOR MALAYSIAN UNIVERSITY STUDENTS: INSIGHTS FROM EXPLORATORY FACTOR ANALYSIS

Nur Raidah Salim[1]*, Nur Izzati Mat Zin[2], Norhaliza Abu Bakar[3], Ahmad Fauzi Mohd Ayub[1,2]

[1]Institut Penyelidikan Matematik, Universiti Putra Malaysia
nurraidah@upm.edu.my https://orcid.org/0000-0002-7941-1878
[2]Fakulti Pengajian Pendidikan, Universiti Putra Malaysia, Malaysia
afmy@upm.edu.my https://orcid.org/0000-0002-4313-2922
zati1103@gmail.com https://orcid.org/0009-0003-6844-5444
[3]Pusat Pengajian Diploma, Universiti Tun Hussein Onn Malaysia, Malaysia
norhaliza@uthm.edu.my https://orcid.org/0000-0002-3115-4366
*Corresponding Author

Article Info:

Article history:
Received date: 28.01.2026
Revised date: 09.02.2026
Accepted date: 01.03.2026
Published date: 10.03.2026

To cite this document:

Salim, N. R., Mat Zin, N. I., Abu Bakar, N., & Mohd Ayub, A. F. (2026). Adapting Cybersecurity Knowledge Measures for Malaysian University Students: Insights from Exploratory Factor Analysis. *International Journal of Modern Education, 8*(29), 700-718.

DOI: 10.35631/IJMOE.829042

Abstract:

The rise of digital threats in Malaysia underscores the need to integrate cybersecurity knowledge into higher education in STEM. However, contextually validated measurement tools remain scarce. This study adapted and validated a multidimensional instrument based on the six-dimensional Cybersecurity Scale (CS-S) framework. Following expert validation (I-CVI ≥ 0.78), the instrument was administered to 115 Malaysian STEM students. An Exploratory Factor Analysis (EFA) procedure using Principal Component Analysis (PCA) with Varimax rotation was employed to determine the factor structure. Results confirmed a robust six-component structure: Confidentiality, Integrity, Availability, Authenticity, Utility, and Possession/Control. The refined instrument demonstrated high internal consistency with a Cronbach's Alpha of 0.80, exceeding the 0.70 threshold recommended for newly developed constructs. These findings provide a psychometrically sound foundation for subsequent Confirmatory Factor Analysis (CFA) and offer educators a reliable tool to assess cybersecurity preparedness. This research supports national digital resilience goals by providing a validated means to identify learning gaps among future STEM professionals.

Keyword:

Cybersecurity Knowledge, Exploratory Factor Analysis, Principal Component Analysis

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

Introduction

In the evolving landscape of digital threats, cybersecurity knowledge has emerged as a critical competency across disciplines and sectors. As the frequency and sophistication of cyberattacks escalate, ensuring individuals, organisations, and nations can effectively safeguard sensitive information and digital infrastructures requires more than general awareness; it demands comprehensive, dynamic cybersecurity education. Globally, cybercrime is projected to cause damages totalling USD 10.5 trillion annually by 2025, making it one of the most pressing challenges of the decade (Vergara Cobos & Cakir, 2024).

Malaysia is particularly vulnerable in this landscape, recording over 19.62 million web attacks in the first half of 2024 alone, making it the most targeted country in Southeast Asia during that period (Hidayat Mohamad, 2025). Threat intelligence reports from early 2024 indicate that hacktivist-oriented threat actors, including groups that publicly announced and conducted disruptive cyberattacks targeting Malaysian web systems and digital infrastructure, were active. These incidents highlight the increasing exposure of national digital assets and underscore the urgency of fostering a cyber-resilient population (PwC, 2024; National Cyber Coordination and Command Centre [NC4], 2024). Consequently, the Malaysian government has accelerated initiatives such as the Malaysia Cyber Security Strategy (MCSS) 2020-2024 and the establishment of the Malaysia Cyber Security Academy (slated for full operation in 2025) to address a critical shortage of approximately 26,430 cybersecurity professionals required by 2025 (Ministry of Digital, 2024).

University students, particularly those in Science, Technology, Engineering, and Mathematics (STEM) disciplines, represent a key demographic in this endeavour. As future engineers, technologists, and scientists, they are the architects of future digital systems. However, empirical evidence suggests a significant "knowing-doing" gap: while students are prolific technology users, they often lack the depth of knowledge required to mitigate sophisticated threats such as AI-powered phishing (Alqahtani et al., 2024), deepfake social engineering (Alghamdi, 2025) and ethical considerations (Shalevska, 2024). Studies indicate that over 99% of successful cyberattacks in Malaysia remain attributable to human error, often stemming from insufficient knowledge of ethical and policy considerations (Hakimi et al., 2024).

Cybersecurity competency extends beyond theoretical understanding to encompass the skills, abilities, and practical experience necessary to navigate complex digital environments (Alammari et al., 2022). This multidimensional requirement underscores the need for structured educational initiatives, especially within university environments, to cultivate a cyber-aware workforce. Frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework serve as vital references in shaping effective cybersecurity education and awareness programs (Nair, 2023). However, the success of these

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

programs depends significantly on the use of engaging, learner-centred methodologies. Recent studies show that strategies such as gamification, simulations, and alignment with real-world scenarios improve learner engagement and knowledge retention among university students (Razack & Saad, 2024; Deng et al., 2022). Furthermore, experiential learning methods such as hands-on labs, problem-based learning, and case-based reasoning have been shown to strengthen both understanding and the practical application of cybersecurity principles (Blanchard et al., 2024; Colomé et al., 2019).

