Contemporary Educational Technology, 2026, **18**(4), ep703
ISSN: 1309-517X (Online)



OPEN ACCESS

Research Article

Prioritizing cybersecurity education: A needs assessment of Thai student digital behaviors and security competencies

Jiraphong Chanthaphot [1]
0000-0001-6766-0239

Thiyaporn Kantathanawat [1*]
0000-0002-4436-8806

Paitoon Pimdee [1]
0000-0002-3724-2885

Kanchana Boonphak [1]
0009-0002-7762-3911

Mai Charoentham [1]
0009-0001-3075-7173

[1] School of Industrial Education and Technology, King Mongkut's Institute of Technology Ladkrabang, Bangkok, THAILAND
[*] Corresponding author: thiyaporn.ka@kmitl.ac.th

Citation: Chanthaphot, J., Kantathanawat, T., Pimdee, P., Boonphak, K., & Charoentham, M. (2026). Prioritizing cybersecurity education: A needs assessment of Thai student digital behaviors and security competencies. *Contemporary Educational Technology, 18*(4), Article ep703. https://doi.org/10.30935/cedtech/19937

ARTICLE INFO

Received: 19 Sep 2026

Accepted: 5 Nov 2026

ABSTRACT

Undergraduate university students are particularly susceptible to cyberattacks; however, increased awareness does not always translate into protective actions. To close this gap in cybersecurity behavior (CSB), this study identified priority needs for educational intervention among Thai undergraduate university students across six key dimensions: password (CSB-PW), social media (CSB-SM), application (CSB-AP), email (CSB-EM), mobile device security (CSB-MD), and security incident reporting (CSB-IR). A sample of 190 second-year Thai undergraduates completed a validated 60-item needs assessment questionnaire. Data were analyzed using SPSS 29/R 4.3 descriptive statistics, dependent-samples t-tests, and the modified priority needs index ($PNI_{modified}$). Results revealed a statistically significant gap ($p < .001$) between students' *current behavior* (mean [M] = 3.303, standard deviation [SD] = 1.018, competence) and their *desired behavior* (M = 4.471, SD = 0.788, proficiency). The overall priority needs index was 0.354. Dimension rankings from highest to lowest priority were mobile device security ($PNI_{modified}$ = 0.371), email security ($PNI_{modified}$ = 0.366), security incident reporting ($PNI_{modified}$ = 0.364), application security ($PNI_{modified}$ = 0.363), social media security ($PNI_{modified}$ = 0.359), and password security ($PNI_{modified}$ = 0.298). These results raise doubts about the effectiveness of standard cybersecurity classes that teach how to manage passwords and imply that future educational interventions should focus on securing email and mobile devices through self-efficacy approaches.

Keywords: cybersecurity behavior, email security, mobile security, needs assessment, phishing, Thailand

INTRODUCTION

Rapid adoption of digital technologies has changed the way we learn, work, and interact. Global Internet use stands at 68% (International Telecommunication Union, 2024), whereas in Thailand the figure is considerably higher at 89.5% (Lapmak, 2025). Moreover, the adoption of digital technology is associated with increased cybercrime. Although there has been massive expenditure on cyber defense mechanisms such as

Copyright © 2026 by authors; licensee CEDTECH by Bastas. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (https://creativecommons.org/licenses/by/4.0/).

firewalls, intrusion prevention, and cryptography, global costs associated with cybercrime are estimated at $10.5 trillion in 2026, with an average cost of a data breach at $4.88 million (Mohsin, 2025).

The contrast between growing technical measures and persistent breaches points to one dominant factor: human behavior. The human element—including human error, privilege misuse, and social engineering—contributes to 62% of data breaches (Verizon, 2026), and attackers increasingly exploit psychological vulnerabilities through social engineering rather than technical flaws (Alqahtani, 2022; Salahdine & Kaabouch, 2019; Siddiqi et al., 2022).

