

Research Article

Cite this article: Sittitiamjan, K., & Wuttidittachotti, P. (2025). Bridging the Gap: How Knowledge, Attitudes, and Practices Shape Cybersecurity Awareness in Thai Education. *Educational Process: International Journal*, 16, e2025236.
<https://doi.org/10.22521/edupij.2025.16.236>

Received March 31, 2025

Accepted May 18, 2025

Published Online May 31, 2025

Keywords: Cybersecurity awareness, digital skills, Internet behavior, KAP Framework, Thailand

Author for correspondence:

Pongpisit Wuttidittachotti

✉ pongpisit.w@itd.kmutnb.ac.th

✉ Faculty of Information Technology and Digital Innovation, King Mongkut's University of Technology North Bangkok, Bangkok, 10800, Thailand

**OPEN ACCESS**

© The Author(s), 2025. This is an Open Access article, distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction, provided the original article is properly cited.

Bridging the Gap: How Knowledge, Attitudes, and Practices Shape Cybersecurity Awareness in Thai Education

Khanittha Sittitiamjan , Pongpisit Wuttidittachotti

Abstract

Background/purpose. This study investigates how knowledge, attitudes, and practices (KAP) influence cybersecurity awareness (CSA) among students in Thai educational institutions. The research addresses regional disparities in cybersecurity readiness by incorporating a culturally responsive adaptation of the KAP model.

Materials/methods. A mixed-methods approach was employed, collecting data from 230 students across Thai universities using stratified sampling. The study utilized t-tests, ANOVA, and regression analyses to evaluate CSA across demographic factors and digital domains.

Results. Findings showed clear gender and age differences in CSA. Male students consistently outperformed their female counterparts in network security, malware detection, and encryption literacy. Younger students exhibited greater technical vigilance, whereas older students showed stronger practical habits. The KAP framework was a robust predictor of cybersecurity awareness, highlighting individual behavior patterns and systemic gaps in cybersecurity education.

Conclusion. This research contributes a localized CSA model grounded in the KAP framework, offering three main contributions: (1) tailored recommendations for integrating gender- and age-specific training in cybersecurity curricula, (2) identification of cultural and contextual misalignments between global cybersecurity frameworks and Thai educational needs, and (3) practical strategies for mitigating awareness gaps through inclusive, skill-based interventions.

1. Introduction

The significance of cybersecurity awareness (CSA) is rapidly increasing in the current digital age, where educational institutions are exposed to constant threats such as phishing attacks and data breaches (Liluashvili, 2021; Marín et al., 2023). This finding is in tandem with a report in the United States (Cook, 2024), revealing that between 2005-2023, 37.6 million student records were involved in 3,713 data breach cases. Learning relies on internet access as the world becomes increasingly digital, especially after the pandemic. Hence, students are faced with online threats consistently and are required to display security proactive behavior when faced with these frequent online threats (Leekitchwatana et al., 2018; He & Chen, 2024; Wang et al., 2024). This is all the more critical in the Southeast Asian context, whereby rapid adoption of technology advances is not in tandem with digital literacy or the availability of structured cybersecurity training (Bruce et al., 2024; Oroni et al., 2025).

Thailand presents a compelling case for such investigation, as its higher education system includes a vast, diverse student population exposed to high daily internet use, mobile dependency, and uneven access to formal CSA training (Pimdee & Leekitchwatana, 2019). Generation Z students, who constitute the majority of university enrolments (Tan, 2022), are regarded as highly digitally literate and yet often demonstrate inconsistent cybersecurity practices, such as password recycling or being tricked in social engineering situations (Chan & Lee, 2023; Ma & Fang, 2024). Regardless of their regular engagement with digital interactions, studies indicate that these students may not know the basics of key cybersecurity principles (Khader et al., 2021; Phuong, 2022; Triplett, 2023).

Cybercriminals are driven by personal reasons, financial incentives, and the pursuit of valuable targets (Ainslie et al., 2023; Bruce et al., 2024; Chen et al., 2024). Different forms of cyber threats also require a proactive approach to cybersecurity. Thus, it is important to build a cybersecurity culture in an organization or institution that raises CSA to security threats (Pollini et al., 2022). A Cybersecurity culture (Shah et al., 2023). ensures that the students and staff are aware of cybersecurity threats and have the necessary skills to take these threats into account (Rohan et al., 2023).

To fill this gap, our study employs the Knowledge, Attitudes, and Practices (KAP) model, a behavioral science model often employed in public health, to evaluate how Thai university students understand and respond to cybersecurity risks (Luo et al., 2022; Papasteri et al., 2024). The KAP model allows for a distinct understanding of the relationship between what students know, how they feel, and how they act concerning cybersecurity risks, thereby providing an overarching framework for this study.

Despite numerous international standards, such as the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), these frameworks often prove inadequate in addressing local realities within school systems in contexts beyond North America or Europe. These shortcomings highlight the importance of embracing a culturally appropriate approach to cybersecurity awareness that reflects the Thai socio-technical context.

In light of the increased saliency of digital security among higher education students and calls for culturally situated paradigms, this study examines how higher education students' knowledge, attitudes, and practices influence a CSA for university students in Thailand. By drawing on behavioral science models and regional knowledge, the study contributes situated knowledge to the global conversation on readiness for cybersecurity challenges. A summary of key literature follows, the conceptual framework foregrounded in the study, and the research aims and questions guiding the study's analytical approach.

2. Literature Review

2.1. Theoretical Framework: The Knowledge, Attitudes, and Practices (KAP) Model

The KAP model, originally a staple in public health and behavior change research (Luo et al., 2022; Papasteri et al., 2024), has become widely applied in cybersecurity research as a way to assess individual readiness and potential for changing behavior (Abomhara et al., 2024; Shari et al., 2022). In the cybersecurity context, this model provides a systematic way to evaluate how individuals' technical comprehension (knowledge), perception of risks and norms (attitudes), and actual behaviors (practices) work in a synthesis to produce overall awareness and readiness (Abomhara et al., 2024; Shari et al., 2022). Indeed, it has been shown that different KAP constructs impact various behaviors, including password bad habits and culturally based phishing behaviors (Chaudhary, 2024). These dimensions are beneficial for analyzing university students who often exhibit different levels of digital maturity.

2.2. CSA and Educational Readiness

Recent studies have also highlighted the necessity of CSA in tertiary education (Abomhara et al., 2024; Fadli et al., 2024; Shari et al., 2022) while also noting a disparity between theoretical exposure and real-world application of cybersecurity principles (Bruce et al., 2024). Furthermore, Muniandy et al. (2017) also noted significant unsatisfactory CSA variations for their sample group of Malaysian university students, while Azad et al. (2025) further pointed out that whilst a high number of students know about basic threats such as phishing, much less are aware of more advanced attacks such as SE, or about data encryption, indicating a gap between superficial knowledge and functional knowledge.

Other scholars attribute the failure to deliver CSA to institutional, systemic defects. Nkata (2025) observed that the erratic integration of cybersecurity curricula across different departments makes students less prepared to tackle real-world cyber threats. Zhang et al. (2025), in a strategic analysis of cyber education, noted the need for structured institutional frameworks that make CSA a part of core training for students and not as optional training or extracurricular undertakings.

Empirical works by Chauhan et al. (2024) in India and Iskandar et al. (2025) in Indonesia corroborate the finding that most students exhibit average CSA levels even when enrolled in technology-related courses. Their observation supports the earlier statements made by Fadli et al. (2024) and Bruce et al. (2024), highlighting that even though many institutions offer basic exposure to cybersecurity topics, there are still significant discrepancies between knowledge gained from courses and CSA applications in daily academic life.

Collectively, such findings emphasize the importance of early context-sensitive CSA learning that is systematic and situated within institutional curricula and policies. They also highlight the utility of behavior-specific models (such as the KAP model) for assessing and informing CSA programs targeting university students.