Despite these advances, there remains a pressing gap in developing validated, psychometrically sound instruments specifically designed to measure cybersecurity knowledge among STEM university students in Malaysia, an essential step toward addressing the global cybersecurity skills shortage, which has been estimated at millions of unfilled positions (Triplett, 2023). Existing measurement tools are often developed in Western contexts and may not reflect Malaysia's socio-cultural and educational environment, limiting their relevance and applicability (Mohamed et al., 2025). Without a reliable, contextually relevant instrument, it is challenging for educators, researchers, and policymakers to accurately assess cybersecurity preparedness, identify learning gaps, or evaluate the effectiveness of educational interventions.

To address this gap, the present study aims to develop and validate a reliable, contextually relevant instrument for measuring cybersecurity knowledge among Malaysian STEM university students. By establishing a robust, empirically validated instrument, this research contributes to both academic and practical efforts to strengthen cybersecurity education and assessment. It provides educational institutions and policymakers with a practical tool for evaluating cybersecurity preparedness, informing curriculum development, and supporting national and global cybersecurity capacity-building initiatives.

Literature Review

The increasing reliance on digital technology across sectors underscores the critical importance of cybersecurity knowledge, particularly in the Science, Technology, Engineering, and Mathematics disciplines (Azzeh et al., 2022). This need extends to higher education institutions, where students are increasingly exposed to cyber threats due to widespread online interactions and their reliance on digital tools for academic purposes (Bognár & Bottyán, 2024). This increased digital engagement requires STEM students to have a comprehensive understanding of cybersecurity principles to reduce the risks stemming from human error, a significant factor in many cybersecurity breaches (Fatokun et al., 2019). Despite various initiatives to improve cybersecurity education, significant gaps persist in the supply of qualified cybersecurity professionals to meet current and future demands (Spencer, 2025). These gaps highlight the urgent need to assess and improve university students' cybersecurity knowledge, particularly those in STEM fields, given their future roles in technology-driven industries (Poulsen et al., 2021). Furthermore, understanding the current state of cybersecurity knowledge among this demographic is essential for developing targeted educational interventions and refining curricula to address specific gaps (Andria et al., 2025).

Cybersecurity Knowledge

The increasing reliance on digital technology across sectors underscores the critical importance of cybersecurity knowledge, particularly in Science, Technology, Engineering, and Mathematics (STEM) disciplines (Azzeh et al., 2022). This need extends to higher education

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

institutions worldwide, where students are increasingly exposed to cyber threats due to extensive online interactions and reliance on digital tools for academic activities (Bognár & Bottyán, 2024). The rapid digitalisation of educational settings, encompassing cloud platforms, learning management systems, and collaborative technologies, has markedly expanded the attack surface at universities. Consequently, STEM students must develop a comprehensive understanding of cybersecurity principles to reduce risks stemming from human error, which remains a major contributor to cybersecurity breaches (Fatokun et al., 2019).

Recent international studies show that cybersecurity knowledge gaps are not limited to any specific geographic region but constitute a broader global challenge. For instance, research conducted in European and North American educational contexts indicates that university students often demonstrate high levels of perceived digital competence while simultaneously lacking practical knowledge of secure digital practices (Garba et al., 2020; Bruin & Mersinas, 2024). Similarly, studies examining digital learning environments suggest that students' self-reported responses regarding technological practices may be influenced by contextual and social factors, including social desirability effects and survey environments (Lavidas et al., 2022a). These findings suggest that assessments of cybersecurity knowledge must carefully consider both measurement reliability and behavioural realities.

Cybersecurity knowledge can be broadly defined as a university student's understanding of digital threats, vulnerabilities, and protective practices—both technical (e.g., passwords, malware, and software updates) and behavioural (e.g., phishing awareness and safe browsing practices). Given the widespread integration of digital technologies in contemporary society, cybersecurity knowledge is no longer confined to IT specialisation. However, it has become a fundamental competency for all digitally active individuals, particularly those in STEM fields (Azzeh et al., 2022). In Malaysian studies, this concept is often operationalised through items assessing knowledge of social media security policies, data protection practices, and appropriate responses to cyber threats (Fatokun et al., 2024). However, cybersecurity knowledge extends beyond technical competence to encompass broader cyber awareness, enabling individuals to effectively identify, evaluate, and mitigate digital risks (Lazarov et al., 2025).

Despite growing awareness initiatives, a recurring issue in cybersecurity education research is the discrepancy between perceived knowledge and actual secure behaviour. While students may report familiarity with cybersecurity concepts, empirical evidence suggests that this awareness does not consistently translate into effective protective practices (Garba et al., 2020; Bruin & Mersinas, 2024). This disconnect is partly due to educational frameworks that emphasise the acquisition of technical skills while overlooking the behavioural and psychological dimensions that influence cybersecurity practices (Pirta-Dreimane et al., 2022). Evaluating the foundational cybersecurity knowledge of university students, particularly those enrolled in STEM disciplines, is crucial for developing educational strategies that integrate both technical proficiency and behavioural competence (Hong et al., 2022).

Cybersecurity Education

Globally, governments and educational institutions have increasingly prioritised STEM education as a key driver of technological innovation and economic competitiveness (Buniel et al., 2025). In Malaysia, this emphasis has been institutionalised through the formal integration of STEM education into secondary and tertiary curricula to cultivate critical

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

thinking, analytical reasoning, and problem-solving skills required for future industries (Amdan et al., 2024). This policy direction embodies extensive global initiatives to equip students for burgeoning technical fields, such as artificial intelligence, data science, and cybersecurity. However, the integration of cybersecurity within STEM education remains uneven across countries and institutions. While some Western universities have begun embedding cybersecurity modules within engineering and computing curricula, many educational systems still treat cybersecurity as a specialised discipline rather than a transversal competency applicable across STEM fields (Dioubate et al., 2022). This gap highlights the need for more interdisciplinary approaches that integrate cybersecurity awareness into broader STEM learning environments.