Students are among the most vulnerable populations. Members of generation Z (digital natives) are competence with technology but not necessarily skilled at protecting themselves from cyberattacks (Hadlington, 2017; Rosenberg et al., 2025). Four elements increase their vulnerability: high engagement with digital technologies in academic, social, and financial activities; financial independence conducted mostly on mobile phones; low metacognition regarding security threats (Alqahtani, 2022); and optimism bias, whereby young individuals believe themselves immune to cybercrime (Dodel & Mesch, 2017). Three cognitive biases—optimism, confirmation, and authority—have been identified as particularly consequential in explaining why students fail to act on security knowledge they possess (Vishwanath et al., 2011).

Therefore, students are key targets of phishing, smishing, and other social engineering attacks (Daudi, 2024; Kovačević et al., 2020; Tanti, 2024). Such attacks exploit cognitive, rather than technical, weaknesses (Siddiqi et al., 2022) and take several forms: phishing, in which scammers send emails that appear legitimate in order to harvest credentials or confidential information (Intarakamhang et al., 2025; Tanti, 2024); smishing, in which messages are sent via SMS or messaging applications and which is becoming more common because of widespread mobile use (Zimba et al., 2025); pretexting, in which fabricated scenarios are used to harvest information (Akeiber, 2025); and baiting, in which people are induced to download malware (Datta & Acton, 2025). Approximately 3.4 billion phishing emails are sent daily, 82.6% of which are generated by artificial intelligence (House, 2026).

The cybersecurity situation in Thailand is particularly worrisome, given the country's high level of Internet use and a disparity in cyber skills. According to Kemp (2025), there are 56.6 million social media accounts in Thailand, representing 79.1% of the population. Of this number, 15% of users are 13 to 24 years old. Moreover, daily Internet usage among generation Y users averages 8 hours and 45 minutes (Chaihanchanchai & Anantachart, 2024). Students in Thai universities are highly active online, particularly given the impact of the COVID-19 pandemic and online learning (Alsaad & Al-Okaily, 2022; Jittam et al., 2026; Pimdee et al., 2024). Thailand has a statutory requirement for digital literacy training (Hoonsopon et al., 2025; Nantha et al., 2024); however, there are disparities in how this mandate is fulfilled. Some research shows that Thai students who are highly dependent on technology struggle to recognize phishing, smishing, and other forms of deception (Kraiwanit et al., 2025).

At Dhonburi Rajabhat University (DRU) in Samut Prakan, Thailand, as with many other universities in the country, cybersecurity is part of the general education program through the *media literacy* course (Hunsapun, 2023). However, the curriculum remains knowledge-oriented, where students learn about topics such as password usage rather than behavior. Hence, the learners know about the security problems but fail to act on them, as a knowledge-behavior gap has been found at all levels of learning (Kruger & Kearney, 2006; Parsons et al., 2014). Protection motivation theory (PMT) explains this phenomenon by suggesting that students have knowledge of the threats and their vulnerability to them (Bandura, 2023). However, they lack the belief that they can perform protective actions due to low self-efficacy.

The Importance of Needs Assessment

A needs assessment identifies the gap between current and desired states and is therefore a prerequisite for designing effective educational interventions (Prasittichok & Klaykaew, 2022). The modified priority needs index ($PNI_{modified}$) (Wongwanich et al., 2014) has been widely adopted in Thailand and the surrounding region. By calculating the ratio of the discrepancy between desired and current states to the current state, $PNI_{modified}$ yields an index that ranks intervention priorities. The $PNI_{modified}$ has been used extensively in Thailand as well as international studies including teacher education (Khong-ngam et al., 2014), computational thinking (Aroonsiwagool et al., 2025), software development (Pimsalee et al., 2026), mobile website design (Shahid et

al., 2022; Wuttikamonchai et al., 2024), higher education curriculum design (Janpirom et al., 2025), medicine (Civaner et al., 2022), information technology (Borriraklert & Kiattisin, 2021), and human resource development (Chimnoy et al., 2023).

