RedFame

Journal of Education and Training Studies
Vol. 14, No. 4; October 2026
ISSN 2324-805X E-ISSN 2324-8068
Published by Redfame Publishing
URL: http://jets.redfame.com

Development and Validation of the Cybersecurity Literacy Assessment Scale for Lower Secondary Students: Initial Evidence from Grade 9 Students in Bangkok, Thailand

Munchukarn Naktoen[1], Daruwan Srikaew[1], Sutiwat Supaluk[1], Vitsanu Nittayathammakul[2], Duangkamon Winitkun[1]

[1]Division of Educational Communications and Technology, Faculty of Industrial Education and Technology, King Mongkut's University of Technology Thonburi, Bangkok, Thailand

[2]Ratchasuda Institute, Faculty of Medicine Ramathibodi Hospital, Mahidol University, Nakhon Pathom, Thailand Correspondence: Daruwan Srikaew, Division of Educational Communications and Technology, Faculty of Industrial Education and Technology, King Mongkut's University of Technology Thonburi, Bangkok, Thailand.

Received: May 12, 2026 Accepted: August 1, 2026 Online Published: August 19, 2026

doi:10.11114/jets.v14i4.9213 URL: https://doi.org/10.11114/jets.v14i4.9213

Abstract

Cybersecurity literacy has become an essential area of digital education, particularly for adolescents who actively use digital devices, social media platforms, and online learning environments. This study aimed to develop and validate the Cybersecurity Literacy Assessment Scale (CLAS) for lower secondary students, using empirical evidence from Grade 9 students in Bangkok, Thailand. An exploratory sequential mixed-methods design was employed. In the qualitative phase, relevant literature was synthesized to identify the components and indicators of cybersecurity literacy. The synthesis identified four components: 1) protecting devices and digital content, 2) protecting personal data and privacy, 3) safe and secure use, and 4) secure identity management—comprising nine indicators. Based on this structure, a 30-item CLAS was developed to assess students' self-reported knowledge, awareness, and cybersecurity-related practices regarding the safe and responsible use of digital technologies. Content validity was examined using the Content Validity Index. The I-CVI values ranged from .80 to 1.00, and the overall S-CVI/Ave was .91, indicating satisfactory content validity. In the quantitative phase, the scale was administered to 455 Grade 9 students. Confirmatory factor analysis supported the four-component measurement structure, with acceptable model fit indices: $\chi^2/df = 1.247$, GFI = .950, AGFI = .930, NFI = .970, TLI/NNFI = .990, CFI = 1.00, RMSEA = .016, RMR = .034, and SRMR = .034. Composite reliability values ranged from .610 to .759. The findings provide initial psychometric evidence for the CLAS as a theoretically grounded instrument for assessing cybersecurity literacy among Grade 9 students in an urban Thai educational context.

Keywords: device protection, personal data privacy, safe digital use, digital identity management, online threat awareness

1. Introduction

In recent years, Thailand has undergone a rapid transformation toward a digital society, driven by continuous advancements in digital technologies and artificial intelligence. These developments have significantly enhanced accessibility, connectivity, and efficiency in daily life. Moreover, the rapid growth of digital communication platforms has transformed the way adolescents interact, creating both opportunities and challenges in online social environments, particularly in urban contexts such as Bangkok, where digital engagement is highly intensive (Sudthongkhong et al., 2026). According to the Digital 2025 Thailand report, social media usage in Thailand has reached approximately 51.0 million users (71.1% of the population), while mobile device penetration has exceeded the total population at 139%. Additionally, Thai users spend an average of 7 hours and 54 minutes per day on the internet (DataReportal, 2025; We Are Social Thailand, 2025).

However, the increasing integration of digital technologies into everyday life has also led to a substantial rise in cybersecurity risks, particularly cybercrime. Common forms of cybercrime include, but are not limited to, online shopping fraud, deceptive job offers, loan scams, and investment fraud. Globally, cybercrime has escalated to a critical level, with individuals losing over one trillion U.S. dollars to scams within a 12-month period (Rogers, 2024). For adolescents, these risks are not limited to financial scams or technical threats but also include privacy violations, unsafe online communication, exposure to harmful content, identity misuse, and inappropriate digital decision-making. Cyberbullying is one important example of broader cyber-related risks in digital environments; however, in this study, it is treated as an

illustrative risk rather than as the central construct of measurement. Evidence from studies conducted in the Bangkok Metropolitan Area indicates that cyberbullying is prevalent among secondary school students and is closely associated with patterns of online interaction and social media use (Sudthongkhong et al., 2026).

In Thailand, cyber-related risks remain a pressing and escalating concern. Recent statistics reveal that more than 43,000 cybercrime cases were reported in early 2025, with total damages exceeding 3.4 billion Thai baht (Thai PBS News, 2025). These risks are particularly critical among adolescents, who are highly active digital users yet often lack sufficient knowledge, understanding, awareness, and behavioral practices to navigate online environments safely. In an urban society such as Bangkok, where students are frequently exposed to mobile technologies, social media platforms, online learning systems, and digital communication tools, cybersecurity literacy has become an essential area of digital learning and everyday digital participation. Thus, the need to strengthen adolescents' cybersecurity literacy should be understood within a broader pattern of everyday digital exposure, rather than being limited to any single online risk.

Addressing these challenges requires a shift from reactive approaches toward preventive and educational strategies. One of the most critical constructs in this regard is cybersecurity literacy, which is conceptualized in this study as a multidimensional construct encompassing self-reported knowledge, awareness, and cybersecurity-related practices required to identify, prevent, and respond to cyber threats. Unlike general digital participation, cybersecurity literacy specifically emphasizes protective knowledge, risk awareness, and security-related practices that enable students to use digital technologies safely and responsibly. For lower secondary students, cybersecurity literacy involves the ability to protect devices and digital content, safeguard personal data and privacy, use digital technologies safely and securely, and manage digital identity in responsible ways. These aspects are directly related to broader digital safety and responsible digital citizenship, but they remain focused on cybersecurity-related protection, prevention, and response.

This perspective is supported by international frameworks such as the Digital Competence Framework for Citizens (DigComp 2.2), which emphasizes key areas related to protecting devices, safeguarding personal data and privacy, ensuring safe digital engagement, and managing digital identity (Vuorikari et al., 2022). These areas align closely with the principles of digital citizenship, which promote respectful, ethical, and responsible participation in online environments (Office of the Education Council, 2023; DQ Institute, 2019). Accordingly, cybersecurity literacy can be understood as a foundational component of digital competence and digital citizenship, particularly for adolescents who are developing lifelong habits of digital participation. In this study, cybersecurity literacy is distinguished from related constructs. Digital literacy refers broadly to the ability to access, evaluate, create, and communicate information using digital technologies. Digital citizenship emphasizes ethical, respectful, and responsible participation in digital society. Online safety focuses on reducing exposure to online risks and harms. Cybersecurity literacy, however, specifically refers to students' self-reported knowledge, awareness, and practices related to identifying, preventing, and responding to cyber threats, including device protection, personal data and privacy protection, safe and secure use, and secure identity management. Thus, cybersecurity literacy is treated as a focused subdomain within broader digital competence and digital citizenship frameworks.