In Malaysia, the national commitment to STEM development has yet to yield sustained student involvement. Recent statistics indicate that STEM enrolment among upper-secondary students declined from 45.20% in 2017 to 40.94% in 2022, falling short of the national target of achieving a 60:40 science-to-arts ratio (Chuan et al., 2023). This decline poses a significant challenge to Malaysia's aspiration to develop a technologically skilled workforce capable of supporting digital transformation and cybersecurity resilience (Lam & Siew, 2024). Moreover, rapid advances in artificial intelligence, automation, and digital platforms have redefined STEM learning environments, necessitating pedagogical approaches that align with these evolving technological contexts. Emerging research suggests that advanced technologies such as generative AI tools can enhance STEM education by supporting personalised learning and improving student engagement (Granström & Oppi, 2025; Ugras, et al., 2024). Nevertheless, these innovations introduce new cybersecurity challenges, as students increasingly interact with cloud-based systems and digital infrastructures that require responsible, secure use. Consequently, cybersecurity education must evolve alongside technological advancements to ensure that STEM graduates are equipped with both technical expertise and responsible digital practices. Despite these developments, existing studies suggest that Malaysian universities still face challenges in integrating cybersecurity principles effectively within STEM curricula (Karpudewan et al., 2022; Ariffin et al., 2018). This highlights the importance of systematically assessing cybersecurity knowledge among university students to inform curriculum design and educational interventions to address emerging digital threats.

University Students Cybersecurity Awareness

At the global level, universities play a critical role in preparing students to navigate increasingly complex digital ecosystems. STEM education, in particular, is expected to equip students with both technical competence and digital responsibility (Buniel et al., 2025). However, the effectiveness of these educational initiatives depends largely on students' awareness of cybersecurity risks and their ability to translate knowledge into secure digital behaviour. In Malaysia, declining enrolment in STEM-related disciplines has raised concerns regarding the long-term supply of skilled professionals in technologically intensive fields, including cybersecurity (Ismail, 2022). Historical trends indicate that participation in science streams has remained relatively low, with only 31.22% of students enrolled in science-based programmes in 2005 (Jin et al., 2023). Such patterns highlight structural challenges in sustaining interest in STEM education and maintaining a robust pipeline of future technology professionals (Terzieva et al., 2024).

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

These challenges are intensified by the growing frequency and sophistication of cyber threats that impact both public and private sectors. As cyber incidents continue to escalate worldwide, cultivating graduates with strong cybersecurity literacy has become an urgent priority. Consequently, strengthening cybersecurity awareness among STEM students is not only an educational concern but also a strategic priority for national digital resilience (Zulkifli et al., 2024). Importantly, studies examining online survey methodologies have emphasised the need for reliable data collection when assessing students' technological knowledge and behaviour, as response patterns can be influenced by contextual factors such as survey delivery mode and participant engagement (Lavidas et al., 2022b). These considerations highlight the importance of developing well-structured measurement instruments to evaluate cybersecurity knowledge among university students effectively. Against this backdrop, assessing cybersecurity awareness among STEM university students provides valuable insights into existing knowledge gaps and the effectiveness of current educational strategies.

Understanding these gaps is particularly significant, as foundational competencies in mathematics, logic, and analytical reasoning, which constitute the core of STEM education, are directly linked to students' capacity to grasp complex cybersecurity concepts and systems (Shim et al., 2017). Hence, investigating the current state of cybersecurity knowledge among Malaysian STEM students is vital, as such insights can guide the development of targeted educational interventions and support the integration of more effective curriculum strategies within higher education institutions.

Methodology

This study employed a quantitative research design using exploratory factor analysis (EFA) to develop and validate an instrument to measure cybersecurity knowledge among STEM university students in Malaysia. An exploratory factor analysis (EFA) was used to identify the underlying latent factor structure and establish the instrument's construct validity. EFA is particularly appropriate at the initial stage of instrument development when theoretical dimensionality has not yet been empirically established (Hair et al., 2019).

Sample and Sampling Procedure

A total of 115 university students from STEM programs across various universities in Malaysia participated in this study. The participants were selected using simple random sampling to ensure equal representation and minimise sampling bias. The sample size was determined based on established rule-of-thumb recommendations for Exploratory Factor Analysis (EFA). According to Hair et al. (2019) and Awang et al. (2023), a minimum sample size of 100 respondents is required to obtain stable and interpretable factor solutions. Although the resulting subject-to-item ratio (4.6:1) is slightly below the frequently cited 5:1 threshold, the sample size is considered sufficiently large for this study, as factor stability is strongly influenced by item loadings. As demonstrated in the Results section (see Table 5), all retained items achieved loadings above 0.60. According to MacCallum et al. (1999), when communalities and loadings are consistently high (>0.60), a sample size of 100 to 200 can reliably recover the population factor structure, confirming that the current sample is adequate to support the factor extraction employed in this study.

Furthermore, this study was conducted as a pilot investigation to evaluate the clarity, feasibility, and preliminary psychometric properties of the proposed cybersecurity knowledge instrument

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

before proceeding to a larger-scale study. As the primary purpose of pilot studies is instrument refinement rather than population inference, strict adherence to proportional sampling ratios or representativeness was not required. Instead, the focus was placed on obtaining sufficient responses to examine the factor structure and internal consistency of the measurement items. Methodological literature suggests that pilot studies for exploratory factor analysis may employ relatively small samples, provided the data are adequate for assessing factorability and reliability (Hair et al., 2019). Therefore, the sample obtained in this pilot study was deemed appropriate for evaluating the instrument's preliminary validity and reliability. To further demonstrate the sample's representativeness, Table 1 presents a detailed breakdown of participants' demographic characteristics, including gender and specific STEM discipline.

Table 1: Demographic Information

Items	Category	Frequency (n)	Percentage (%)
Gender	Male	52	45.2%
	Female	63	54.8%
STEM Discipline	Engineering	40	34.8%
	Information Technology/CS	35	30.4%
	Pure Sciences (Bio/Chem/Phy)	25	21.7%
	Mathematics/Statistics	15	13.1%

Instrument Development and Content Validation

The development of the Cybersecurity Knowledge instrument followed a structured adaptation and validation process to ensure psychometric rigour within the Malaysian STEM context.