In cybersecurity education, however, awareness and behavior do not coincide (Parsons et al., 2014), and awareness levels are not homogeneous across behavioral dimensions (Kovačević et al., 2020). Studies that measure cyber awareness among Thai undergraduates, therefore, cannot be assumed to describe what those students actually do. To date, the authors are unaware of any study that has applied a systematic needs assessment to determine the gap between desired and current cybersecurity behavior (CSB) among Thai undergraduate students—a gap this study addresses (Li et al., 2022).

The six categories upon which this assessment is based are as follows: passwords, social media security, applications, email, mobile devices, and security incidents. These categories have been chosen as they all constitute a unique avenue of student vulnerability. Password management is among the most frequently studied aspects of information security awareness (Parsons et al., 2014), yet students often prioritize convenience over security (Alqahtani, 2022). Social media interactions can lead to social engineering through oversharing and weak privacy settings, but awareness of this threat among Thai students does not guarantee safe behavior (Pushsapavardhana, 2025; Samae et al., 2014). Application security comprises the aspects of application downloading, installation, and permissions. Vulnerabilities in applications are the most common targets for cyber criminals (Kruger & Kearney, 2006). Emails remain the primary medium for phishing attacks, especially targeting college students (Lallie et al., 2025). The use of mobile devices has become an inseparable part of students' communication, studying, and finances; however, small screens and always-on connectivity have created a specific security situation (Beyer, 2014; Hadlington, 2017; Pollini et al., 2022). The final behavior to be discussed is security incident reporting, which is extremely important but understudied owing to uncertainty about thresholds and a lack of reporting mechanisms (Pushsapavardhana, 2025).

Problem Statement

The digital economy in Thailand is developing, but cybersecurity remains a weakness in both Thai academia and industry. College students have become easy targets for various cyberattacks, including phishing, credential theft, and social engineering. The problem worsens when they transition to academic and professional activities in online environments (Pimdee et al., 2024). However, cybersecurity education in Thai universities remains underdeveloped for various reasons.

First, existing studies of Thai undergraduates focus predominantly on cybersecurity awareness rather than behavior. Because awareness and behavior do not coincide (Parsons et al., 2014), instructional interventions based on awareness data may target knowledge that students already possess while leaving the behaviors they actually perform unaddressed. There is a lack of systematic, empirically grounded needs assessment identifying the current and desired CSB of Thai undergraduate students.

Second, this gap is especially pronounced for students in the industrial education and technology program with an emphasis on computer technology, a program-level subgroup within the faculty of science and technology (n = 67), who will enter the job market as technology educators, software engineers (Sureeyatanapas et al., 2024), or industry technology experts. These students will need both technological and pedagogical cybersecurity skills, and this group cannot rely on needs assessments conducted for general undergraduates or professional software developers, because their needs differ.

Third, without prioritizing behaviors, curriculum developers and teachers will be unable to determine which cybersecurity domains require the most instruction. This is because the educational effort is undertaken without any empirical guidelines, thereby risking attention to unimportant behaviors and neglecting important ones.

To address these problems, this study applies $PNI_{modified}$ to evaluate and prioritize cybersecurity behavioral needs across six domains—password security, social media activity security, application security, email security, mobile device security, and security incident reporting. The findings aim to provide a data-driven foundation for aligning curriculum design, instructional strategies, and skill-development planning with the real cybersecurity demands faced by Thai undergraduates.

Research Objectives

RO1. To identify priority needs for improving CSB among undergraduates across six behavioral domains: password security (CSB-PW), social media activity security (CSB-SM), application security (CSB-AP), email security (CSB-EM), mobile device security (CSB-MD), and security incident reporting (CSB-IR).

RO2. To prioritize these behavioral needs and thereby define the most urgent areas for educational intervention.

Research Questions

RQ1. What are the current and desired levels of CSB among undergraduates across the six behavioral domains?