Despite the growing importance of cybersecurity literacy, empirical evidence indicates that adolescents' cybersecurity knowledge, awareness, and safe digital practices remain insufficient. The Thailand Cyber Wellness Index (CWI) shows that the overall digital well-being of Thai citizens is at a basic level, with a large proportion requiring further improvement (Advanced Info Service Public Company Limited [AIS], 2025). Adolescents aged 13–15 are particularly vulnerable, as they frequently encounter online risks such as cyberbullying, exposure to harmful content, and online exploitation (eSafety Commissioner, 2025; Thorn, 2024). Although cybersecurity concepts have been integrated into the national curriculum, particularly within computing science education (Ministry of Education, 2017), existing instructional approaches often emphasize knowledge acquisition rather than systematic assessment of students' cybersecurity literacy and safe digital practices.

Furthermore, prior research has primarily focused on awareness and intervention outcomes, with limited attention to the development of standardized and psychometrically validated instruments for assessing cybersecurity literacy among lower secondary school students, particularly within urban environments such as Bangkok (Sudthongkhong et al., 2026). This lack of validated measurement tools limits the ability to systematically evaluate students' self-reported cybersecurity knowledge, awareness, and cybersecurity-related practices and to design evidence-based interventions for improving digital safety and reducing cyber-related risks. In particular, there remains a need for an assessment scale that reflects the multidimensional nature of cybersecurity literacy and is appropriate for Grade 9 students in the Thai urban school context. Grade 9 students are a particularly relevant group for initial validation because they are at the final stage of lower secondary education, typically aged 13–15 years, and are increasingly expected to use digital technologies with greater independence as they prepare to transition to upper secondary or vocational education.

Given these gaps, there is a critical need to develop an assessment tool and examine its initial validity and reliability

evidence in relation to the multidimensional nature of cybersecurity literacy among adolescents. Therefore, this study aims to develop and validate a Cybersecurity Literacy Assessment Scale (CLAS) for lower secondary school students in an urban educational context, using evidence from Grade 9 students in Bangkok, Thailand. The scale was constructed based on synthesized theoretical frameworks and empirical evidence, and its initial psychometric properties were examined through expert-based content validation, confirmatory factor analysis, composite reliability, and supplementary analyses of convergent and discriminant validity. The findings of this study are expected to contribute preliminary evidence to the conceptualization and measurement of cybersecurity literacy and to inform the development of educational strategies aimed at enhancing digital safety, promoting responsible online behavior, strengthening digital resilience, and supporting safer digital participation among youth in Thailand and similar urban contexts.

2. Research Objectives

1) To synthesize the components and indicators of cybersecurity literacy for lower secondary school students.

2) To develop the Cybersecurity Literacy Assessment Scale (CLAS) and examine its content validity.

3) To examine the construct validity and reliability of the developed scale.

3. Methodology

3.1 Research Design

This study employed an exploratory sequential mixed-methods design to develop and validate the Cybersecurity Literacy Assessment Scale (CLAS) for lower secondary school students. This design was appropriate for instrument development because it allowed the constructs and indicators to be first explored through qualitative synthesis and then empirically validated using quantitative data (Creswell & Plano Clark, 2018). The study was conducted in three sequential phases: qualitative exploration, instrument development, and quantitative validation. The qualitative phase informed the conceptual framework and item development, while the quantitative phase examined the proposed factorial structure and reliability of the scale through confirmatory factor analysis (CFA) and composite reliability (CR), together with supplementary analyses of convergent and discriminant validity.

3.2 Research Setting

The study was conducted in Bangkok, Thailand, representing an urban educational context characterized by high levels of digital technology usage and internet accessibility among adolescents, as reflected in national and regional reports on internet penetration, mobile connectivity, and social media use in Thailand (We Are Social Thailand, 2025). Bangkok was selected as an urban study context because adolescents in the area have intensive access to digital communication, social media, and online learning environments, which may increase their exposure to privacy, security, and harmful-interaction risks (DQ Institute, 2019; eSafety Commissioner, 2025; Sudthongkhong et al., 2026). Therefore, Bangkok provides an appropriate context for developing and validating an assessment scale that reflects real-world digital behaviors and cybersecurity challenges faced by lower secondary school students, particularly in urban educational settings where adolescents' digital participation is intensive and closely linked to online safety concerns (DQ Institute, 2019; eSafety Commissioner, 2025; Sudthongkhong et al., 2026). Although the scale is intended for lower secondary students, the empirical validation in this study focused specifically on Grade 9 students, who were selected because they are at the final stage of lower secondary education and are typically between 13 and 15 years old, a developmental period in which adolescents increasingly use digital devices, social media platforms, online communication tools, and digital learning environments with greater autonomy. At this stage, students are also preparing to transition to upper secondary or vocational education, where independent digital participation becomes more intensive.

3.3 Participants

The target population comprised lower secondary school students at the Matthayomsuksa 3 (M.3; Grade 9) level, aged 13–15 years, enrolled in secondary schools under the Bangkok Secondary Educational Service Area Offices, totaling 35,954 students. For clarity, the empirical sample in this study was limited to Grade 9 students, while the broader scale development framework was designed for lower secondary education. Therefore, the findings should be interpreted as initial validation evidence for Grade 9 students rather than as evidence for all lower secondary grade levels. A sample of 455 students was selected using a multi-stage random sampling technique to obtain participants from selected schools under the Bangkok Secondary Educational Service Area Offices, as this approach is appropriate for educational research involving large populations distributed across multiple institutional units or geographical areas (Creswell & Creswell, 2018; Cochran, 1977). The sampling process involved selecting schools from the Bangkok Secondary Educational Service Area Offices and subsequently selecting eligible Grade 9 students from the participating schools. Inclusion criteria were as follows: 1) Enrollment in Matthayomsuksa 3 (M.3; equivalent to Grade 9) level and 2) Basic ability to use digital devices. Students who were unable to complete the questionnaire or who did not provide assent were excluded from the study. The sample size was considered adequate for confirmatory factor analysis, as it exceeded recommended thresholds

for structural equation modeling, which typically suggest a minimum sample size of 200 or an acceptable ratio of participants to estimated parameters, depending on model complexity and estimation method (Brown, 2015; Hair et al., 2019; Kline, 2016).