Adaptation of the Conceptual Framework

The instrument was operationalised by adapting the six-dimensional framework proposed by Arpaci and Sevinc (2021) in their Cybersecurity Scale (CS-S). This framework extends beyond the traditional "CIA triad" (Confidentiality, Integrity, and Availability) to include three additional critical dimensions: Authenticity, Possession/Control, and Utility. These dimensions collectively reflect a holistic view of cybersecurity knowledge, encompassing not only technical safeguards but also the legitimacy, control, and effective utilisation of digital resources.

Contextualization and Refinement

To ensure relevance for STEM university students in Malaysia, the original items were refined linguistically and contextually. Minor wording modifications were implemented to align the items with the local higher education environment and digital landscape (e.g., referencing local cyber threat scenarios). This adaptation process aimed to preserve the conceptual integrity of the original dimensions while enhancing the instrument's face validity for the target demographic.

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

Ethical Considerations

This study adhered to internationally accepted ethical standards for research involving human participants. Ethical approval was obtained from the Universiti Putra Malaysia Research Ethics Committee (Jawatankuasa Etika Universiti Putra Malaysia) under approval reference JKEUPM-2023-1477 prior to data collection.

All participants were informed of the purpose of the study, the voluntary nature of their participation, and their right to withdraw from the study at any time without consequences. Informed consent was obtained from all participants prior to the administration of the questionnaire. Additionally, the survey was conducted anonymously, and no personally identifiable information was collected to ensure participant confidentiality and data protection. The collected data were used solely for academic research purposes.

Expert Validation (CVI and CVR)

Following adaptation, the preliminary instrument underwent a rigorous content validation process involving three subject matter experts (SMEs) specialising in cybersecurity education and psychometrics. The validation was conducted in two stages:

1. Quantitative Evaluation: The SMEs evaluated each item using a 4-point Likert scale based on "Relevance," "Clarity," and "Contextual Appropriateness." To ensure statistical stringency, the Content Validity Index (CVI) and Content Validity Ratio (CVR) were calculated. Following the recommendations of Shi et al. (2012), only items achieving an Item-level Content Validity Index (I-CVI) ≥0.78 were retained. This threshold ensured the instrument remained technically accurate and linguistically appropriate for the Malaysian academic context.
2. Qualitative Refinement: Experts provided qualitative feedback regarding the phrasing and potential ambiguity of specific items. In accordance with the scale development guidelines by Hair et al. (2019), redundant or ambiguous items were eliminated, and the remaining items were reworded to maximise clarity. This iterative refinement resulted in a finalised item pool prepared for Exploratory Factor Analysis (EFA).

The Finalised Research Instrument

Following content validation and linguistic adjustments, the original 25-item instrument was used in this study. To ensure the items were suitable for the Malaysian STEM context, they were coded and categorised according to their respective dimensions. The full list of adapted items and their corresponding codes is presented in Table 2 below.

Table 2: Adapted Items for Cybersecurity Knowledge Instruments

Dimensions	Item Code	Adapted Item Description
Confidentiality	CONFI1	I am cautious about the personal information I share in cyberspace.
	CONFI2	I do not share information and documents in cyberspace that I do not want to share with third parties in real life.

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

	CONFI3	I ensure that the data I share in cyberspace can only be viewed by the necessary people.
	CONFI4	I do not share my contact information in cyberspace.
Control/ Possession	CONTROL5	I do not share my passwords for my accounts with anyone.
	CONTROL6	When creating my passwords, I choose a hard-to-guess password that contains symbols, numbers and capital letters.
	CONTROL7	I use the phone verification service to protect my email password.
	CONTROL8	I correctly answer the security question required to recover my account passwords.
Authenticity	AUTHENT14	I do not trust e-mails from people I do not know.
	AUTHENT15	I do not trust websites without a security certificate.
	AUTHENT16	I do not open spam mails sent to my e-mail address.
	AUTHENT17	I ignore social engineering e-mails sent to my e-mail address.
	AUTHENT18	I do not open links and attachments from unknown sources.
Availability	AVAIL19	I use an up-to-date antivirus program on my devices.
	AVAIL20	I regularly scan my devices with an antivirus program.
	AVAIL21	I keep the firewall installed on my devices turned on.
	AVAIL22	I do not open the files I downloaded from the Internet without scanning with an anti-virus program.
Utility	UTILITY23	I use social media applications to share information in cyberspace.
	UTILITY24	I use services provided in cyberspace (such as Google Scholar, cloud applications, and social media) to solve problems.
	UTILITY25	I use the services provided in cyberspace for information management (information acquisition, storage, sharing and application).

Source: (Arpaci & Sevinc, 2021)

Data Analysis Procedure

The collected data were analysed using Exploratory Factor Analysis (EFA), with Principal Component Analysis (PCA) as the extraction method. PCA was selected for its effectiveness in data reduction and in identifying underlying component structures, particularly in the preliminary stages of instrument development (Hair et al., 2019). To enhance the interpretability of the extracted components, a varimax orthogonal rotation was applied.

The suitability of the data for factor analysis was evaluated using the Kaiser–Meyer–Olkin (KMO) measure of sampling adequacy, with values of 0.60 or higher indicating adequate shared variance among items, and Bartlett's Test of Sphericity, which was required to be statistically significant ($p < 0.05$). These tests confirm that the correlation matrix was appropriate for component extraction (Hair et al., 2019; Awang et al., 2023).