RQ2. What are the priority needs for improving CSB in each domain, as ranked by $PNI_{modified}$?

RQ3. Which behavioral domains represent the most urgent targets for educational intervention, and what is the relative magnitude of need across domains?

Study Contributions

Contextual: This is the first empirical analysis, to the authors' knowledge, of behavior-related cybersecurity needs of Thai university students, moving beyond awareness-based studies and focusing on a body of knowledge that is largely Western-centric.

Methodological: This study serves as an illustration of the use of $PNI_{modified}$ in cybersecurity education, demonstrating how proportional scaling enables prioritization that cannot be achieved through gap scoring alone.

Practical: The developed priorities guide the allocation of limited teaching resources and treat mobile and email security as priorities of comparable urgency, which previous studies have not done.

METHODS

Research Design

This study employed a cross-sectional quantitative survey design to examine the priority needs for developing CSB among undergraduate students. The $PNI_{modified}$ (Wongwanich et al., 2014) was adopted because it compares *current behavior* (actual state) and their *desired behavior* (ideal state) to produce a ranked index of intervention priorities.

Participants and Sampling

The target population comprised 370 second-year undergraduate students enrolled in the *media literacy* general education course in the 2026 academic year at DRU, Samut Prakan Province, Thailand. The population spans four faculties: education (n = 103), management science (n = 159), science and technology (n = 67), and humanities and social sciences (n = 41).

The faculty of science and technology stratum (n = 67) includes students in the industrial education and technology program with a computer technology emphasis referenced in the problem statement; the survey did not sample by program within faculty, so this subgroup is represented proportionally through the faculty stratum rather than as a separately identified subsample.

The minimum sample size was determined using the Krejcie and Morgan (1970) table, which specifies 189 respondents for a population of 370 at a 95% confidence level and a 5% margin of error (Singh & Masuku, 2014). To allow for incomplete responses, 200 students were invited. Proportional stratified random sampling was used: strata were defined by faculty and sampled proportionally, with participants then selected by simple random sampling from the university roster. A total of 190 valid responses were obtained, a response rate of 95% (**Table 1**).

Table 1. Distribution of population and sample by faculty

No	Faculty	Population	Sample	Percentage of population
1	Faculty of education	103	53	27.86
2	Faculty of management science	159	82	43.01
3	Faculty of science and technology	67	34	18.13
4	Faculty of humanities and social sciences	41	21	11.09
Total		370	190	100

Instrumentation

A 60-item needs assessment questionnaire was developed to measure six dimensions of CSB, with 10 items per dimension (**Appendix A**):

Password security (CSB-PW): e.g., "I do not use the same password for all websites or applications" (item 1.2); "I enable two-factor authentication (2FA) for important applications" (item 1.5).

Social media activity security (CSB-SM): e.g., "I adjust privacy settings to limit who can access my information" (item 2.5); "I do not click on suspicious links attached to chat messages, even if sent by someone I know" (item 2.7).

Application security (CSB-AP): e.g., "I review and manage app permissions (e.g., camera, microphone access) appropriately" (item 3.5); "I regularly update applications and operating systems to the latest versions to patch vulnerabilities" (item 3.6).

Email security (CSB-EM): e.g., "I verify the sender's email address before replying or clicking any links" (item 4.4); "I do not click links or open attachments from unsolicited emails" (item 4.2).

Mobile device security (CSB-MD): e.g., "I always set a screen lock using a password, fingerprint, or facial recognition" (item 5.4); "I am cautious when using public free Wi-Fi to log into important systems" (item 5.3).

Security incident reporting (CSB-IR): e.g., "I know how and where to contact the system administrator or relevant authorities when a security incident occurs" (item 6.5); "I immediately alert friends or close contacts when I discover their accounts have been hacked or show unusual activity" (item 6.7).