3.4 Research Procedure

The research procedure was conducted in three sequential phases in accordance with the exploratory sequential mixed-methods design, as follows:

3.4.1 Phase 1 Qualitative Exploration

The components and indicators of cybersecurity literacy were synthesized through document analysis and literature review, which are appropriate qualitative approaches for identifying, organizing, and interpreting conceptual patterns across theoretical frameworks, policy documents, and empirical studies (Bowen, 2009; Krippendorff, 2018; Snyder, 2019). Relevant theoretical frameworks—including digital competence models (e.g., DigComp 2.2) and digital citizenship frameworks—were systematically reviewed to identify core aspects related to cybersecurity literacy. The findings were analyzed using content analysis, a systematic approach for interpreting textual data and identifying meaningful categories, themes, and conceptual relationships (Bowen, 2009; Krippendorff, 2018), and were subsequently integrated into a conceptual framework. Cybersecurity literacy was conceptualized as a multidimensional construct comprising four key components: 1) protecting devices and digital content, 2) protecting personal data and privacy, 3) safe and secure use, and 4) secure identity management, in alignment with international digital competence and digital citizenship frameworks that emphasize online safety, privacy protection, secure technology use, and responsible digital identity management (Vuorikari et al., 2022; DQ Institute, 2019; Ribble, 2015). The results of this phase informed the development of the initial item pool and the specification of the four-component measurement model.

3.4.2 Phase 2 Instrument Development

Scale items were generated based on the identified components and indicators, following established principles of instrument development that emphasize construct definition, item-content alignment, and the systematic translation of theoretical dimensions into measurable indicators (DeVellis, 2017; Boateng et al., 2018). Initially, an item pool of 90 items was generated to represent the four components and nine indicators identified in the qualitative synthesis. The research team developed the items by translating each indicator into observable statements reflecting students' knowledge, awareness, and cybersecurity-related practices in everyday digital contexts. The items were designed to be age-appropriate, contextually meaningful, and aligned with the lived experiences of Grade 9 students, including situations related to digital devices, social media platforms, online communication, personal data protection, privacy settings, and digital identity management.

The initial item pool was reviewed for clarity, age appropriateness, non-duplication, and alignment with the operational definitions of each component. The review focused on vocabulary difficulty, sentence length, item redundancy, relevance to Grade 9 students' digital experiences, and consistency between each item and its intended indicator. Items with unclear wording, overlapping meanings, or weak alignment with the operational definitions were revised, combined, or removed. After this internal review, 30 items were retained across four components and nine indicators.

The preliminary instrument was evaluated for content validity by a panel of five experts using the Content Validity Index (CVI), a widely used method for determining the relevance and representativeness of items in scale development studies (Lynn, 1986; Polit & Beck, 2006; Yusoff, 2019). The expert panel consisted of specialists in cybersecurity, educational technology, measurement and evaluation, and lower secondary education. Experts rated each item on its relevance using a four-point scale (1 = not relevant, 2 = somewhat relevant, 3 = quite relevant, and 4 = highly relevant), with ratings of 3 or 4 considered indicative of content validity.

The item-level CVI (I-CVI) was calculated as the proportion of experts who rated each item as either 3 or 4. Items with I-CVI values of 0.80 or higher were retained, following established recommendations for content validation involving expert panels of three or more reviewers (Lynn, 1986; Polit & Beck, 2006; Yusoff, 2019). The scale-level CVI (S-CVI) was also computed to assess the overall content validity of the instrument. Because all items met the acceptable I-CVI threshold, no item was removed after expert validation; however, minor wording refinements were made based on expert feedback where appropriate. The refined 30-item CLAS was then prepared for quantitative validation with Grade 9 students in Bangkok.

3.4.3 Phase 3 Quantitative Validation

The refined instrument was administered to 455 Grade 9 students to conduct an initial empirical examination of the proposed measurement structure and reliability of the Cybersecurity Literacy Assessment Scale. Prior to analysis, the returned questionnaires were screened for completeness and suitability. The quantitative validation phase aimed to examine whether the theoretically specified four-component structure of the CLAS was supported by empirical data. The

results of this phase provided initial evidence regarding the proposed factorial structure and reliability of the developed scale, while also identifying limitations in convergent and discriminant validity.

3.5 Data Collection

Data collection was conducted in alignment with the exploratory sequential mixed-methods design. In the qualitative phase, data were obtained through document analysis and literature review to establish the conceptual framework. Expert judgments were then collected from five specialists in cybersecurity and related fields to evaluate the content validity of the developed items. In the quantitative phase, data were collected from Grade 9 students in Bangkok, Thailand, between November and December 2025, during the first semester of the 2025 academic year, after ethical approval had been obtained on August 5, 2025. The finalized Cybersecurity Literacy Assessment Scale was administered as a structured questionnaire in classroom settings with the cooperation of school administrators and teachers. Students responded to each item using a three-category response format consisting of Yes, No, and Uncertain. For scoring purposes, Yes was coded as 1, whereas No and Uncertain were coded as 0. This scoring approach represented confirmed endorsement of the knowledge, awareness, or practice described by each item. Although No and Uncertain represent conceptually different response states, neither response indicated confirmed endorsement and they were therefore assigned a score of 0 in the present study. Participation was voluntary, and data collection was conducted anonymously without collecting personally identifiable information. Students were encouraged to respond according to their actual knowledge, awareness, and usual digital practices and were informed that their responses would be used only for research purposes. Completed questionnaires were screened for completeness prior to statistical analysis.

3.6 Data Analysis

Data analysis was conducted in alignment with the exploratory sequential mixed-methods design to address the research objectives. In the qualitative stage, content analysis was used to synthesize the components and indicators of cybersecurity literacy (Krippendorff, 2018). The findings informed the development of the conceptual framework and measurement instrument. Content validity was evaluated using the Content Validity Index (CVI), including both item-level (I-CVI) and scale-level (S-CVI) indices. In the quantitative stage, preliminary analyses, including descriptive statistics, missing data screening, item response distribution, and inter-item correlations, were conducted using IBM SPSS Statistics.

Construct validity was examined through confirmatory factor analysis (CFA) conducted using jamovi version 2.3.28 with the SEMLj module. CFA was used to test the hypothesized four-factor measurement model derived from the qualitative synthesis and expert validation. Because the CLAS items were dichotomously scored (0/1), the observed indicators were specified as categorical variables. The model was estimated using diagonally weighted least squares (DWLS) with robust standard errors. CFA was selected because the four-component structure was specified a priori based on literature synthesis, theoretical frameworks, and expert-based content validation rather than being derived solely from empirical exploration. Therefore, the purpose of the quantitative validation phase was to examine whether the theoretically specified measurement model was supported by the empirical data. No error covariances were added unless theoretically justified. Modification indices were reviewed only to identify potential areas for future item refinement rather than to capitalize on chance. Model fit was evaluated using multiple fit indices, including χ^2/df, GFI, AGFI, NFI, TLI, CFI, RMSEA, RMR, and SRMR, as the use of multiple fit indices is recommended to provide a more comprehensive evaluation of measurement model adequacy (Hu & Bentler, 1999; Schermelleh-Engel et al., 2003; Kline, 2016; Hair et al., 2019).