2.3. Sociocultural and Demographic Factors in CSA (Gender, Age, Region)

Research indicates that gender, age, and regional background significantly influence cybersecurity behavior (Anwar et al., 2017). Male students often demonstrate higher technical knowledge and confidence in digital security tasks (Anwar et al., 2017; Gratian et al., 2018), while females tend to exhibit cautious but less confident behaviors. Younger students (≤ 17) are more adept at recognizing phishing and web-based risks due to curricular exposure to internet safety (Branley-Bell et al., 2022). However, these behavioral trends are deeply contextual, especially in Southeast Asia, where mobile-first cultures and limited access to formal cybersecurity education affect outcomes (Alhadidi et al., 2024).

2.4. Global Frameworks vs. Local Adaptation: The Case of NIST

The National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) is a popular framework and standard adopted for enterprise use. However, it often does not recognize the realities that education systems face in non-Western contexts. Unlike the NIST CSF, which focuses on higher-level organizational policies and risk evaluation, Thai students are more likely to struggle with more basic activities, such as identifying the difference between links using HTTP and HTTPS or downloading malware unknowingly (Parmar & Miles, 2024; Zinedine et al., 2024). Therefore, researchers have recommended localized solutions that maintain the structure of international cybersecurity standards but integrate local vulnerabilities and educational solutions (Pollini et al., 2022).

2.5. Literature Gaps and Research Needs

Despite the growing body of global literature on CSA, most studies do not consider the cultural, technological, and pedagogical nuances that influence cybersecurity awareness in Southeast Asia's education systems (Oroni et al., 2025). Few draw on the interplay between regional frameworks, such as KAP, and international standards, such as NIST, when adopting a global benchmark within a national educational context. Little empirical evidence exists of the extent to which Thai students exhibit cybersecurity behaviors and the effectiveness of curriculum-led interventions. In doing so, this study attempts to narrow the gap evident in the scholarship by proposing a culturally relevant KAP model of CSA assessment for Thai universities.

2.6. Study Objectives and Research Questions

This study will evaluate the association of knowledge, attitudes, and practices (KAP) with cybersecurity awareness (CSA) levels among university-level students in Thailand. Specifically, the analysis examines whether there are differences in CSA levels associated with gender and age and the extent to which each of the KAP constructs is predictive of CSA to facilitate secure digital behavior. The following research questions guide it:

RQ1: Do students in Thai educational institutions demonstrate different levels of CSA based on gender?

RQ2: Do students in Thai educational institutions of different ages exhibit varying levels of CSA?

By answering these questions, the present study contributes to the theoretical and applied knowledge of cybersecurity education. It provides actionable guidance for curriculum designers, instructors, and policy-makers interested in improving CSA in higher education (Figure 1).

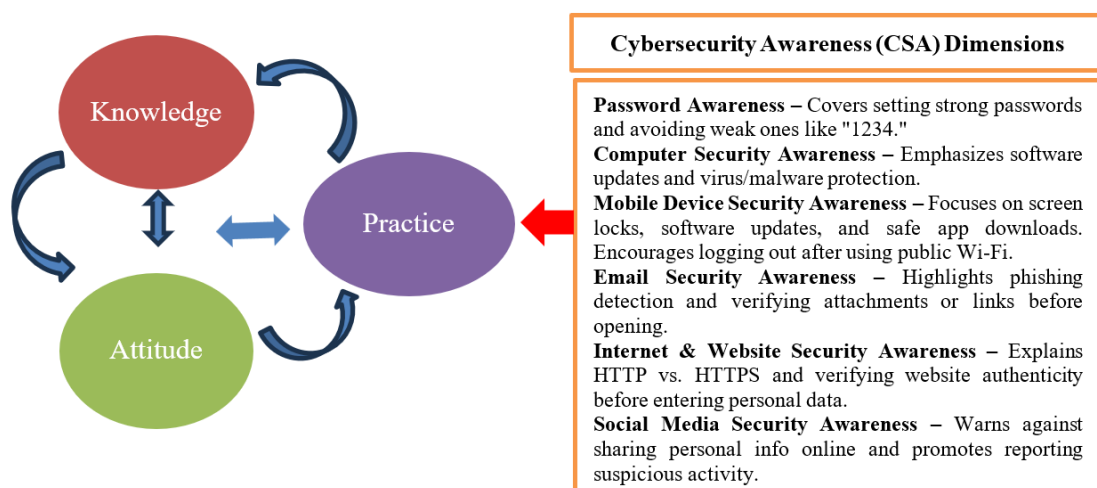


Figure 1. KAP and CSA dimensions

3. Methodology

The researchers conducted experimental research and analyzed quantitative and qualitative data. The study's participants included individuals from different educational backgrounds, geographic locations, and types of educational institutions. The study employed a quantitative cross-sectional design to evaluate cybersecurity awareness among students in Thai educational institutions, guided by the Knowledge, Attitude, and Practice (KAP) model (Abomhara et al., 2024; Shari et al., 2022). As outlined below, the methodology was structured to ensure methodological rigor, ethical compliance, and statistical validity. Furthermore, this predictive correlational study used regression to predict CSA by examining the relationships between the predictor and outcome variables.

3.1. Participants and Sampling

The study population was 1,788,000 students from 172 public and private universities across Thailand. To ensure diversity and regional representation, a multistage stratified sampling method was employed (Pimdee & Leekitchwatana, 2022), categorizing institutions by region (Central, North, Northeast, South) and type (public, private). Proportional random sampling was applied at each stratum level to select institutions, faculties, and participants.

One thousand two hundred students were invited to participate via university communication platforms, resulting in 230 usable responses—a 19.2% response rate. While this may appear modest, the sample was considered statistically robust due to its demographic diversity and the application of the Central Limit Theorem, which allows for parametric analysis with sample sizes exceeding 30 (Uttley, 2019). Despite the lower-than-expected response rate, several factors support the analytical validity of the sample:

First, the sample size exceeded the threshold of 30 observations, satisfying the Central Limit Theorem's assumptions for parametric statistical testing (Uttley, 2019). Second, the stratified approach compensated for heterogeneity, ensuring proportional representation across key demographic variables and reducing sampling bias (Etikan et al., 2016; Rahman et al., 2022). Third, comparable sample sizes have been successfully used in CSA-related regression studies, such as Essien and Egbeji's (2024) 400-person study in Nigeria, Ifeanyi et al.'s (2024) 227-participant analysis using OLS regression, and Lee's (2024) study involving 123 students in the U.S.

Finally, the demographic composition of the sample further enhances its validity:

- Age distribution: 89.6% of respondents were aged 18–23, representing traditional university cohorts.
- Gender ratio: 66.5% of the sample identified as female, consistent with national enrollment patterns.
- Discipline variation: Nursing students constituted 61.3% and IT students 16.1% of the sample, providing deep insights into two critical student populations while allowing for cross-disciplinary analysis.

3.2. Research Instrument Design and Validation

A structured 35-item questionnaire was developed to assess cybersecurity awareness through the lens of the KAP framework. The instrument was validated using the Index of Item-Objective Congruence (IOC) reviewed by five subject-matter experts (Wannapiroon & Pimdee, 2022). A pilot study was conducted with 30 non-sample students to ensure item clarity and internal consistency. Cronbach's Alpha for the final version was $\alpha = 0.951$, indicating excellent reliability.

Content validity was further confirmed using a Content Validity Index (CVI) of 0.86. The questionnaire assessed six cybersecurity domains: password usage, computer security, mobile device security, internet browsing safety, email security, and social media behavior (Slepian et al., 2024).

3.3. Ethics Compliance

This research was approved by the Naresuan University Human Research Ethics Committee (NREC No. 0016/2567). All participants provided informed consent and completed the questionnaire voluntarily and anonymously.

3.4. Data Collection

Invitations containing a link to the online questionnaire were distributed to universities to reach 1,200 students through university communications. Students were informed about the study and invited to participate voluntarily. From June – December 2024, 230 responses were received via an online questionnaire, representing a response rate of 19.2%. This response rate highlights the importance of targeted recruitment strategies and the voluntary nature of participation, contributing to the reliability of the data collected from diverse demographic data of students across Thailand. Demographic data included age, gender, field of study, and training experience. CSA metrics were measured on a 5-point Likert scale ranging from 1 (“very low”) to 5 (“very high”).