For each item, participants rated both their *current behavior* (actual state) and their *desired behavior* (ideal state) on a 5-point Likert scale (1 = strongly disagree, 2 = disagree, 3 = neutral, 4 = agree, 5 = strongly agree). The full questionnaire appears in **Appendix A**.

Content validity was assessed by five experts—university lecturers specializing in software development and cybersecurity education from five different institutions, none of whom were affiliated with the target population's faculty or program. The item-objective congruence index ranged from 0.67 to 1.00. All 60 items met the ≥ 0.67 threshold and were retained.

Reliability was evaluated through a pilot test with 30 students who were not part of the main sample. Cronbach's alpha coefficients were: CSB-PW (α = 0.85), CSB-SM (α = 0.89), CSB-AP (α = 0.87), CSB-EM (α = 0.88), CSB-MD (α = 0.91), and CSB-IR (α = 0.90). Overall reliability was α = 0.91, exceeding the accepted 0.80 threshold.

Data Collection

Data were collected in August 2026 via an online Google Forms questionnaire. The students received an information sheet about the purpose of the study, voluntariness, and data confidentiality. Informed consent was obtained online prior to answering the questionnaire. The questionnaire took 15-20 minutes to complete; the survey period was 14 days, with follow-up emails sent to non-respondents after 5 days. Of the 200 students invited, 190 participated, yielding a response rate of 95%.

Data Analysis

Data analysis focused on identifying gaps between current and desired CSB. $PNI_{modified}$ was calculated as $PNI_{modified} = \frac{I-D}{D}$, where I is the mean score for the desired (ideal) state and D is the mean score for the current (actual) state. Higher $PNI_{modified}$ values indicate a greater need and higher priority for development. This method has been widely applied in Thai educational, medical, information technology, and human resource development research (Borriraklert & Kiattisin, 2021; Chimnoy et al., 2023; Civaner et al., 2022; Janpirom et

Table 2. Participant demographic profiles (n = 190)

Item	Category	Number	Percentage (%)
Gender	Male	71	37.37
	Female	118	62.11
	Other	1	0.53
Current cumulative grade point average (GPAX)	3.51-4.00	55	28.95
	3.01-3.50	79	41.58
	2.51-3.00	46	24.21
	2.01-2.50	10	5.26
Faculty	Education	53	27.86
	Management science	82	43.01
	Science and technology	34	18.13
	Humanities and social sciences	21	11.09

Note. Percentages may not total exactly 100% due to rounding

Table 3. Ms, SDs, and proficiency levels of current and desired cybersecurity behaviors

Dimension	Condition	M	SD	Level
CSB-PW (password)	Desired (I)	4.358	0.880	Proficiency
	Actual (D)	3.356	1.053	Competence
CSB-SM (social media)	Desired (I)	4.462	0.769	Proficiency
	Actual (D)	3.283	1.017	Competence
CSB-AP (application)	Desired (I)	4.486	0.777	Proficiency
	Actual (D)	3.291	1.000	Competence
CSB-EM (email)	Desired (I)	4.517	0.751	Mastery
	Actual (D)	3.306	1.001	Competence
CSB-MD (mobile device)	Desired (I)	4.504	0.784	Mastery
	Actual (D)	3.285	1.029	Competence
CSB-IR (incident reporting)	Desired (I)	4.499	0.766	Proficiency
	Actual (D)	3.297	1.009	Competence
Overall	Desired (I)	4.471	0.788	Proficiency
	Actual (D)	3.303	1.018	Competence

Note. Level criteria: Mastery (4.50-5.00); Proficiency (3.50-4.49); Competence (2.50-3.49); Developing (1.50-2.49); Novice (1.00-1.49)

al., 2025; Khamcharoen et al., 2022; Prasittichok & Klaykaew, 2022; Yurayat & Seechaliao, 2021). The resulting indices were used to rank the six behavioral domains in order of priority.