Additional psychometric analyses were conducted to examine reliability and supplementary evidence of convergent and discriminant validity. Reliability was assessed using composite reliability (CR) to examine the internal consistency of the measurement components, as CR is considered suitable for evaluating reliability in latent variable models and is commonly used in structural equation modeling and confirmatory factor analysis (Fornell & Larcker, 1981; Raykov, 1997; Hair et al., 2019). Average Variance Extracted (AVE) was used as a supplementary indicator of convergent validity, while the Fornell–Larcker criterion and the Heterotrait–Monotrait ratio of correlations (HTMT) were used as supplementary checks of discriminant validity (Fornell & Larcker, 1981; Henseler et al., 2015). These additional analyses were used to support a cautious interpretation of the measurement model and to identify areas for future item refinement.

3.7 Ethical Considerations

This study was approved by the relevant institutional ethics committee under proposal number KMUTT-IRB-2025/0717/197. The certificate of approval was issued on August 5, 2025. Written informed consent from parents or legal guardians and student assent were obtained prior to participation. Participation was voluntary, and all responses were kept confidential and used solely for research purposes.

4. Results

4.1 Components and Indicators of Cybersecurity Literacy

The synthesis of relevant literature, digital competence frameworks, digital citizenship frameworks, and cybersecurity

education studies resulted in a multidimensional framework of cybersecurity literacy for lower secondary school students.

For measurement purposes in this study, cybersecurity literacy was operationalized in terms of students' self-reported knowledge, awareness, and cybersecurity-related practices regarding the safe and responsible use of digital technologies. Based on the synthesis, cybersecurity literacy was organized into four interrelated components comprising nine indicators. The four components included 1) protecting devices and digital content, 2) protecting personal data and privacy, 3) safe and secure use, and 4) secure identity management. Together, these components and indicators reflect students' self-reported knowledge, awareness, and cybersecurity-related practices regarding the safe and responsible use of digital technologies. The operational definitions and indicators of each component are presented in Table 1.

Table 1. Components and Indicators of Cybersecurity Literacy

Component	Operational Definition	Indicators
1. Protecting Devices and Digital Content	The ability to protect digital devices and digital content by understanding risks and threats in digital environments, recognizing safety and security measures, and exercising caution regarding credibility and privacy.	1.1 Protecting devices and digital content 1.2 Understanding risks and threats in the digital world 1.3 Recognizing safety and security measures 1.4 Exercising caution regarding credibility and privacy
2. Protecting Personal Data and Privacy	The ability to protect personal data and privacy in digital environments, including understanding how personally identifiable information can be used and shared while protecting oneself and others from potential harm.	2.1 Protecting personal data 2.2 Protecting privacy in the digital world
3. Safe and Secure Use	The ability to use digital tools effectively to manage cybersecurity risks and cyber threats, as well as to protect digital content and digital infrastructure.	3.1 Ability to use digital tools safely and effectively
4. Secure Identity Management	Knowledge and understanding of secure digital identity management, including the creation and maintenance of digital identities through safe, responsible, and ethical online practices.	4.1 Managing digital identity securely 4.2 Creating and maintaining digital identity through safe, responsible, and ethical online practices

As shown in Table 1, the identified components represent both technical and behavioral aspects of cybersecurity literacy. Protecting devices and digital content focuses on device security, digital content protection, awareness of risks and threats, and caution regarding credibility and privacy. Protecting personal data and privacy emphasizes the safeguarding of personal information and privacy in digital environments. Safe and secure use concerns the ability to use digital tools safely and effectively and the appropriate management of cybersecurity risks in everyday digital activities. Secure identity management focuses on the safe, responsible, and ethical management of students' digital identities. Together, these components and indicators provided the conceptual foundation for developing the Cybersecurity Literacy Assessment Scale (CLAS). They guided the construction of the initial item pool and ensured that the scale reflected the core domains of cybersecurity literacy relevant to lower secondary students.

4.2 Development and Content Validity of the Cybersecurity Literacy Assessment Scale (CLAS)

Based on the components and indicators identified in the previous section, the Cybersecurity Literacy Assessment Scale (CLAS) was developed as a 30-item instrument to assess lower secondary students' self-reported knowledge, awareness, and cybersecurity-related practices regarding the safe and responsible use of digital devices, social media platforms, and digital technologies. The items were organized according to the four components and nine indicators of cybersecurity literacy. The structure of the scale is presented in Table 2, and the full version of the CLAS items is provided in Appendix A.

The 30 items were designed to reflect students' everyday digital experiences, including the use of digital devices, social media platforms, online communication, personal data protection, privacy management, and digital identity management. Each item was assessed using a three-category response format consisting of Yes (scored as 1), No (scored as 0), and Uncertain (scored as 0), where higher scores indicate confirmation of the knowledge, awareness, or practice represented by the item. The wording of the items was reviewed to ensure clarity, age appropriateness, and alignment with the intended indicators before the instrument was submitted for expert validation.

Content validity was evaluated by five experts in cybersecurity, educational technology, measurement and evaluation, and lower secondary education. Each expert assessed the relevance of each item using a four-point relevance scale, ranging from 1 = not relevant to 4 = highly relevant. Ratings of 3 or 4 were considered relevant. The item-level Content Validity Index (I-CVI) was calculated as the proportion of experts who rated each item as relevant, while the scale-level Content Validity Index based on the average method (S-CVI/Ave) was calculated to summarize content validity at both the component and overall scale levels.

As shown in Table 3, the I-CVI values of the CLAS items ranged from .80 to 1.00, indicating that all items met the acceptable criterion for content validity. The S-CVI/Ave values for the four components ranged from .80 to .93, and the overall S-CVI/Ave was .91. These results indicated that the CLAS demonstrated satisfactory content validity at both the item and scale levels. The findings also suggested that the items were sufficiently relevant to the intended components and indicators of cybersecurity literacy.

Table 2. Structure of the Cybersecurity Literacy Assessment Scale

Component	Indicator	No. of Items	Item Numbers
1. Protecting Devices and Digital Content	1.1 Protecting devices and digital content	3	1–3
	1.2 Understanding risks and threats in the digital world	2	4–5
	1.3 Recognizing safety and security measures	3	6–8
	1.4 Exercising caution regarding credibility and privacy	4	9–12
2. Protecting Personal Data and Privacy	2.1 Protecting personal data	4	13–16
	2.2 Protecting privacy in the digital world	3	17–19
3. Safe and Secure Use	3.1 Ability to use digital tools safely and effectively	3	20–22
4. Secure Identity Management	4.1 Managing digital identity securely	4	23–26
	4.2 Creating and maintaining digital identity through safe, responsible, and ethical online practices	4	27–30
Total		30	1–30

Table 3. Content Validity of the Cybersecurity Literacy Assessment Scale

Component	No. of Items	I-CVI Range	S-CVI/Ave	Interpretation
1. Protecting Devices and Digital Content	12	.80–1.00	.92	Acceptable
2. Protecting Personal Data and Privacy	7	.80–1.00	.91	Acceptable
3. Safe and Secure Use	3	.80	.80	Acceptable
4. Secure Identity Management	8	.80–1.00	.93	Acceptable
Overall Scale	30	.80–1.00	.91	Acceptable

The development process, together with content validation by five experts, confirmed that the CLAS items were relevant to the intended components and indicators of cybersecurity literacy. Following expert review and item refinement, the final version of the CLAS consisted of 30 items across four components and nine indicators. The refined scale was subsequently prepared for empirical validation with Grade 9 students in Bangkok, Thailand.