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

Factor retention was guided by eigenvalues greater than 1.0 and inspection of the scree plot. In line with Awang et al. (2023), items with factor loadings below 0.40 were considered for removal, while loadings of 0.60 and above were interpreted as strong. Items exhibiting substantial cross-loadings or low communalities were also removed to ensure a clear and parsimonious factor structure. The internal consistency reliability of each factor was subsequently assessed using Cronbach's alpha, with values of 0.70 or higher indicating acceptable reliability (Hair et al., 2019).

Results

The Exploratory Factor Analysis (EFA) of the Cybersecurity Knowledge construct yields several key insights that contribute to the validation and refinement of the measurement model. In accordance with the data analysis procedure described in Section 3.3, the analysis employed principal component analysis (PCA) with varimax rotation to examine the underlying component structure. The results revealed a multidimensional solution comprising six distinct components, indicating that cybersecurity knowledge among STEM university students encompasses multiple interrelated dimensions.

Based on established item retention criteria, three items were removed due to insufficient component loadings and/or substantial cross-loadings across multiple components. The refined component structure provides greater clarity and enhances the robustness of the measurement model.

Sampling Adequacy and Factorability

The Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was recorded at 0.730, indicating a middling but acceptable level for factor analysis according to Kaiser's (1974) guidelines. Bartlett's Test of Sphericity was significant ($\chi^2 = 978.180$, df = 231, $p < .001$), confirming that the correlation matrix is not an identity matrix and is thus appropriate for factor extraction as shown in Table 3:

Table 3: KMO and Barlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		**.730**
Bartlett's Test of Sphericity	Approx. Chi-Square	978.180
	df	231
	Sig.	.000

Factor Structure and Total Variance Explained

The final EFA model retained six components, which together explained 65.083% of the total variance, considered satisfactory for social science research, as shown in Table 4. The rotated component matrix suggests a clear factor structure as follows:

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

1. Confidentiality (Component 1): Items CONFI1, CONFI2, CONFI3, CONFI4, and CONTROL5 loaded strongly on this component, reflecting knowledge related to maintaining the privacy and security of information.
2. Authentication (Component 2): AUTHENT14, AUTHENT15, AUTHENT16, and AUTHENT17 grouped under this factor, indicating knowledge about verifying the identity of users and systems.
3. Integrity (Component 3): INTEGRITY9, INTEGRITY10, INTEGRITY12, and INTEGRITY13 represented this dimension, highlighting knowledge of ensuring data accuracy and trustworthiness.
4. Availability (Component 4): AVAIL19, AVAIL20, AVAIL21, and AVAIL22 loaded clearly, signifying awareness of maintaining system uptime and access to information.
5. Utility (Component 5): Items UTILITY23, UTILITY24, and UTILITY25 grouped together, relating to the usefulness and practical application of cybersecurity measures.
6. Control Measures (Component 6): CONTROL7 and CONTROL8 represented specific control mechanisms, reflecting knowledge about the enforcement of security policies and regulations.

Table 4: Eigenvalues and Total Variance Explained

Component	Initial Eigenvalues			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.207	23.667	23.667	2.875	13.067	13.067
2	2.903	13.197	36.865	2.637	11.986	25.054
3	2.109	9.586	46.450	2.520	11.457	36.510
4	1.596	7.256	53.706	2.199	9.994	46.504
5	1.314	5.973	59.679	2.190	9.954	56.459
6	1.189	5.404	65.083	1.897	8.624	65.083
7	0.946	4.301	69.384			

Item Removal and Construct Refinement

During the analysis, three items: CONTROL6, INTEGRITY11, and AUTHENT18 were identified as problematic. These items exhibited low factor loadings, inconsistent with theoretical expectations. Their removal improved the clarity and interpretability of the item's factor structure, as shown in Table 5.

Table 5: Factor Loading of an Item after Rotated Component Matrix

	Component					
	1	2	3	4	5	6
CONFI1		.693				
CONFI2		.682				
CONFI3		.814				
CONFI4		.609				
CONTROL5		.559				

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

CONTROL7					.851	
CONTROL8					.562	
INTEGRITY9					.814	
INTEGRITY10				.721		
INTEGRITY12				.832		
INTEGRITY13				.736		
AUTHENT14			.750			
AUTHENT15			.714			
AUTHENT16			.816			
AUTHENT17			.675			
AVAIL19	.837					
AVAIL20	.864					
AVAIL21	.863					
AVAIL22	.510					
UTILITY23						.563
UTILITY24						.670
UTILITY25						.806

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalisation.
a. Rotation converged in 8 iterations.

Reliability of Cybersecurity Knowledge Construct

The value of the cybersecurity knowledge construct after the EFA procedure indicates good reliability (Cronbach's Alpha = 0.80). It suggests that the items retained after EFA consistently measure the cybersecurity knowledge construct. Reliability is within the recommended threshold, confirming the scale's internal consistency. Awang et al. (2023) suggest that a minimum Cronbach's Alpha of 0.70 is required for newly developed constructs.

Discussion

The results of this study provide strong empirical support for conceptualising cybersecurity knowledge as a multidimensional construct, consistent with established theoretical and measurement frameworks in the cybersecurity literature. The six-component structure identified through Exploratory Factor Analysis (EFA) closely aligns with the dimensions proposed by Arpaci and Sevinc in developing the Cybersecurity Scale: availability, authenticity, confidentiality, integrity, possession/control, and utility. This convergence between empirical findings and prior theoretical models strengthens the construct validity of the present instrument.

The availability dimension reflects students' understanding of ensuring that authorised users can reliably access information systems and digital resources when required. This finding is consistent with the classical CIA triad and highlights availability as a foundational component of cybersecurity knowledge, particularly relevant in academic and cloud-based environments where service continuity is critical.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume: 8 Issue: 29 (March 2026) PP. 700-718

The authenticity dimension captures respondents' awareness of identity verification, legitimacy, and trust mechanisms in cyberspace. Its emergence as a distinct component supports prior research emphasising authentication as a core cybersecurity competency, particularly in mitigating identity-based threats such as phishing, impersonation, and unauthorised access. This suggests that students cognitively distinguish authentication mechanisms from broader access control concepts.