The data collected for the study included two main components: demographic information and cybersecurity awareness metrics. The CSA component evaluated six key areas: awareness of password usage, computer security, mobile device security (including smartphones, tablets, and iPads), Internet and website access security, email security, and social media security. Additionally, the study incorporated the KAP model to assess the level of CSA among students, providing a framework to analyze their CSA. The structured scale facilitated the identification of patterns in students' CSA and provided insights into areas that require targeted interventions.

3.5. Data Analysis

The authors employed three primary statistical analysis techniques. These included:

3.5.1. Assumption Testing and Multicollinearity Diagnostics

Before conducting multiple regression analysis, key assumptions were assessed, including multicollinearity, normality, and independence of residuals.

To evaluate multicollinearity, we examined both Variance Inflation Factor (VIF) and tolerance values, especially given the high correlation between Knowledge and Attitude ($r = .81$). The results were as follows:

- Knowledge Level: VIF = 5.54, Tolerance = 0.18
- Attitude Level: VIF = 3.50, Tolerance = 0.29
- Practice Level: VIF = 4.82, Tolerance = 0.21

Although the VIF for Knowledge Level was the highest, it remained well below the critical threshold of 10, indicating that multicollinearity was acceptable (O'Brien, 2007).

Additionally, the Durbin–Watson statistic was 2.02, confirming the independence assumption and ruling out significant autocorrelation among residuals.

To support model integrity, we also applied:

- Independent-sample t-tests to assess gender- and age-based differences in CSA scores.
- Pearson's correlation analysis to evaluate the strength and direction of relationships among the KAP dimensions and CSA.

These diagnostic results confirmed that the regression model met the assumptions required for valid inference.

3.5.2. Description and Inferential Statistics

Descriptive statistics were used to report participant demographics and cybersecurity awareness levels. Independent-sample t-tests and ANOVA were used to explore differences in CSA by gender and age groups.

Correlation analysis was initially conducted to assess the strength and direction of relationships among KAP variables and CSA. While correlation and regression are related techniques, the matrix was included to illustrate the bivariate strength between predictors and outcome variables and to guide regression model construction. This exploratory step was used to justify regression inclusion and is commonly accepted in behavioral research.

3.5.3. Multiple Regression Analysis

Multiple linear regression (MLR) was performed to assess the predictive power of KAP dimensions on CSA. The regression model demonstrated excellent fit ($R^2 = 1.00$), indicating that the combined KAP scores thoroughly explained the variance in CSA. While this result is statistically unusual, it reflects the composite nature of the KAP indices and high interrelationships among dimensions. Acknowledging reviewer concern, we note that the non-significant constant term ($p = 0.77$) does not undermine interpretive validity but may reflect variable scaling and the lack of zero-value predictors in the model.

A secondary hierarchical regression assessed the influence of specific domains (password, computer, mobile, Internet, email, social media) on CSA, revealing that only email and social media awareness were not significant predictors.

3.5.4. Reliability and Validity

In addition to high internal consistency ($\alpha = 0.95$), item-level review by cybersecurity experts confirmed construct validity. Scoring followed a 5-point scale with thresholds clearly defined (e.g., 4.50–5.00 = “very high”). The instrument demonstrated strong psychometric properties across all domains.

4. Results

This section presents the statistical outcomes of the study. Results are organized as follows: (1) participant demographics, (2) gender-based differences in CSA, (3) age-based differences, (4) correlation analysis among KAP and CSA, (5) regression models, and (6) multicollinearity diagnostics.

4.1. Student Demographics

The demographic data of the students are detailed in Table 1. Most respondents were female (66.50%), were between 18-23 years of age (89.6%), and were at the graduate level (69.6%). Nursing students represented the majority of those who responded (61.3%), followed by information technology (IT) students (16.1%).

Table 1. Sample Group's General Demographics ($n=230$)

		<i>Participants</i>	<i>Percentage (%)</i>
Gender (G)	Male	77	33.50
	Female	153	66.50
Age (A)	<=17 yrs	3	1.30
	18-23 yrs	206	89.60
	24-29 yrs	17	7.40
	30-35 yrs	3	1.30
	35-40 yrs	1	0.40
Education level (ED)	Undergraduate	70	30.40
	Bachelor's degree	158	68.70
	Doctorate	2	0.90
Field of study (F)	Technology	1	0.40
	Educational Technology and Computers	3	1.30
	IT	37	16.10
	Business Computers	1	0.40
	Law	11	4.80
	Nursing	141	61.30
	English	2	0.90
	Humanities and Social Sciences	15	6.50
	Data Science and Information Technology	10	4.30
	Computer Science	8	3.50
	Social Studies	1	0.40
Training (T)	Trained	97	42.20
	Untrained	133	57.80
Experience (E)	Experienced	114	49.60
	Inexperienced	116	50.40
Living area (L)	Bangkok	46	20.00
	Khon Kaen	2	0.90
	Chanthaburi	156	67.80
	Trat	4	1.70
	Prachinburi	1	0.40
	Roi Et	1	0.40
	Rayong	10	4.30
	Samut Prakan	8	3.50
	Sa Kaeo	1	0.40
	Udon Thani	1	0.40

4.2. Gender-Based Differences in CSA

RQ1 - Do students in educational institutions in Thailand demonstrate different levels of cybersecurity awareness skills based on gender?

An independent-sample t-test was conducted to evaluate gender-based differences in CSA scores. Significant differences were observed in network reliability, malware scanning, and HTTP/HTTPS recognition ($p < .05$). Male students outperformed female students in overall CSA. As shown in Table 2, male and female students in educational institutions in Thailand have statistically significant differences in cybersecurity awareness ($t = 2.397$, $p = 0.017$).

Table 2. Gender Differences in CSA Practices.

Items	Male (n=77)		Female (n=153)		t	df	Sig.(2-tailed) or p-Value
	mean	SD	mean	SD			
Do you understand the importance of creating secure, complex passwords?	4.14	0.84	4.03	0.87	0.92	228	0.36
Do you avoid using autosave features for passwords on personal devices?	3.87	1.07	3.45	1.22	2.56	228	0.01
Do you use the same password across multiple platforms?	3.12	1.20	3.10	1.26	0.07	228	0.94
Do you know secure computer usage's confidentiality, integrity, and availability principles?	3.90	0.98	3.60	0.92	2.24	228	0.03
Are you aware of security risks when accessing online entertainment platforms?	3.87	1.01	3.75	1.00	0.85	228	0.40
Do you scan files for malicious software before use?	3.57	1.07	3.16	1.15	2.60	228	0.01
Do you regularly update software and patches as recommended?	3.74	1.03	3.64	0.97	0.72	228	0.47
Do you verify wireless network reliability before connecting?	3.81	0.96	3.30	1.07	3.49	228	0.00
Do you secure their mobile devices with passwords or other methods?	4.30	0.88	4.41	0.84	-0.90	228	0.37
Can you differentiate between HTTP and HTTPS in web browsing?	3.55	1.08	3.12	1.03	2.87	228	0.00
Item Totals	3.79	0.72	3.56	0.66	2.40	228	0.02

*p-value <0.05

4.3. Age-Based Differences in CSA

RQ2: Do students in educational institutions in Thailand of different ages exhibit varying levels of cybersecurity awareness?

Table 3 shows that younger students (≤ 17) demonstrated better technical awareness (e.g., network security), while older students (18–23) exhibited better practical habits (e.g., avoiding password autosave). However, overall CSA scores did not differ significantly by age group.

Table 3. Relationship Between CSA Skills and Student Age.