4.3 Initial Evidence of Factorial Structure, Reliability, and Validity of the CLAS

The refined 30-item CLAS was administered to 455 Grade 9 students in Bangkok, Thailand to examine its proposed factorial structure, composite reliability, and supplementary evidence of convergent and discriminant validity. Confirmatory factor analysis (CFA) was conducted to test whether the empirical data supported the theoretically specified structure of cybersecurity literacy consisting of four components: protecting devices and digital content, protecting personal data and privacy, safe and secure use, and secure identity management. The results of the first-order CFA indicated that all observed variables had positive standardized factor loadings and were statistically significant at the .01 level. The standardized factor loadings ranged from .30 to .77. Although all loadings were positive and statistically significant, several items had modest loadings, indicating that their relationships with the intended components were relatively weak. Therefore, statistical significance alone should not be interpreted as evidence that all items performed adequately. The highest loading was found in the safe and secure use component, while the lowest loading was found in the protecting devices and digital content component. The summary of standardized factor loadings and explained variance is presented in Table 4.

Table 4. Ranges of Standardized Factor Loadings and Explained Variance for the CLAS Components

Component	No. of Items	Standardized Loading Range	R^2 Range
1. Protecting Devices and Digital Content (PRO_DEV)	12	.30–.59	.09–.35
2. Protecting Personal Data and Privacy (PRO_PER)	7	.36–.62	.13–.39
3. Safe and Secure Use (SAFE_SEC)	3	.44–.77	.23–.59
4. Secure Identity Management (SECU_IDE)	8	.43–.61	.18–.37
Overall Scale	30	.30–.77	.09–.59

As shown in Table 4, all four components demonstrated positive and statistically significant standardized factor loadings. The protecting devices and digital content component showed standardized factor loadings ranging from .30 to .59. The protecting personal data and privacy component ranged from .36 to .62. The safe and secure use component ranged from .44 to .77, while the secure identity management component ranged from .43 to .61. Although several items demonstrated relatively low standardized factor loadings (e.g., around .30), they were retained due to their theoretical importance in representing essential domains of cybersecurity literacy. These relatively low loadings suggest that selected items should be reviewed in future studies to determine whether they should be reworded, replaced, or removed.

Additionally, these items showed acceptable content validity based on expert evaluation and contributed to preserving the conceptual breadth of the construct. This approach aligns with recommendations in measurement development literature that emphasize balancing statistical criteria with theoretical considerations. Nevertheless, future studies should further refine and revalidate these items.

The global fit indices indicated that the specified four-component model demonstrated acceptable overall model fit. However, global model fit was interpreted together with the magnitude of the standardized factor loadings and supplementary evidence of convergent and discriminant validity. As presented in Table 5, the first-order four-component CFA model demonstrated acceptable to good global fit with the empirical data. The chi-square value was 385.18 with 309 degrees of freedom and a p-value of .002. Although the chi-square test was statistically significant, which is common in models with moderate to large sample sizes, the χ^2/df value was 1.247, indicating a good fit. Other fit indices also met or exceeded recommended criteria, including GFI = .950, AGFI = .930, NFI = .970, TLI/NNFI = .990, CFI = 1.00, RMSEA = .016, and SRMR = .034, indicating acceptable global model fit, although these indices should be considered together with the relatively modest factor loadings and the limitations in convergent and discriminant validity reported below.

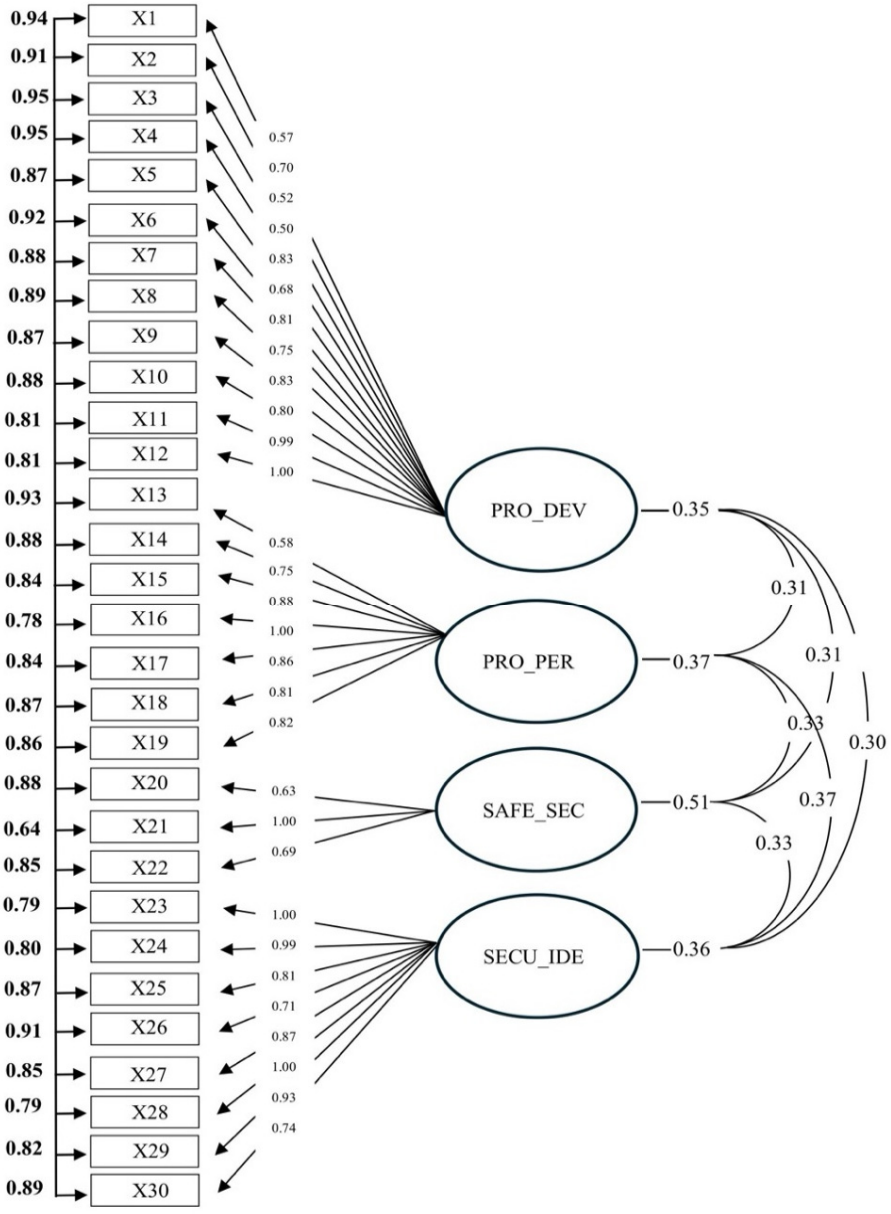

Figure 1. Results of the Confirmatory Factor Analysis of the Cybersecurity Literacy Assessment Scale (CLAS)