The confidentiality component concerns protecting information from unauthorised disclosure. Factor structure aligns with longstanding cybersecurity principles and confirms that confidentiality remains a salient and well-understood dimension among STEM students. This finding is consistent with prior studies indicating that confidentiality-related concepts are often the most recognised aspect of cybersecurity knowledge in educational contexts.

Similarly, the integrity dimension reflects awareness of the need to maintain the accuracy, consistency, and trustworthiness of information systems. The separation of integrity from confidentiality and availability in the factor solution indicates that respondents perceive data manipulation and data leakage as conceptually distinct cybersecurity concerns. This distinction is theoretically meaningful, and mirrors established cybersecurity standards and frameworks.

The possession or control dimension concerns knowledge of ownership, control, and authority over digital assets. Its inclusion supports Arpaci and Sevinc's argument that cybersecurity extends beyond technical safeguards to include governance, access rights, and control mechanisms. This dimension is particularly relevant in contemporary environments that involve cloud services, shared infrastructure, and distributed data ownership.

Finally, the utility dimension captures respondents' understanding of the effective and purposeful use of information and digital services in cyberspace. The emergence of this component suggests that cybersecurity knowledge extends beyond protection mechanisms to encompass the ability to balance security with usability. This aligns with prior literature, which emphasises that overly restrictive security measures may undermine system effectiveness and user compliance.

The overall reliability of the Cybersecurity Knowledge construct (Cronbach's alpha = 0.80) indicates satisfactory internal consistency, exceeding the recommended threshold for newly developed scales. Importantly, removing items with weak or cross-loadings led to a clearer, more theoretically coherent component structure. This refinement process aligns with best practices in scale development and enhances the instrument's psychometric robustness.

Taken together, the findings confirm that cybersecurity knowledge among STEM university students is not unidimensional but rather comprises interrelated yet distinct domains that collectively represent the complexity of cybersecurity competence. The alignment between the EFA-derived components and established dimensions in the literature provides strong empirical justification for the proposed six-component structure. This validated structure offers a solid foundation for subsequent Confirmatory Factor Analysis (CFA) and structural modelling, as well as for practical applications in cybersecurity education, assessment, and curriculum design.

International Journal of Modern Education
EISSN: 2637-0905
IJMOE
Volume: 8 Issue: 29 (March 2026) PP. 700-718

Conclusion

In conclusion, the findings indicate that cybersecurity knowledge among respondents is not a single entity but rather comprises various interconnected elements. The clarity of the rotated component matrix confirms the theoretical foundation of cybersecurity domains, including confidentiality, integrity, availability, authentication, utility, and control measures. The removal of problematic items enhanced the construct validity and indicates the importance of careful item refinement in future questionnaire development. The EFA findings provide empirical support for a six-component structure of the cybersecurity knowledge construct. This structure accounts for a substantial proportion of variance and offers a reliable foundation for subsequent Confirmatory Factor Analysis (CFA) and structural modelling. The refinement process, including item removal, strengthens the instrument's psychometric properties, ensuring its suitability for both academic research and practical applications in cybersecurity competency assessment.

Beyond methodological contributions, this study also provides important implications for cybersecurity education and policy development. By identifying the multidimensional nature of cybersecurity knowledge among STEM students, the findings highlight the need for more comprehensive integration of cybersecurity within STEM curricula at higher education institutions. The validated measurement instrument developed in this study can serve as a diagnostic tool for educators and policymakers to identify knowledge gaps and design targeted educational interventions to strengthen cybersecurity competencies among future technology professionals. Ultimately, enhancing cybersecurity literacy among STEM students contributes to the development of a more cyber-resilient workforce capable of addressing emerging digital security challenges in an increasingly interconnected world.

Acknowledgements: The authors would like to express their sincere gratitude to Universiti Putra Malaysia for providing the necessary resources and support throughout the course of this research. Special appreciation is extended to colleagues and peers who contributed valuable insights and constructive feedback, which greatly enhanced the quality of this paper.

Funding Statement: This research received financial support from the Malaysia Research University Network (MRUN) through the MRUN Research Officer Grant Scheme (MROGS) under Grant Number 5539640. The funding body had no role in the design of the study, data collection, analysis, interpretation of results, or the decision to publish this manuscript.

Conflict of Interest Statement: The authors declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Modern Education (IJMOE).

Ethics Statement: This study was conducted in accordance with ethical research standards. All procedures involving human participants were reviewed and approved by the Jawatankuasa Etika Universiti Putra Malaysia (approval number JKEUPM-2023-1477). Informed consent was obtained from all participants prior to data collection. Participation was voluntary, and respondents were assured of confidentiality and anonymity. The data collected were used solely for academic purposes.

Author Contribution Statement: All authors contributed significantly to the development of this manuscript. Nur Raidah Salim was responsible for the conceptualisation of the study framework and instrumentation, the methodology, data collection, the overall literature review, and the drafting and critical revision of the manuscript. and overall supervision of the study. Nur Izzati Mat Zin handled data analysis and interpretation of results. Norhaliza Abu Bakar contributed to drafting the literature review and data collection. Ahmad Fauzi Mohd Ayub was involved in the conceptualisation, instrument development and overall supervision of the study. All authors read and approved the final version of the manuscript prior to submission.

International Journal of Modern Education
IJMOE
EISSN: 2637-0905
Volume: 8 Issue: 29 (March 2026) PP. 700-718

References

Alammari, A., Sohaib, O., & Younes, S. (2022). Developing and evaluating cybersecurity competencies for students in computing programs. Peerj Computer Science, 8, e827. https://doi.org/10.7717/peerj-cs.827

Alghamdi, M. A. (2025). Understanding Social Engineering in Cybersecurity and Mitigating Human-Centric Threats. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 563-584). IGI Global Scientific Publishing.