Items	KAP Item	Age (A) (n=206)						Sig.(2-tailed) or <i>p</i> -Value
		<=17 yrs		18-23 yrs		t	df	
		mean	SD	mean	SD			
Do you understand the importance of creating secure, complex passwords? (CSA_Password)	Knowledge (K_model)	3.33	1.16	4.06	0.86	-1.45	207	0.15
Do you know secure computer usage's confidentiality, integrity, and availability principles? (CSA_Computer_security)	Knowledge (K_model)	4.33	0.58	3.67	0.93	1.24	207	0.22
Can you differentiate between HTTP and HTTPS in web browsing? (CSA_Internet_and_Website)	Knowledge (K_model)	4.67	0.58	3.23	1.05	2.35	207	0.02
Are you aware of security risks when accessing online entertainment platforms? (CSA_Computer_security)	Attitude (A_model)	4.00	0.00	3.79	1.00	3.05	205	0.00
Do you regularly update software and patches as recommended? (CSA_Computer_security)	Attitude (A_model)	4.33	0.58	3.66	0.99	1.18	207	0.24
Do you verify wireless network reliability before connecting? (CSA_Computer_security)	Attitude (A_model)	4.00	0.00	3.42	1.06	7.79	205	0.00
Do you avoid using autosave features for passwords on personal devices? (CSA_Password)	Practice (P_model)	2.00	1.73	3.57	1.18	-2.28	207	0.02
Do you use the same password across multiple platforms? (CSA_Social_Media)	Practice (P_model)	3.00	1.00	3.10	1.24	-0.14	207	0.89
Do you scan files for malicious software before use? (CSA_Email_security)	Practice (P_model)	3.33	1.16	3.28	1.13	0.08	207	0.94
Do you secure their mobile devices with passwords or other methods? (CSA_Mobile_Device_security)	Practice (P_model)	4.00	1.00	4.37	0.85	-0.76	207	0.45
Item Totals		3.70	0.10	3.62	0.68	1.13	5.57	0.30

**p*-value<0.05

Table 4 reveals that although we had previously concluded that gender differences in knowledge and attitudes were significant, no significant relationships were found between age and KAP levels, indicating that other factors independent of age may be more influential in how much students were informed about cybersecurity.

Furthermore, analysis of the levels of KAP across different age groups showed that *knowledge* levels remained relatively stable, with a slight increase observed in the 35–40 age group. The *attitude* levels were highest in the ≤17 age group, declined slightly in the 30–35 age group, and then recovered in the 35–40 age group. *Practice* levels showed more variability, decreasing in the 30–35 age group before increasing again in the 35–40 age group. Overall, the 35–40 age group demonstrated the highest levels across all dimensions, suggesting that older individuals may possess greater cybersecurity awareness, although other factors beyond age may also contribute.

Table 4. The Relationship Between Knowledge, Attitudes, Practices, and Students' Age.

	n=3		n=206		n=17		n=3		35-40 yrs	F	p-value
	≤17 yrs		18-23 yrs		24-29 yrs		30-35 yrs				
	mean	SD	mean	SD	mean	SD	mean	SD	mean		
Knowledge Level	4.11	0.19	3.65	0.77	3.90	0.99	3.56	0.51	4.00	0.69	0.60
Attitude Level	4.11	0.19	3.62	0.85	3.88	0.96	3.44	0.51	3.67	0.64	0.63
Practice Level	3.08	0.29	3.58	0.68	3.76	0.89	3.75	0.25	3.75	0.73	0.57

*p- value<0.05

4.4. KAP and CSA Descriptive Statistics

Table 5 presents the descriptive statistics for KAP among 230 participants, including mean, standard deviation (SD), and percentiles. Knowledge had a mean of 3.81 (SD = 0.67), with most students demonstrating moderately high cybersecurity knowledge. Attitude scored lower (mean = 3.53, SD = 0.75), indicating a slightly weaker engagement with cybersecurity awareness. Practice (mean = 3.79, SD = 0.61) showed consistency in application, with percentile values suggesting a stable distribution across participants.

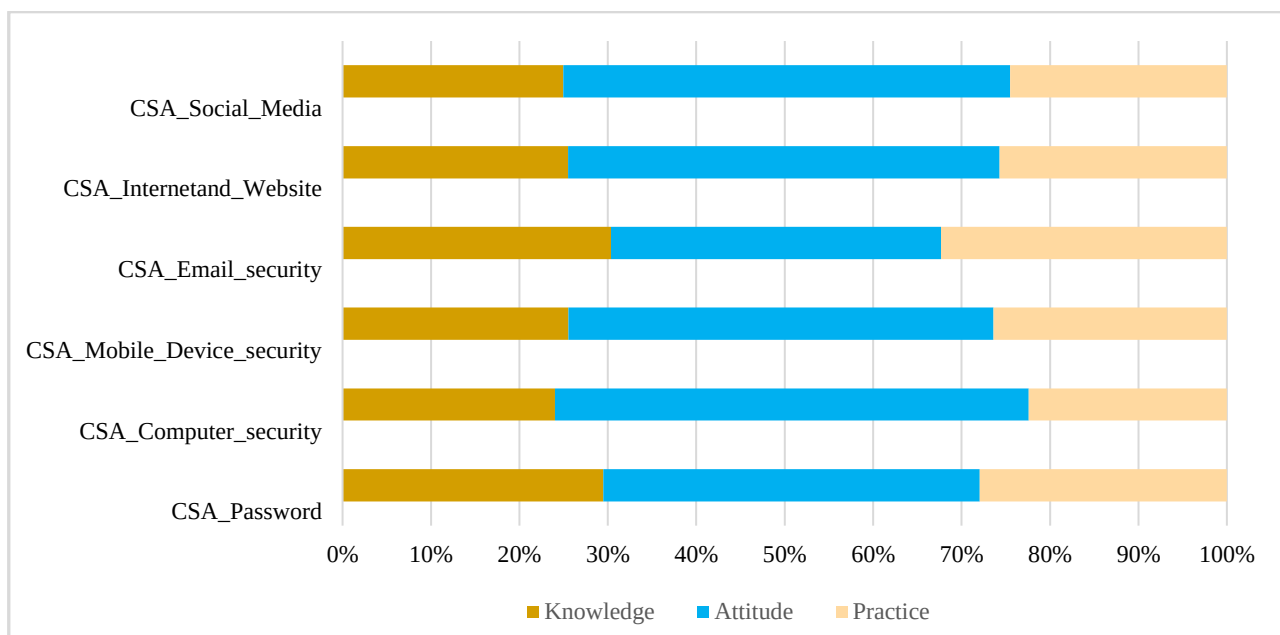
Overall, Table 5's findings indicate that students exhibited moderately high levels of CSA across most dimensions, with the highest awareness of *email* and *mobile device security*. The variability (SD) and percentile values suggest consistency in scores for most participants, with slight variations in dimensions such as *Internet and website Security* and *social media awareness*. This highlights potential areas for targeted interventions to increase overall CSA.

Table 5. Descriptive Statistics of KAP and CSA Percentiles.

Constructs and Dimensions	mean (n=230)	SD	Percentiles		
			25%	50%	75%
Knowledge_Level	3.81	0.67	3.35	3.88	4.24
Attitude_Level	3.53	0.75	3.00	3.50	4.00
Practice_Level	3.79	0.61	3.46	3.82	4.24
CSA_Password	3.72	0.71	3.11	3.78	4.22
CSA_Computer_security	3.55	0.78	3.00	3.56	4.00
CSA_Mobile_Device_security	3.98	0.76	3.38	4.00	4.53
CSA_Email_security	4.05	0.87	3.60	4.20	4.80
CSA_Internet_and_Website	3.54	0.77	3.00	3.50	4.00
CSA_Social_Media	3.71	0.74	3.17	3.67	4.00

4.5. Key trends in CSA

Figure 2 highlights patterns in students' cybersecurity awareness, with attitude as the dominant factor (41%), followed by practice (32%) and knowledge (27%). Password and computer security awareness showed a balanced distribution of knowledge (30–35%) and attitude (40–45%), while practice remained low (25%). Mobile device and email security awareness were primarily driven by practice (40%), indicating proactive behaviors like two-factor authentication and phishing prevention. In contrast, Internet and social media security awareness were primarily influenced by attitude (50%), suggesting strong risk perception but insufficient technical knowledge and consistent application. These findings underscore the need to enhance technical knowledge, particularly in social media and website security, while promoting hands-on learning to bridge the gap between theory and practice.