Table 5. Model Fit Indices of the First-Order Four-Component CFA Model

Fit Index	Recommended Criteria	Obtained Value	Interpretation
χ^2	—	385.18	—
df	—	309	—
χ^2/df	< 2.00	1.247	Good fit
GFI	≥ .95	.950	Acceptable
AGFI	≥ .90	.930	Acceptable
NFI	≥ .95	.970	Good fit
TLI / NNFI	≥ .95	.990	Good fit
CFI	≥ .95	1.00	Good fit
RMSEA	< .05	.016	Good fit
RMR	< .05	.034	Good fit
SRMR	< .05	.034	Good fit

Taken together, the CFA results indicated that the hypothesized four-component model demonstrated acceptable global fit with the empirical data. All 30 items had positive and statistically significant loadings on their intended components; however, several loadings were modest. Therefore, the CFA results provide preliminary evidence regarding the proposed factorial structure rather than conclusive evidence of construct validity. The interpretation should also consider the limitations in convergent and discriminant validity reported in the following analyses. Reliability evidence was further examined using composite reliability (CR). The results are presented in Table 6.

Table 6. Composite Reliability and Average Variance Extracted of the Cybersecurity Literacy Assessment Scale

Component	No. of Items	AVE	CR	Interpretation
1. Protecting Devices and Digital Content	12	.207	.750	CR acceptable; AVE below threshold
2. Protecting Personal Data and Privacy	7	.260	.706	CR acceptable; AVE below threshold
3. Safe and Secure Use	3	.356	.610	CR below the recommended .70 criterion; AVE below threshold
4. Secure Identity Management	8	.285	.759	CR acceptable; AVE below threshold

As shown in Table 6, the CR values ranged from .610 to .759, while the AVE values ranged from .207 to .356. The components of protecting devices and digital content, protecting personal data and privacy, and secure identity management showed CR values above .70, indicating acceptable composite reliability. The safe and secure use component yielded a CR value of .610, which was below the commonly recommended .70 criterion and indicates limited internal consistency requiring further item development and re-evaluation. This may be partly attributable to the limited number of items in this component and the relatively narrow coverage of safe and secure digital practices represented by the current items.

However, the AVE values for all four components were below the recommended threshold of .50, suggesting that convergent validity should be interpreted cautiously. Specifically, the AVE values were .207 for protecting devices and digital content, .260 for protecting personal data and privacy, .356 for safe and secure use, and .285 for secure identity management. These findings indicate acceptable composite reliability for three components, whereas the safe and secure use component requires further refinement. Moreover, the low AVE values indicate that convergent validity was not established across the four components.

Additional discriminant validity checks also suggested overlap among some components. The Fornell–Larcker results showed that the square roots of AVE for several components were lower than their correlations with other components, particularly between protecting devices and digital content and protecting personal data and privacy. The HTMT results similarly indicated high overlap for some component pairs, especially protecting devices and digital content with protecting personal data and privacy (HTMT = .965) and protecting personal data and privacy with secure identity management (HTMT = .903). These findings suggest that discriminant validity was not fully established for all component pairs. However, this overlap may reflect the conceptual relatedness of cybersecurity literacy subdimensions, as device protection, personal data protection, privacy management, and secure digital practices are closely connected in students' everyday digital behavior.

Taken together, the findings indicate acceptable composite reliability for three components, whereas the safe and secure use component demonstrated limited internal consistency and requires further refinement. The supplementary analyses did not establish adequate convergent validity for any of the four components and did not fully establish discriminant validity for all component pairs. These findings indicate the need for substantial item refinement and validation with independent samples. Future studies should expand the item pool, review items with modest factor loadings, and re-examine the reliability, convergent validity, discriminant validity, and dimensionality of the scale using independent samples.

5. Discussion

This study aimed to develop and validate the Cybersecurity Literacy Assessment Scale (CLAS) for lower secondary students, using empirical evidence from Grade 9 students in Bangkok, Thailand. The findings provide initial evidence that cybersecurity literacy among Grade 9 students can be conceptualized as a multidimensional construct consisting of four components: 1) protecting devices and digital content, 2) protecting personal data and privacy, 3) safe and secure use, and 4) secure identity management. These components reflect students' self-reported knowledge, awareness, and cybersecurity-related practices regarding the safe and responsible use of digital technologies.

The first major finding concerns the structure of cybersecurity literacy. The synthesis of relevant literature, digital competence frameworks, digital citizenship frameworks, and cybersecurity education studies resulted in four components and nine indicators. This structure is consistent with international digital competence and digital citizenship frameworks, which emphasize the protection of devices, personal data and privacy, safe digital engagement, and responsible digital identity management (Vuorikari et al., 2022; Office of the Education Council, 2023; DQ Institute, 2019). These findings suggest that cybersecurity literacy should not be viewed only as technical knowledge related to device protection, but rather as an integrated construct involving privacy protection, safe digital interaction, responsible online behavior, and digital identity management.

In the context of lower secondary students, this broader conceptualization is particularly important. Adolescents regularly engage with digital devices, social media platforms, online communication tools, and digital learning environments, which may increase their exposure to cyber-related risks, privacy concerns, harmful content, unsafe online interaction, and identity misuse (eSafety Commissioner, 2025; Thorn, 2024; Sudthongkhong et al., 2026). Therefore, cybersecurity literacy should be understood as an integrated form of self-reported digital knowledge, awareness, and cybersecurity-related practices that supports responsible participation in digital society. This interpretation is also consistent with the principles of digital citizenship, which emphasize ethical, respectful, and responsible participation in online environments (Office of the Education Council, 2023; DQ Institute, 2019).

The second finding relates to the development and content validity of the CLAS. The scale was developed as a 30-item instrument organized according to four components and nine indicators. The expert-based content validation results showed that the I-CVI values ranged from .80 to 1.00, while the overall S-CVI/Ave was .91. These values indicate that the items were sufficiently relevant to the intended components and indicators. The involvement of experts in cybersecurity, educational technology, measurement and evaluation, and lower secondary education strengthened the content validation process, consistent with recommended practices for establishing content validity in instrument development studies (Lynn, 1986; Polit & Beck, 2006). The results indicate that the experts judged the items to be relevant to the intended components and indicators. However, content validity evidence should not be interpreted as confirming the empirical dimensionality or overall psychometric adequacy of the scale.