Paired-samples t tests were used to compare the mean current (D) and desired (I) scores for each of the six dimensions and for the overall scale, because the same participants rated both states for every item. For each comparison we report the t statistic, degrees of freedom (n - 1 = 189), the two-tailed p value, and Cohen's d for paired samples, computed as the mean of the within-participant differences divided by the standard deviation (SD) of those differences. Values of d ≥ 0.80 are interpreted as large, following Cohen's conventional benchmarks. Because six dimension-level tests were conducted, a Bonferroni-corrected alpha of .0083 (α = .05/6) was applied to those six comparisons, following Bland and Altman (1995). The overall-scale test was evaluated at the conventional α = .05 because it is a single, non-multiplied comparison and is not part of the family of six-dimension tests. All tests were two-tailed. Confidence intervals for the $PNI_{modified}$ values are not reported; comparisons among dimensions are based on the point estimates reported.

RESULTS

Participant Characteristics

The 190 respondents were predominantly female (62.11%), with cumulative GPAs clustering in the 3.01-3.50 range (41.58%). By faculty, management science contributed the largest share (43.01%), followed by education (27.86%), science and technology (18.13%), and humanities and social sciences (11.09%). Detailed demographics are shown in **Table 2**.

Descriptive Statistics of Current and Desired Cybersecurity Behaviors

Table 3 shows the mean (M) and SD scores for the current (actual) and desired states for each of the six CSB dimensions. In general, the participants rated their current behaviors at the level of competence (M =

Table 4. Priority needs index, ranking, and statistical comparison of actual vs. desired cybersecurity behaviors (n = 190)

Dimension	D	I	I - D	$PNI_{modified}$	Rank	t	df	p	Cohen's d
CSB-MD	3.285	4.504	1.219	0.371	1	16.59	189	< .001	1.20
CSB-EM	3.306	4.517	1.211	0.366	2	17.01	189	< .001	1.23
CSB-IR	3.297	4.499	1.202	0.364	3	16.69	189	< .001	1.21
CSB-AP	3.291	4.486	1.195	0.363	4	16.62	189	< .001	1.21
CSB-SM	3.283	4.462	1.179	0.359	5	16.26	189	< .001	1.18
CSB-PW	3.356	4.358	1.002	0.298	6	12.93	189	< .001	0.94
Overall	3.303	4.471	1.168	0.354	-	15.98	189	< .001	1.16

Note. $PNI_{modified}$ = (I - D)/D, where D is actual state and I is desired state; Cohen's d > 0.80 indicates a large effect; CI is 95% bootstrap CI (1,000 resamples)