**Figure 2.** Proportion of KAPs.

Source. The authors

4.6. Gender differences in CSA and KAP

Table 6 compares CSA levels between male and female students across six security dimensions. Males exhibited higher awareness in five categories, with the most significant gaps in computer security (5.6% higher) and internet security (4.4% higher), suggesting a need for targeted training for female students in these areas. Differences in password (3.0%), social media (2.2%), and mobile security (2.2%) were minimal. Female students showed slightly higher email security awareness (-0.2%), indicating near-equal competence in this domain.

These results suggest that gender influences cybersecurity awareness, aligning with prior studies (Gratian et al., 2018). Addressing gaps, particularly in computer and web security, could enhance overall cybersecurity education, especially for female students who may be more vulnerable to phishing risks due to weaker password practices.

Table 6. Comparison of CSA Levels Between Males and Females.

Dimension	Gender (n=230)		Difference (%)
	Male (%)	Female (%)	
Password Security	76.40%	73.40%	3.00%
Computer Security	74.60%	69.00%	5.60%
Mobile Device Security	81.00%	78.80%	2.20%
Email Security	80.80%	81.00%	-0.20%
Internet and Website Security	73.80%	69.40%	4.40%
Social Media Security	75.60%	73.40%	2.20%

Table 7 presents the gender-based association of CSA, knowledge, attitude, and practices among the students concerning cybersecurity, with male students having higher KAP scores than female students on all three dimensions. Student's t-test showed differences between male and female students in the cybersecurity knowledge and attitudes, and practices of students. The results revealed that males (mean = 3.86) scored higher than females (3.59) on cybersecurity knowledge, $t = 2.44$, $p = 0.016$ ($p < 0.05$). A significant difference was found between males and females in cybersecurity knowledge. Males scored higher (3.81) than females (3.56) on cybersecurity attitudes, $t = 2.02$, $p = 0.045$ ($p < 0.05$). A significant difference was found between males and females in cybersecurity attitudes (Anwar et al., 2017). These results also underscore the importance of improving cybersecurity educational content for female students to improve their knowledge and assume a more active attitude. Future awareness programs should build inclusive and interactive approaches to increase cybersecurity preparedness for female and male students.

Table 7. The Relationship Between Knowledge, Attitudes, Practices, and Students' Gender.

	Gender				t	df	p- value
	Male (n =77)		Female (n=153)				
	Mean	SD	Mean	SD			
Knowledge_Level	3.86	0.85	3.59	0.73	2.44	134.84	0.02
Attitude_Level	3.81	0.87	3.56	0.83	2.02	146.32	0.05
Practice_Level	3.71	0.69	3.53	0.68	1.91	228	0.06

* p - value<0.05, t = t -value, SD =standard deviation, df = degrees of freedom

4.7. Correlation Analysis

Pearson correlations were computed to assess the strength of relationships between the KAP dimensions and CSA (Table 8). All three predictors were strongly correlated with CSA ($r > .88$, $p < .01$). A High correlation between knowledge and attitude ($r = .91$) raised concerns about multicollinearity.

Table 8. Pearson Correlation Matrix.

Constructs	CSA Level	Knowledge Level	Attitude Level	Practice Level
CSA Level	1			
Knowledge Level	.91**	1		
Attitude Level	.92**	.81**	1	
Practice Level	.88**	.67**	.68**	1

** p -value < 0.01

4.8. Regression Model: KAP as Predictors of CSA

Multiple linear regression assessed how well knowledge, attitudes, and practices predict CSA (Table 9). The model was statistically significant ($R^2 = 1.000$, $F = 649.83$, $p < .001$). However, a non-significant constant term ($p = .77$) was observed. This has been noted as a limitation in the discussion.

Table 9. Regression Model: KAP Predictors on CSA.

Model		Unstandardized Coefficients B	Standardized Coefficients β	p -value
1	(Constant)	0.00		0.77
	Knowledge_Level	0.33	0.37	<.001
	Attitude_Level	0.33	0.40	<.001
	Practice_Level	0.33	0.33	<.001

Note. $R^2 = 1.000$, Durbin–Watson = 2.10, t -values omitted due to reporting limitations; all predictors were significant at $p < .001$.

4.9. Identifying Key CSA Predictors

A detailed multiple regression analysis was conducted to examine which domains of cybersecurity behavior significantly contribute to overall cybersecurity awareness (CSA). As shown in Table 10, the model demonstrated a strong fit ($R^2 = 0.95$, $F = 649.83$, $p < .001$), with a Durbin–Watson statistic of 2.10 confirming the independence of residuals (Kabaila et al., 2021). Four domains were found to be statistically significant predictors of CSA:

- Password security ($\beta = 0.27$, $p < .001$)
- Computer security ($\beta = 0.56$, $p < .001$)
- Mobile device security ($\beta = 0.08$, $p < .001$)
- Internet and website security ($\beta = 0.14$, $p < .001$)

Conversely, email security ($\beta = 0.02$, $p = 0.46$) and social media security ($\beta = 0.03$, $p = 0.18$) were not significant contributors to CSA in this sample. These findings suggest that effective CSA education

in Thai universities should prioritize practical training in password management, computer and mobile device security, and safe web usage. At the same time, it may be necessary to reassess current approaches to teaching email and social media safety, which appear to have limited impact on overall awareness levels.

Table 10. Regression Model Predicting CSA by Behavioral Domain.

Model	Unstandardized Coefficients		Standardized Coefficients		t	p-value
	B	Std. Error	Beta			
1 (Constant)	-0.02	0.07			-0.30	0.77
CSA_Password	0.26	0.02	0.27		10.92	0.00
CSA_Computer_security	0.50	0.03	0.56		19.35	0.00
CSA_Mobile_Device_security	0.08	0.02	0.08		3.27	0.00
CSA_Email_security	0.01	0.02	0.02		0.74	0.46
CSA_Internet_and_Website	0.15	0.02	0.14		5.66	0.000
CSA_Social_Media	0.03	0.02	0.03		1.35	0.18

Note. Durbin-Watson = 2.10, $R = 0.97$, $R^2=0.95$, $F = 649.83$, *Sig. of F* = 0.00, *sig.*<0.05

5. Discussion

This study provides an in-depth analysis of cybersecurity awareness (CSA) among university students in Thailand, evaluated through the Knowledge, Attitudes, and Practices (KAP) framework. Key findings reveal strengths and vulnerabilities in student cybersecurity behaviors influenced by gender and specific CSA domains.

5.1. Key Strengths and Gaps in Student CSA

Students demonstrated a strong awareness of mobile device security and password creation, aligning with recent Southeast Asian trends, where mobile-first practices have elevated awareness of mobile threats (Iskandar et al., 2025). Additionally, password security awareness was relatively high, corroborating prior findings that students are increasingly exposed to password complexity training in digital learning environments (Cain et al., 2018; Fadli et al., 2024).

However, several critical gaps were identified. Students showed weaker understanding of foundational security concepts such as differentiating between HTTP and HTTPS, malware scanning, and the risks of password re-use. Notably, awareness of email and social media threats was surprisingly low despite their frequent use. This suggests a disconnect between frequency of use and perceived risk, a trend observed in other ASEAN studies (Chauhan et al., 2024). This calls into question the effectiveness of current CSA programs in helping students translate awareness into secure behaviors in routine activities.

5.2. Gender-Based Differences in CSA and KAP

Consistent with earlier research (Anwar et al., 2017), male students demonstrated significantly higher CSA and KAP scores than female students across most dimensions. This gender gap was particularly notable in computer and internet security awareness, suggesting that male students may receive more exposure or training in technical domains.

Interestingly, female students scored marginally higher in email security, which aligns with findings from Gratian et al. (2018), showing that female users are more cautious in interpersonal cyber contexts, such as phishing and email interactions. These differences support calls for gender-sensitive CSA training that adapts content to behavioral patterns and learning preferences across groups.