The third finding concerns the initial empirical examination of the proposed factorial structure. The global CFA fit indices were broadly consistent with the proposed four-component model. The use of CFA was appropriate because the measurement model was theoretically specified in advance and empirically tested using multiple model fit indices, as recommended in measurement validation studies (Kline, 2016; Hair et al., 2019). Although some standardized factor loadings were relatively modest, all observed items had positive and statistically significant loadings on their intended components. The overall model fit indices also indicated an acceptable fit with the empirical data, including $\chi^2/df = 1.247$, GFI = .950, AGFI = .930, NFI = .970, TLI/NNFI = .990, CFI = 1.00, RMSEA = .016, RMR = .034, and SRMR = .034. These findings suggest that the proposed four-component model is a plausible preliminary representation of cybersecurity literacy among the participating Grade 9 students. Nevertheless, the low AVE values and incomplete discriminant validity evidence prevent a definitive conclusion regarding the adequacy and distinctiveness of the four components. However, the evidence should be interpreted as initial rather than conclusive psychometric support. Supplementary analyses indicated that convergent validity should be interpreted cautiously because the AVE values were below the recommended threshold across all components. In addition, selected discriminant validity checks suggested overlap among some components, particularly between protecting devices and digital content and protecting personal data and privacy. This overlap may be conceptually understandable because device protection, content protection, personal data protection, privacy management, and secure digital practices are closely connected in adolescents' everyday digital behavior. Therefore, the four components may be interpreted as closely related subdimensions of a broader cybersecurity literacy construct rather than as fully independent dimensions. Accordingly, the present findings should be interpreted as preliminary support for a four-component representation rather than as definitive evidence that the four components constitute clearly distinct dimensions. Future studies may further examine whether cybersecurity literacy is better represented as a higher-order construct.

The relatively modest standardized factor loadings of some items also require careful interpretation. Although these items

were retained because they represented theoretically important aspects of cybersecurity literacy and had acceptable content validity, their lower loadings suggest that item refinement is still needed. Future studies should review items with modest factor loadings to determine whether they should be reworded, replaced, or removed. Such refinement may help strengthen convergent validity, discriminant validity, and the overall internal structure of the CLAS while maintaining adequate conceptual coverage.

The reliability results were mixed across the four CLAS components. The composite reliability values ranged from .610 to .759. Three components—protecting devices and digital content, protecting personal data and privacy, and secure identity management—showed CR values above .70, indicating acceptable composite reliability. However, the safe and secure use component yielded a comparatively low CR value (.610), suggesting that this component requires further refinement. This may be partly attributable to the limited number of items in this component, as it consisted of only three items. In addition, the current items may represent a relatively narrow range of safe and secure digital practices. Future refinement should consider adding indicators related to evaluating online risks before clicking links or downloading files, using public Wi-Fi and shared devices safely, responding appropriately to suspicious online incidents, and applying basic security tools such as two-factor authentication, privacy settings, and secure application permissions. These additional indicators may strengthen the conceptual coverage and internal consistency of the safe and secure use component.

The findings have several theoretical and practical implications. Theoretically, this study contributes to the conceptualization of cybersecurity literacy as a multidimensional construct for lower secondary students. The four-component structure provides a basis for understanding cybersecurity literacy as a combination of device protection, privacy protection, safe digital use, and secure identity management. At the same time, the supplementary validity evidence suggests that these components should be understood as interrelated dimensions within a broader cybersecurity literacy framework. Practically, the current version of the CLAS may be used cautiously as a preliminary research or formative assessment tool to examine patterns in students' self-reported cybersecurity knowledge, awareness, and practices. It should not yet be used for high-stakes decisions, individual diagnosis, student ranking, or formal certification. The scale may also support the design of educational interventions, digital citizenship programs, and cybersecurity learning activities that address students' needs in urban digital environments. This is particularly relevant in Bangkok and similar urban contexts, where adolescents' intensive digital engagement may increase exposure to online risks and cybersecurity challenges (Sudthongkhong et al., 2026; eSafety Commissioner, 2025; Thorn, 2024).

In addition, the CLAS may help schools move beyond general digital literacy instruction toward more targeted assessment and development of safe and responsible digital practices. As cybersecurity-related concepts have been integrated into computing science and digital learning contexts, an assessment scale with preliminary psychometric evidence may provide formative information for curriculum development, instructional design, and future research, provided that its current validity limitations are recognized (Ministry of Education, 2017). By identifying patterns in students' self-reported responses across the four components, teachers and schools can design more focused learning activities related to device protection, personal data privacy, safe digital interaction, and responsible digital identity management. However, because this study provides initial validation evidence, the CLAS should be used primarily as a formative assessment and research tool while further psychometric refinement is undertaken.

Despite these contributions, several limitations should be acknowledged. First, the empirical validation was conducted with Grade 9 students in Bangkok, Thailand; therefore, generalizability to other grade levels, regions, or contexts should be examined in future research. Grade 9 students were selected as an appropriate group for initial validation because they are at the final stage of lower secondary education and are expected to engage in digital technologies with increasing independence. Nevertheless, the findings should not be generalized to all lower secondary students, other age groups, rural contexts, or different educational systems without further validation. Future studies should examine the CLAS across different grade levels, geographical regions, school types, and cultural contexts.

Second, although this study used CFA to validate a four-component model, future studies may further examine the structure using exploratory factor analysis with independent samples or cross-validation across different contexts. The decision to use CFA was based on the fact that the four-component structure was specified a priori through literature synthesis, theoretical frameworks, and expert validation. However, because the CLAS is a newly developed instrument, the absence of EFA with an independent sample remains a limitation. Future research should conduct EFA and CFA using separate samples to further examine the dimensionality and stability of the scale. In addition, future studies should replicate the categorical CFA using independent and more diverse samples to further examine the stability of the four-component structure under the current response format.

Third, some factor loadings were modest, and one component showed marginal composite reliability. Future studies should refine selected items, expand the safe and secure use component, and revalidate the scale with diverse student populations.

Fourth, supplementary analyses showed that the AVE values were below the recommended threshold across all components, suggesting that convergent validity should be interpreted cautiously. Selected discriminant validity checks also suggested overlap among some components, particularly between protecting devices and digital content and protecting personal data and privacy. Future studies should refine items with modest factor loadings, examine discriminant validity more rigorously, and consider whether cybersecurity literacy may be better represented as a higher-order construct with closely related subdimensions.

Fifth, because the quantitative data were collected using a self-report instrument at a single time point, the findings may be subject to common method bias. Although procedural remedies such as anonymity, voluntary participation, and clear questionnaire instructions were used, future studies should include additional statistical assessments of common method bias and consider multi-source or longitudinal designs.

Finally, the study did not fully examine students' response processes through formal pilot testing or cognitive interviews. Although item clarity and age appropriateness were reviewed by the research team and expert panel, future studies should include preliminary tryouts, cognitive interviews, or readability checks with students to examine how they interpret the items and response options. These efforts would strengthen the psychometric evidence of the CLAS and support its broader application in cybersecurity literacy assessment.

6. Conclusion

This study developed the Cybersecurity Literacy Assessment Scale (CLAS) for lower secondary students and provided initial validation evidence based on Grade 9 students in Bangkok, Thailand. The findings indicated that cybersecurity literacy comprises four components and nine indicators: protecting devices and digital content, protecting personal data and privacy, safe and secure use, and secure identity management. Based on this framework, a 30-item scale was constructed to assess students' self-reported knowledge, awareness, and practices related to safe and responsible digital technology use. Content validity was satisfactory, with I-CVI values ranging from .80 to 1.00 and an overall S-CVI/Ave of .91. Composite reliability was acceptable for three components, whereas the safe and secure use component had a CR value below the recommended criterion and requires further development. AVE values were below .50 for all four components, and the Fornell–Larcker and HTMT results indicated that discriminant validity was not fully established. Thus, the current findings do not provide conclusive evidence of convergent or discriminant validity, suggesting the need for further item refinement and validation with independent samples.