Alqahtani, S., Nanda, P., & Mohanty, M. (2024, December). Strengthening Cybersecurity: The Influence of Student Behavior, Perceived Factors, and Mitigating Strategies on Phishing Attack Perception. In *International Conference on Web Information Systems Engineering* (pp. 313-329). Singapore: Springer Nature Singapore.

Amdan, M. A., Janius, N., Saidin, M. S., & Kasdiah, M. A. H. (2024). Impact of Artificial Intelligence in TVET and STEM education among higher learning students in Malaysia. Journal of Research in Mathematics, Science and Technology Education. 1(2).

Andria, R. D. L., Sussolaikah, K., M-Dawam, S. R., Din, M. M. & Mansor, S. (2025). Bridging The Gaps: Evaluating Cybersecurity Awareness and Practices For Enhanced Digital Security. *Journal Information and Technology Management (JISTM)*, *10*(38). https://doi.org/10.35631/JISTM.1038013

Ariffin, S. A., Side, S. F., & Mutalib, M. F. H. (2018). A Preliminary Investigation of Malaysian Student's Daily Use of Mobile Devices as Potential Tools for STEM in a Local University Context. *International Journal of Interactive Mobile Technologies*, *12*(2). https://doi.org/10.3991/ijim.v12i2.8015

Arpaci, I. & Sevinc, K. (2021). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, 1 – 9, doi: 10.1177/0266666921997512

Awang, Z., Athanorhan, W., Lim, S., & Zainudin, N. F. S. (2023). SEM Made Simple 2.0. A Gentle Approach of Structural Equation Modelling. *Gong Badak: Penerbit Unisza*.

Azzeh, M., Altamimi, A. M., Albashayreh, M., & Al-Oudat, M. A. (2022). Adopting the Cybersecurity Concepts into Curriculum The Potential Effects on Students Cybersecurity Knowledge. *arXiv preprint arXiv:2209.10407*

Bognár, L., & Bottyán, L. (2024). Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students. *Education Sciences*, *14*(6), 588. https://doi.org/10.3390/educsci14060588

Blanchard, E., Feldman, S., White, M., Allen, R., Phillips, T., & Brown, M. (2024). Design and implementation of tabletop cybersecurity simulation for health informatics graduate students. *Applied Clinical Informatics, 15*(05), 921-927. https://doi.org/10.1055/s-0044-1790551

Bruin, M. D., & Mersinas, K. (2024). Individual and Contextual Variables of Cyber Security Behaviour - An empirical analysis of national culture, industry, organisation, and individual variables of (in)secure human behaviour. *ArXiv, abs/2405.16215.*

Buniel, J. M., Intano, J., Cuartero, O., Grustan, K. J., Sumaoy, R., Reyes Jr, N,...& Cortes, S. (2025). Modeling the influence of AI dependence to research productivity among STEM undergraduate students: case of a state university in the Philippines. In *Frontiers in Education* (Vol. 10, p. 1535466). Frontiers Media SA.

Chuan, Z. L., Wei, C. T., Japashov, N., Yuan, S. K., Qing, T. W., Ismail, N., Liong, C., Hiae, T. E. (2023). Analyzing Enrolment Patterns: Stacked Ensemble Statistical Learning-Based Approach to Educational Decision Making.13 December 2023, PREPRINT (Version 1) available at Research Square.

Colomé, M., Nunes, R., & Silva, L. (2019). Case-based cybersecurity incident resolution. https://doi.org/10.18293/seke2019-204

Deng, Y., Zeng, Z., Jha, K., & Huang, D. (2022). Problem-based cybersecurity lab with a knowledge graph as guidance. *Journal of Artificial Intelligence and Technology*, *2*(2). 55-61. https://doi.org/10.37965/jait.2022.0066

Dioubate, B. M., Daud, W., & Norhayate, W. (2022). Cyber security risk management frameworks implementation in Malaysian higher education institutions. *International journal of academic research in business and social sciences*, *12*(4), 1356-1371. https://doi.org/10.6007/IJARBSS/v12-i4/12300

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019, December). The impact of age, gender, and educational level on the cybersecurity behaviors of tertiary institution students: an empirical investigation on Malaysian universities. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012098). IOP Publishing.

Garba, A. A., Siraj, M. M., & Musa, M. A. (2020). A Study on Cybersecurity Awareness Among Students in Yobe: A Quantitative Approach. *International Journal on Emerging Technology*, 11(5), 41-49.

Granström, M. & Oppi, P. (2025) Student engagement with AI tools in learning: evidence from a large-scale Estonian survey. Front. Educ. 10:1688092. doi: 10.3389/feduc.2025.1688092

Hakimi, M., Quchi, M. M., & Fazil, A. W. (2024). Human factors in cybersecurity: an in depth analysis of user centric studies. Jurnal Ilmiah Multidisiplin Indonesia (JIM-ID), 3(01), 20-33. https://doi.org/10.58471/esaprom.v3i01.3832.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate data analysis. Cengage Learning EMEA.