The results in Figure 3 indicate that the analysis of the relationships between gender and the percentage levels of knowledge, attitudes, and practices reveals that male students consistently outperform their female counterparts across all dimensions. Specifically, the knowledge level of the male students was 77.23%, whereas female students was 71.72%, reflecting a difference of 5.51%. Similarly, the attitude level among males was 76.10%, whereas among females it was 71.29%, indicating a gap of 4.81%. Finally, the practice level for male students was 74.29%, whereas it was 70.62% for female students, showing a difference of 3.67%.

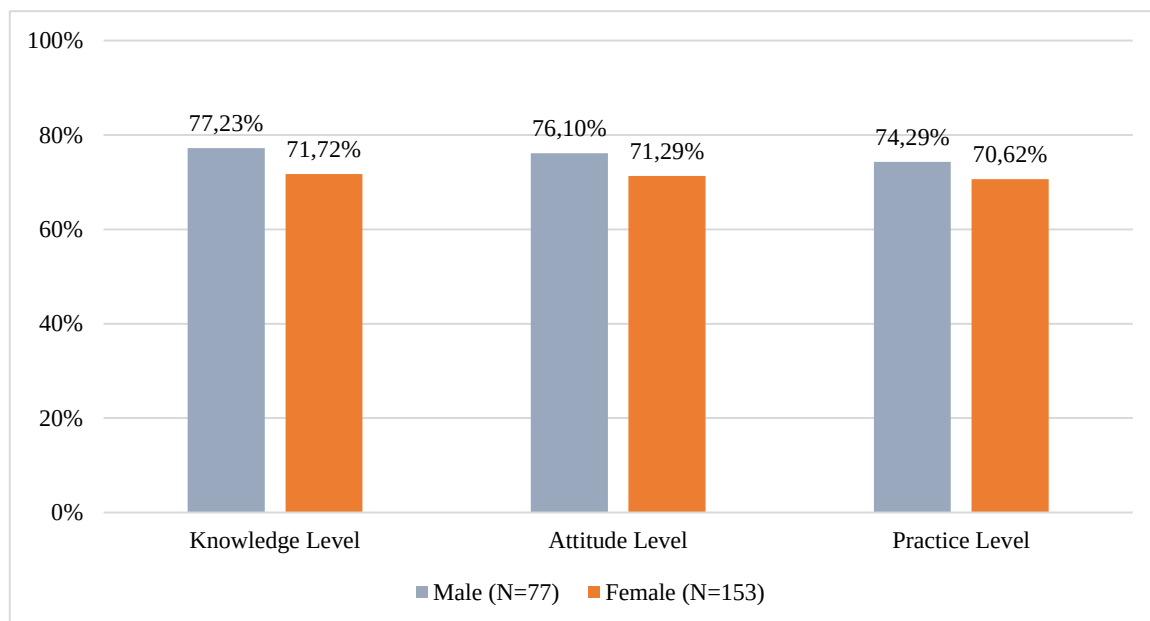


Figure 3. Comparison of Percentage Relationships Between Students' KAP and Gender.

Source. The authors

5.3. Age and Field of Study Influences

While earlier results suggested that age had limited predictive power for overall CSA, younger students (≤ 17) tended to outperform in technical indicators such as network verification and HTTP/HTTPS differentiation. This may reflect recent updates in digital literacy curricula at secondary levels (Branley-Bell et al., 2022), reinforcing the importance of early CSA education.

No statistically significant differences in CSA were found across fields of study, though students in IT-related majors did exhibit slightly higher scores. This suggests that formal exposure to cybersecurity concepts may help, but is insufficient to ensure behavioral adoption—a finding supported by Nkata (2025) and Zhang et al. (2025).

5.4. CSA Education Implications

The results support the applicability of the KAP framework in identifying CSA gaps and designing targeted interventions. The regression model revealed that passwords, computers, mobile devices, and internet security awareness were significant predictors of CSA. This suggests that CSA curricula should prioritize these domains while reevaluating how topics like social media and email safety are taught.

Moreover, the gap between attitude and practice, particularly in high-attitude but low-practice areas like internet security, reinforces the need for hands-on cybersecurity education. Workshops, simulations, and gamified learning may help students internalize risk perceptions into secure habits (Taherdoost, 2024).

5.5. KAP and CSA Correlation Level Relationships

The correlations for KAP levels and students' fields of study for CSA are as follows:

Students in Data Science and Information Technology had the highest level of mean score (4.03, IT (3.94), Computer Science (3.79)). However, Educational Technology and Computers had the lowest mean score (2.89) and English (3.17). The result was based on the statistical analysis; an F- value of 1.73 with a 0.10 p -value showed no statistically significant differences in knowledge level between the field of study (p -value > 0.05).

A similar pattern was also obtained for the attitude level, where the same students from data science and information technology also scored the highest mean score (3.97). Next to them were students from information technology (3.85) and nursing (3.61), while students drawn from English scored the lowest (3.17), followed by students who came from educational technology and computers (3.33). As the F- value = 0.90 and p -value = 0.50, it can be ascertained that there are no statistically significant differences in the attitudes across the fields of study (p -value > 0.05).

In terms of practice level, the means score of students from Data Science and Information Technology was the highest (4.18), followed by Computer Science (3.81) and then Law (3.66), while students from Educational Technology and Computers (3.42) and then English attained the lowest (3.38) average mean scores. Furthermore, the F- value = 1.41 and p -value = 0.20 confirm no statistically significant differences in the level of practice across the study fields (p -value > 0.05). In summary, differences in knowledge, attitudes, and practices were observed across various fields of study; however, these differences were not statistically significant. Hence, the field of study does not effectuate statistically significant differences in cybersecurity awareness.

One statistical limitation is the non-significance of the constant term in the regression model ($p = .77$), which may indicate that the model does not predict values significantly different from zero when predictors are held constant. While not uncommon in behavioral models using scaled predictors, this feature reflects possible constraints in model specification or centering procedures.

6. Conclusion

This study explored cybersecurity awareness (CSA) among Thai university students using the Knowledge, Attitudes, and Practices (KAP) framework. Drawing on a nationally stratified sample and validated survey instrument, the research examined how demographic variables—particularly gender and age—and domain-specific behaviors influence students' CSA levels.

Responding to RQ1, male students scored significantly higher overall on CSA, especially in technical domains such as network verification and malware detection. For RQ2, age-related differences were more nuanced: younger students (≤ 17) showed stronger technical awareness, while older students exhibited more secure behavioral habits. However, age alone did not emerge as a significant predictor of CSA.

Regression analysis confirmed that passwords, computers, mobile devices, and internet security were the strongest predictors of CSA. In contrast, email and social media security awareness did not show statistically significant effects. These findings indicate that CSA education should strategically focus on high-impact domains, integrating technical and behavioral training.

7. Practical Recommendations

1. Prioritize training in high-impact CSA areas, such as password and network security, especially for female students and non-IT majors.
2. Reevaluate email and social media training modules, which showed limited predictive power for CSA in this study.
3. Integrate CSA into general education curricula, ideally at pre-university levels, to foster early digital resilience.
4. To promote behavioral adoption, implement hands-on learning approaches, including cybersecurity simulations, interactive platforms, and scenario-based training.

8. Theoretical Contributions

This study reaffirms the utility of the KAP model in cybersecurity education research and advocates for culturally contextualized CSA frameworks in higher education. It offers empirical insights from a Southeast Asian setting—an underrepresented region in CSA literature—and provides a localized baseline for comparative studies across ASEAN nations.

9. Limitations and Future Work

9.1. Limitations

- The non-significant constant in the regression model ($p = .77$) suggests possible issues with model centering or limited CSA relevance without specific behaviors.
- Sample generalizability may be limited by the overrepresentation of nursing and IT students despite stratified sampling.
- Self-reporting bias may have influenced results, particularly for sensitive behaviors like password re-use and malware prevention.