Overall, the CLAS is a theoretically grounded candidate instrument that provides preliminary psychometric evidence regarding the assessment of self-reported cybersecurity literacy among Grade 9 students in an urban Thai context. At its current stage of development, the scale may support formative educational research and preliminary needs assessment, but it should not be considered a fully validated instrument or used for high-stakes individual decisions. Further item refinement and validation with independent and more diverse samples are required before broader implementation. Future studies should validate the CLAS across broader samples and contexts to improve generalizability. They should also refine items with modest factor loadings, expand the safe and secure use component, examine convergent and discriminant validity more rigorously, and consider whether cybersecurity literacy may be represented as a higher-order construct with closely related subdimensions.

Acknowledgments

The authors gratefully acknowledge the experts in cybersecurity, educational technology, measurement and evaluation, and lower secondary education for their valuable review of the instrument's content validity and constructive feedback on item refinement. We also extend our appreciation to the participating school administrators, teachers, parents, and Grade 9 students under the Bangkok Secondary Educational Service Area Offices for their support and participation in this study.

Author contributions

Munchukarn Naktoen was responsible for conceptualization, methodology, synthesis of the components and indicators of cybersecurity literacy, and development of the scale items. Daruwan Srikaew and Sutiwat Supaluk were responsible for data collection and quantitative data analysis. Vitsanu Nittayathammakul contributed to methodology, validation, and manuscript revision. Duangkamon Winitkun contributed to methodology, validation, and review of the manuscript for language quality and methodological rigor. All authors contributed to the revision, read, and approved the final manuscript.

Funding

This work was supported by the Petchra Pra Jom Klao Master's Degree Research Scholarship from King Mongkut's University of Technology Thonburi.

Competing interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Informed consent

Obtained.

Ethics approval

The Publication Ethics Committee of the Redfame Publishing.

The journal's policies adhere to the Core Practices established by the Committee on Publication Ethics (COPE).

Provenance and peer review

Not commissioned; externally double-blind peer reviewed.

Data availability statement

The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

Data sharing statement

No additional data are available.

References

Advanced Info Service Public Company Limited [AIS]. (2025). Thailand Cyber Wellness Index 2025. https://sustainability.ais.co.th/th/sustainability-projects/thailands-cyber-wellness-index

Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quiñonez, H. R., & Young, S. L. (2018). Best practices for developing and validating scales for health, social, and behavioral research: A primer. *Frontiers in Public Health, 6,* Article 149. https://doi.org/10.3389/fpubh.2018.00149

Bowen, G. A. (2009). Document analysis as a qualitative research method. *Qualitative Research Journal, 9*(2), 27–40. https://doi.org/10.3316/QRJ0902027

Brown, T. A. (2015). *Confirmatory factor analysis for applied research* (2nd ed.). The Guilford Press.

Cochran, W. G. (1977). *Sampling techniques* (3rd ed.). John Wiley & Sons.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Creswell, J. W., & Plano Clark, V. L. (2018). *Designing and conducting mixed methods research* (3rd ed.). SAGE Publications.

DataReportal. (2025). *Digital 2025: Thailand*. https://datareportal.com/reports/digital-2025-thailand

DeVellis, R. F. (2017). *Scale development: Theory and applications* (4th ed.). SAGE Publications.

DQ Institute. (2019). DQ global standards report 2019: Common framework for digital literacy, skills and readiness.

eSafety Commissioner. (2025). Digital use and risk: Online platform engagement among children aged 10 to 15. Australian Government. https://www.esafety.gov.au/research/the-online-experiences-of-children-in-australia/report-digital-use-and-risk-among-children-aged-10-to-15

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18*(1), 39–50. https://doi.org/10.1177/002224378101800104

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage Learning.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8

Hu, L.-T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1–55. https://doi.org/10.1080/10705519909540118

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). The Guilford Press.

Krippendorff, K. (2018). *Content analysis: An introduction to its methodology* (4th ed.). SAGE Publications.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nursing Research, 35*(6), 382–385. https://doi.org/10.1097/00006199-198611000-00017

Ministry of Education. (2017). Learning standards and indicators for mathematics, science, and geography in the social studies, religion, and culture learning area (Revised Edition B.E. 2560 [2017]) under the Basic Education Core Curriculum B.E. 2551 [2008]. Bureau of Academic Affairs and Educational Standards, Office of the Basic Education Commission.

Office of the Education Council. (2023). Guidelines for developing collaborative networks to enhance digital intelligence skills among learners of all ages: Case studies from other countries and Thailand (Easy-to-understand edition). Office of the Education Council.

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. *Research in Nursing & Health, 29*(5), 489–497. https://doi.org/10.1002/nur.20147

Raykov, T. (1997). Estimation of composite reliability for congeneric measures. *Applied Psychological Measurement, 21*(2), 173–184. https://doi.org/10.1177/01466216970212006

Ribble, M. (2015). *Digital citizenship in schools: Nine elements all students should know* (3rd ed.). International Society for Technology in Education.

Rogers, S. (2024, November 7). International scammers steal over $1 trillion in 12 months in Global State of Scams Report 2024. Global Anti-Scam Alliance. https://www.gasa.org/knowledge-base/blog/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online, 8*(2), 23–74. https://doi.org/10.23668/psycharchives.12784

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sudthongkhong, C., Nonthasitthichai, P., Phungsombun, S., & Nittayathammakul, V. (2026). The development of mockumentary short film to support secondary school students' perceived awareness, empathy, and new perspectives on cyberbullying toward LGBTQ+ peers. *Journal of Education and Training Studies, 14*(3), 76–89. https://doi.org/10.11114/jets.v14i3.8587

Thai PBS News. (2025, February 13). Online crime losses reach 3.4 billion baht in less than two months of 2025. https://www.thaipbs.or.th/news/content/349248

Thorn. (2024). Youth perspectives on online safety, 2023. https://www.thorn.org/research/library/2023-youth-perspectives-on-online-safety/

Vuorikari, R., Kluzer, S., & Punie, Y. (2022). DigComp 2.2: The Digital Competence Framework for Citizens—with new examples of knowledge, skills and attitudes. *Publications Office of the European Union*. https://doi.org/10.2760/115376

We Are Social Thailand. (2025, February). Digital 2025: Your ultimate guide to the evolving digital world. *We Are Social*. https://wearesocial.com/th/blog/2025/02/digital-2025/

Yusoff, M. S. B. (2019). ABC of content validation and content validity index calculation. *Education in Medicine Journal, 11*(2), 49–54. https://doi.org/10.21315/eimj2019.11.2.6