Hidayat Muhamad. (2025, January 5). *Keselamatan siber di Malaysia: Analisis trend tahun 2024 dan harapan untuk tahun 2025*. Dewan Kosmik. https://www.majalahsains.com/keselamatan-siber-di-malaysia-analisis-trend-tahun-2024-dan-harapan-untuk-tahun-2025/

Hong, W.C.H., Chi, C., Liu, J. *et al.* (2022). The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates. *Education and Information Technology, 28*, 439–470. https://doi.org/10.1007/s10639-022-11121-5

Ismail, M. H., Fadzil, H. M., Saat, R. M., & Salleh, M. F. M. (2022). A needs analysis study for the preparation of integrated STEM instructional practices through Scientist-Teacher-Student Partnership (STSP). *ASM Science Journal*, *17*, 1-16. https://doi.org/10.32802/asmscj.2022.1112

Jinn, L. C., Zaman, I. A. K., Zakaria, S., Mahali, S. & Aleng, N. A. (2023). Analysing The Undergraduate Enrolment Pattern In Malaysian Public Universities Using Statistical Methods. *Journal of Mathematical Sciences and Informatics, 2*(2), 1 – 16, http://doi.org/10.46754/jmsi.2022.12.001

Karpudewan, M., Krishnan, P., Ali, M. N., & Yoon Fah, L. (2022). Analysing The Undergraduate Enrolment Pattern In Malaysian Public Universities Using Statistical Methods. Designing instrument to measure STEM teaching practices of Malaysian teachers. *Plos One*, *17*(5), e0268509. https://doi.org/10.1371/journal.pone.0268509

Lam, C. P., & Siew, N. M. (2024). Flipped classroom in science education: Correlating student experience with attitudes. *Problems of Education in the 21st Century, 82*(5), 672.

Lavidas, K., Papadakis, S., Manesis, D., Grigoriadou, A. S., & Gialamas, V. (2022a). The effects of social desirability on students' self-reports in two social contexts: Lectures vs. lectures and lab classes. *Information, 13*(10), 491.

Lavidas, K., Petropoulou, A., Papadakis, S., Apostolou, Z., Komis, V., Jimoyiannis, A., & Gialamas, V. (2022b). Factors affecting response rates of the web survey with teachers. *Computers, 11*(9), 127.

Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., Fujdiak, R. (2025). Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. *Technology, Knowledge Learning*. https://doi.org/10.1007/s10758-025-09840-y

MacCallum, R. C., Widaman, K. F., Zhang, S., & Hong, S. (1999). Sample size in factor analysis. *Psychological Methods, 4*(1), 84–99. https://doi.org/10.1037/1082-989X.4.1.84

Ministry of Digital (2024). Press Statement: Malaysia Cyber Security Academy to Begin Operations In 2025. Kuala Lumpur: Ministry of Digital Malaysia.

Mohamed, M., Awang, M., & Syariff, M. (2025). Development of Items to Measure Work Stress Among Secondary School Teachers in Sarawak: An Exploratory Factor Analysis Procedure. *International Journal of Academic Research*, *14*(1).

Nair, P. (2023). Enhancing cybersecurity awareness training through the nist framework. Ijarcce, 12(12). https://doi.org/10.17148/ijarcce.2023.121203

National Cyber Coordination and Command Centre. (2024). *Advisory on heightened cyber activities targeting Malaysian digital infrastructure*. National Cyber Security Agency (NACSA). https://www.nc4.gov.my

Pirta-Dreimane, R., Brilingaitė, A., Roponena, E., Parish, K., Grabis, J., Lugo, R. G., Bonders, M. (2023). CyberEscape Approach to Advancing Hard and Soft Skills in Cybersecurity Education. In: Schmorrow, D.D., Fidopiastis, C.M. (eds) Augmented Cognition. HCII 2023. Lecture Notes in Computer Science, vol 14019. Springer, Cham. https://doi.org/10.1007/978-3-031-35017-7_28

Poulsen, S., Herman, G. L., Peterson, P. A., Golaszewski, E., Gorti, A., Oliva, L., ... & Sherman, A. T. (2021). Psychometric evaluation of the cybersecurity concept inventory. *ACM Transactions on Computing Education (TOCE)*, *22*(1), 1-18.

PwC. (2024). *Cyber threat intelligence: A year in retrospect*. PricewaterhouseCoopers. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html

Razack, A. and Saad, M. (2024). Enhancing cybersecurity awareness through gamification: design an interactive cybersecurity learning platform for multimedia university students. Journal of Informatics and Web Engineering, 3(3), 21-40. https://doi.org/10.33093/jiwe.2024.3.3.2

Shalevska, E. (2024). Human Rights in the Age of AI: Understanding the Risks, Ethical Dilemmas, and the Role of Education in Mitigating Threats. *Journal of Legal and Political Education*, *1*(2), 38-52.

Shi, J., Mo, X., & Sun, Z. (2012). Content validity index in scale development. Zhong Nan Da *Xue Xue Bao Yi Xue Ban (Journal of Central South University. Medical Sciences), 37*(2), 152–155. https://doi.org/10.3969/j.issn.1672-7347.2012.02.007

Spencer, R. (2025). The Urgency of Instituting Systemic Cybersecurity Curriculum within STEM at Secondary Educational Levels in Preparation for Postsecondary Institutions. *Journal of Cybersecurity Education, Research and Practice*, *2025*(1), 4

Tee Kai Vern (2025). Study on Awareness of Cybersecurity Issues and Social Media Usage Among Youths. (Master's Thesis/Scopus-indexed proceeding), Universiti Kebangsaan Malaysia.

Terzieva, V., Paunova-Hubenova, E., Slavcheva, S. (2024). Trends, Challenges, Opportunities, and Innovations in STEM Education, *IFAC-PapersOnLine, 58*(3), 106 – 111, https://doi.org/10.1016/j.ifacol.2024.07.134

Triplett, W. (2023). Addressing cybersecurity challenges in education. International Journal of Stem Education for Sustainability, 3(1), 47-67. https://doi.org/10.53889/ijses.v3i1.132

Ugraş, H., Ugraş, M., Papadakis, S., & Kalogiannakis, M. (2024). Innovative early childhood STEM education with ChatGPT: Teacher perspectives. *Technology, Knowledge and Learning.*

Vergara Cobos, E. B., & Cakir, S. (2024). *A Review of the Economic Costs of Cyber Incidents.* World Bank Group, Working Paper.

Zulkifli, I. Z. Z., Razi, N. F. M., Mohammad, N. H.,& Sarkam, N. A. (2024). The association between performance and mathematical subjects among diploma students. *Journal of Computing Research and Innovation, 9*(2), 232-243.