9.2. Future Directions

- Longitudinal research could track CSA development over students' academic careers.
- Experimental studies should evaluate the impact of gamified and peer-led CSA interventions.
- Cross-cultural comparisons with other ASEAN nations could enrich the understanding of regional cybersecurity readiness and inform policy adaptations.

10. Knowledge Contribution and Novelty

This study contributes to CSA literature by emphasizing behavioral and foundational security awareness over purely technical metrics. The research underscores the importance of context-aware CSA education by identifying critical gaps, such as a limited understanding of HTTP vs. HTTPS. The findings highlight the need for holistic approaches that blend technical skills with behavioral habits, offering clear guidance for academic program design and national digital safety initiatives.

Declarations

Author Contributions.

Khanittha Sittitiamjan - Conceptualization, Software, Validation, Formal analysis, Investigation, Resources, Writing—original draft preparation, review and editing, Supervision.

Pongpisit Wuttidittachotti - Conceptualization, Software, Validation, Formal analysis, Investigation, Resources, Writing—original draft preparation, Writing—review and editing, Supervision. Both authors have read and agreed to the published version of the manuscript.

Conflict of Interests. The authors explicitly state that this paper has no conflicts of interest.

Funding. The authors received no outside funding for their research.

Informed Consent. Informed consent was obtained from all survey participants.

Data Availability Statement. The data supporting this study's findings are available upon reasonable request from the corresponding author.

References

- Abomhara, M., Nweke, L. O., Yayilgan, S. Y., Comparin, D., Teyras, K., & de Labriolle, S. (2024). Enhancing privacy protections in national identification systems: an examination of stakeholders' knowledge, attitudes, and privacy practices by design. *International Journal of Information Security*, 23, 3665–3689. <https://doi.org/10.1007/s10207-024-00905-0>
- Alhadidi, I., Nweiran, A., & Hilal, G. (2024). The influence of cybercrime and legal awareness on the behavior of University of Jordan students. *Heliyon*, 10(12), e32371. <https://doi.org/10.1016/j.heliyon.2024.e32371>
- Ainslie, S., Thompson, D., Maynard, S., & Ahmad, A. (2023). Cyber-threat intelligence for security decision-making: A review and research agenda for practice. *Computers & security*, 132, 103352. <https://doi.org/10.1016/j.cose.2023.103352>
- Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, 69, 437–443. <https://doi.org/10.1016/j.chb.2016.12.040>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333. <https://doi.org/10.3390/electronics12061333>
- Azad, R. U., Tasmim, S., & Atikuzzaman, M. (2025). Investigating students' awareness of online privacy and cybersecurity: an empirical study with effective cybersecurity training framework. *Global Knowledge, Memory, and Communication*. Vol. ahead-of-print No. ahead-of-print. <https://doi.org/10.1108/GKMC-05-2024-0319>
- Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, 2022(1), 2693080. <https://doi.org/10.1155/2022/2693080>
- Bruce, M., Lusthaus, J., Kashyap, R., Phair, N., & Varese, F. (2024). Mapping the global geography of cybercrime with the World Cybercrime Index. *PLOS ONE*, 19(4), e0297312. <https://doi.org/10.1371/journal.pone.0297312>
- Cain, A. A., Edwards, M. E., & Nevertheless, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, 42, 36–45. <https://doi.org/10.1016/j.jisa.2018.08.002>
- Chan, C. K. Y., & Lee, K. K. W. (2023). The AI generation gap: Are Gen Z students more interested in adopting generative AI, such as ChatGPT, in teaching and learning than their Gen X and millennial generation teachers? *Smart Learning Environments*, 10(1), 60. <https://doi.org/10.1186/s40561-023-00269-3>
- Chaudhary, S. (2024). Driving behavior change with cybersecurity awareness. *Computers & security*, 142, 103858. <https://doi.org/10.1016/j.cose.2024.103858>
- Chauhan, R., Mehtar, K., Kaur, H., & Alankar, B. (2024, April). Evaluating cyber-crime using machine learning and AI approach for environmental sustainability. In P. Whig, N. Silva, A. A. Elngar, N. Aneja, & P. Sharma (Eds.), *Sustainable development through machine learning, AI and IoT: ICSD 2024* (Vol. 2196). *Communications in Computer and Information Science*. Springer. https://doi.org/10.1007/978-3-031-71729-1_4

- Chen, Y., Cui, M., Wang, D., Cao, Y., Yang, P., Jiang, B., Lu, Z., & Liu, B. (2024). A survey of large language models for cyber threat detection. *Computers & Security*, 145, 104016. <https://doi.org/10.1016/j.cose.2024.104016>
- Cook, S. (2024, May 14). U.S. schools leaked 37.6 million records in 3,713 data breaches. *Comparitech*. <https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/>
- Essien, E. S., & Egbeji, E. E. (2024). Digitalizing Cyber Security for Data Management in Higher Education Implication for Educational Management in Nigeria. *Journal of Advanced Education Philosophy*, 8(4), 234- 238. <https://doi.org/10.36348/jaep.2024.v08i04.001>
- Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4. <https://doi.org/10.11648/j.ajtas.20160501.11>
- Fadli, R., Surjono, H. D., Sari, R. C., Hidayah, Y., & Eliza, F. (2024). Assessing cybersecurity awareness among vocational students in office administration. *International Journal of Safety and Security Engineering*, 14(4), 1115–1123. <https://doi.org/10.18280/ijss.140410>
- Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, 345–358. <https://doi.org/10.1016/j.cose.2017.11.015>
- He, S. Q., & Chen, I. H. (2024). Internet addiction among teachers: A systematic review. *Environment and Social Psychology*, 9(6), 2513. <https://doi.org/10.54517/esp.v9i6.2513>
- Ifeanyi, T. T., Nwaosu, O. P., & Ezeanokwasa, F. N. (2024). Digital knowledge and market positioning of micro, small, and medium-scale enterprises (MSMEs) in Asaba, Delta State, Nigeria. *Journal of Global Accounting*, 10(4), 85-106. <https://journals.unizik.edu.ng/joga/article/view/5177>
- Iskandar, I., Putra, D. D., Yasin, A. I., & Khairan, K. (2025). *Cyber Smart Campus: Cakap Digital & Aman Siber*. PT. Sonpedia Publishing Indonesia.
- Kabaila, P., Farchione, D., Alhelli, S., & Bragg, N. (2021). The effect of a Durbin–Watson pretest on confidence intervals in regression. *Statistica Neerlandica*, 75(1), 4-23. <https://doi.org/10.1111/stan.12222>
- Khader, M., Karam, M., & Fares, H. (2021). Cybersecurity awareness framework for academia. *Information*, 12(10), 417. <https://doi.org/10.3390/info12100417>
- Lee, S. S. (2024). *Predicting the Effects of CyberPatriot Participation, Internet Experience, Gender, and Grade Level on Cybersecurity Judgment (Intuitive and Rational) Among Middle and High School Students: A Quantitative Predictive Correlational Study*. (Doctoral dissertation- Liberty University). Virginia. <https://digitalcommons.liberty.edu/doctoral/6363>
- Leekitchwatana, P., Pimdee, P., & Moto, S. (2018). Using the Internet for development of structural equation model of teaching behavior of junior high school teachers. *Kasetsart Journal of Social Sciences*, 39(3), 868-878. <https://so04.tci-thaijo.org/index.php/kjss/article/view/242614>
- Liluashvili, G. B. (2021). Cyber risk mitigation in higher education. *Law & World*, 17, 15.
- Luo, Y. F., Chen, L. C., Yang, S. C., & Hong, S. (2022). Knowledge, attitude, and practice (KAP) toward COVID-19 pandemic among the public in Taiwan: a cross-sectional study. *International Journal of environmental research and public health*, 19(5), 2784. <https://doi.org/10.3390/ijerph19052784>

- Ma, K., & Fang, B. (2024). Exploring Generation Z's expectations at future work: the impact of digital technology on job searching. *European Journal of Training and Development*, 48(9), 933-953. <https://doi.org/10.1108/EJTD-05-2023-0076>
- Marín, V. I., Carpenter, J. P., Tur, G., & Williamson-Leadley, S. (2023). Social media and data privacy in education: An international comparative study of perceptions among pre-service teachers. *Journal of Computers in Education*, 10(4), 769–795. <https://doi.org/10.1007/s40692-022-00243-x>
- Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity*, 800299. <https://doi.org/10.5171/2017.800299>
- NIST Cybersecurity Framework (CSF) 2.0. (2024, February 26). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.CSWP.29>
- Nkata, A. S. (2025). Impact of Teaching Cybersecurity Professional Courses for Students of Higher Learning Institutions: What Should the Society Expect? *BIMA Journal of Science and Technology*, 8(4B), 140-149. <https://doi.org/10.56892/bima.v8i4B.1191>
- O'Brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. *Quality & Quantity*, 41(5), 673–690. <https://doi.org/10.1007/s11135-006-9018-6>
- Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Cyber safety in e-learning: The effects of cyber awareness and information security policies with moderating effects of gender and experience levels among e-learning students. *Education and Information Technologies*, 1-40. <https://doi.org/10.1007/s10639-025-13366-2>
- Papasteri, C., Letzner, R. D., & Pascal, S. (2024). Pandemic KAP framework for behavioral responses: initial development from lockdown data. *Current Psychology*, 43(26), 22767-22779. <https://doi.org/10.1007/s12144-024-05670-w>
- Parmar, M., & Miles, A. (2024, May). Cyber Security Frameworks (CSFs): An assessment between the NIST CSF v2. 0 and EU Standards. In *2024 Security for Space Systems (3S)* (pp. 1-7). IEEE. <https://doi.org/10.23919/3S60530.2024.10592293>
- Phuong, C. (2022). *Teaching cybersecurity: A project-based learning and guided inquiry collaborative learning approach* (Doctoral dissertation, University of Tennessee at Chattanooga). University of Tennessee at Chattanooga. <https://scholar.utc.edu/theses/757>
- Pimdee, P., & Leekitchwatana, P. (2019). Structural equation modeling of teaching behavior in Internet use of teachers in Thailand. *TEM Journal*, 8(4), 1499-1507. <http://dx.doi.org/10.18421/TEM84-56>
- Pimdee, P., & Leekitchwatana, P. (2022). Appropriate Internet Use Behavior (AIUB) of Thai preservice teachers: A Hierarchical Linear Model (HLM) analysis. *International Journal of Instruction*, 15(1), 489-508. <https://doi.org/10.29333/iji.2022.15128a>
- Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging human factors in cybersecurity: An integrated methodological approach. *Cognition, Technology & Work*, 24(2), 371–390. <https://doi.org/10.1007/s10111-021-00683-y>
- Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W., & Thapliyal, H. (2023). A systematic literature review of cybersecurity scales assessing information security awareness. *Heliyon*, 9(3), e14234. <https://doi.org/10.1016/j.heliyon.2023.e14234>

- Shah, M. U., Iqbal, F., Rehman, U., & Hung, P. C. K. (2023). A comparative assessment of human factors in cybersecurity: Implications for cyber governance. *IEEE Access*, 11, 87970–87984. <https://doi.org/10.1109/ACCESS.2023.3296580>
- Shari, A. M. J., Ahmad, M., Razali, R. R. R., & Sujak, A. F. A. (2022, December). Knowledge, attitude, and practices towards internet safety and security among generation Z in Malaysia: A conceptual paper. In *Proceedings of the International Conference on Communication, Language, Education, and Social Sciences*. CLESS (pp. 4-11). <https://doi.org/10.1016/j.heliyon.2024.e32371>
- Slepian, R. C., Vincent, A. C., Patterson, H., & Furman, H. (2024). Social media, wearables, telemedicine and digital health—A Gen Y and Z perspective. In *Reference Module in Biomedical Sciences*. <http://dx.doi.org/10.1016/B978-0-12-824010-6.00072-1>
- Taherdoost, H. (2024). A critical review of cybersecurity awareness frameworks and training models. *Procedia Computer Science*, 235, 1649–1663. <https://doi.org/10.1016/j.procs.2024.04.156>
- Tan, S. (2022, October 10). Generational trends in Thailand's social media use: How Gen Z differs from other age groups. *YouGov*. <https://tinyurl.com/5n8yctvw>
- Triplett, W. J. (2023). Addressing cybersecurity challenges in education. *International Journal of STEM Education for Sustainability*, 3(1), 47-67. <https://www.journal.gmpionline.com/index.php/ijses/article/view/132>
- Rahman, M. M., Tabash, M. I., Salamzadeh, A., Abduli, S., & Rahaman, M. S. (2022). Sampling techniques (probability) for quantitative social science researchers: A conceptual guidelines with examples. *Seeu Review*, 17(1), 42-51. <https://doi.org/10.2478/seeur-2022-0023>
- Uttley, J. (2019). Power analysis, sample size, and assessment of statistical assumptions—Improving the evidential value of lighting research. *Leukos*, 5(2-3). <https://doi.org/10.1080/15502724.2018.1533851>
- Wang, C., Tang, H., Zhu, H., Zheng, J., & Jiang, C. (2024). Behavioral authentication for security and safety. *Security and Safety*, 3, 2024003. <https://doi.org/10.1051/sands/2024003>
- Wannapiroon, N., & Pimdee, P. (2022). Thai undergraduate science, technology, engineering, arts, and math (STEAM), creative thinking and innovation skill development: a conceptual model using a digital virtual classroom learning environment. *Education and Information Technologies*, 27(4), 5689-5716. <https://doi.org/10.1007/s10639-021-10849-w>
- Zhang, Y., Du, Y., & Liu, C. (2025). Enhancing Cybersecurity Awareness among University Students: A Strategic Approach. *Learning & Education*, 14(1). <https://ojs.piscomed.com/index.php/L-E/article/view/4275>
- Zineddine, A., Chakir, O., Sadqi, Y., Maleh, Y., Gaba, G. S., Gurtov, A., & Dev, K. (2024). A systematic review of cybersecurity assessment methods for HTTPS. *Computers and Electrical Engineering*, 115, 109137. <https://doi.org/10.1016/j.compeleceng.2024.109137>

About the Contributor(s)

Khanittha Sittitiamjan is an Assistant Professor at the Faculty of Computer Science and Information Technology at Thailand's Rambhai Barni Rajabhat University. She obtained a Master of Science Education from the Faculty of Industrial Education and Technology (M.Sc) at the King Mongkut's Institute of Technology Ladkrabang (KMUTL) in Bangkok, Thailand. Currently, she is also a Ph.D. Candidate at the King Mongkut's University of Technology North Bangkok (KMUTNB), Bangkok,

Thailand. Her research interests include IT acceptance, information security, computer networks, and management information systems.

Email: khanittha.s@email.kmutnb.ac.th

ORCID: <https://orcid.org/0009-0002-2561-5266>

Pongpisit Wuttidittachotti, serves as an Associate Professor with the Department of Digital Network and Information Security Management (DNS) at the Faculty of Information Technology and Digital Innovation, the King Mongkut's University of Technology North Bangkok (KMUTNB), Bangkok, Thailand. He holds a Ph.D. in Networks, Telecommunications, Systems, and Architectures from INPT-ENSEEIH, France, in 2009. He specializes in Cybersecurity awareness, Cybersecurity management systems, VoIP, QoS/QoE, mobile networks, wireless networks, network communications, telecommunications, IoT, and AI.

Email: pongpisit.w@itd.kmutnb.ac.th

ORCID: <https://orcid.org/0000-0002-0076-4882>

Publisher's Note: *The opinions, statements, and data presented in all publications are solely those of the individual author(s) and contributors and do not reflect the views of Universitepark, EDUPIJ, and/or the editor(s). Universitepark, the Journal, and/or the editor(s) accept no responsibility for any harm or damage to persons or property arising from the use of ideas, methods, instructions, or products mentioned in the content.*