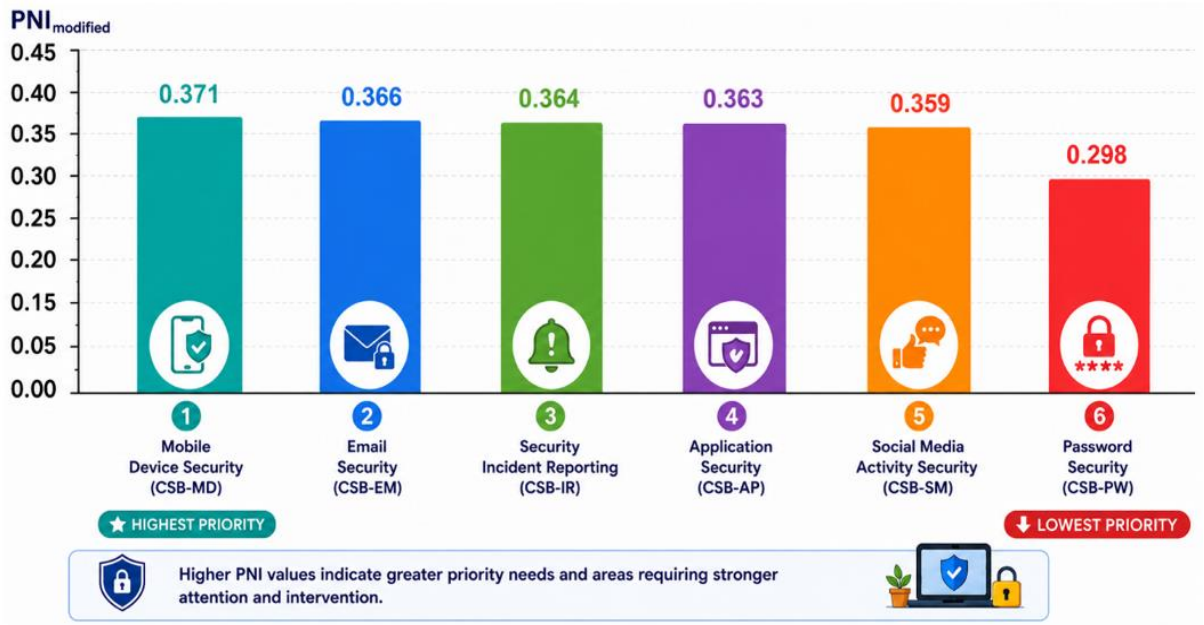


Figure 1. $PNI_{modified}$ values for six cybersecurity behavior dimensions, ranked from highest to lowest priority (higher values indicate greater urgency for intervention) (created by the authors with assistance from ChatGPT)

3.303, SD = 1.018) and their desired state at the level of proficiency (M = 4.471, SD = 0.788). There was a difference of 1.168 scale units between the current state and desired state levels. According to the five-level mastery continuum, competence (2.50-3.49) is the ability to perform a task functionally but not perfectly, while proficiency (3.50-4.49) is reliable performance.

Priority Needs Index and Ranking

Results for the $PNI_{modified}$ variable, its ranking, and the *t* tests between the actual and desired states are presented in **Table 4**. All dimensions showed statistically significant differences ($p < .001$) with substantial effect sizes (Cohen's d = 0.94-1.23). The Bonferroni-corrected alpha of .0083 was used for this analysis (Bland & Altman, 1995). All six dimension-level paired-samples t tests remained significant after Bonferroni correction ($\alpha = .05/6 = .0083$), and the overall-scale comparison was significant at $\alpha = .05$.

Priority Ranking

Figure 1 presents the $PNI_{modified}$ values ranked from highest to lowest priority. Mobile device security (CSB-MD; $PNI_{modified}$ = 0.371) ranked first, followed by email security (CSB-EM; 0.366), security incident reporting (CSB-IR; 0.364), application security (CSB-AP; 0.363), social media activity security (CSB-SM; 0.359), and password security (CSB-PW; 0.298).

DISCUSSION

In this study, the CSB needs of 190 Thai undergraduates were analyzed using the $PNI_{modified}$ index across six dimensions. Three findings warrant discussion: the consistent gap between actual and desired behavior, the emergence of mobile and email security as top priorities, and the unexpectedly low priority assigned to passwords.

RQ1. Current and Desired Cybersecurity Behaviors

Participants rated their current CSB at the competence level (M = 3.303) and their desired behaviors at the proficiency level (M = 4.471), a gap of 1.168 scale units with large effect sizes across all six dimensions (Cohen's d = 0.94-1.23). This pattern is consistent with the well-documented knowledge-behavior gap in cybersecurity (Kruger & Kearney, 2006; Parsons et al., 2014) and indicates that students are aware of security risks: they recognize their behavioral deficiencies and express a desire to change.

According to PMT (Bandura, 2023), this pattern indicates an appraisal-coping deficit rather than a threat-appraisal deficit (Susyanto et al., 2026). Students appreciate the seriousness of cybersecurity risks and their own vulnerability; however, they lack the self-efficacy to carry out the required behaviors. This interpretation is consistent with Susyanto et al. (2026), whose systematic review found that coping appraisal—specifically self-efficacy—has a greater influence on CSB than threat appraisal. From the perspective of the theory of planned behavior (La Barbera & Ajzen, 2020; Sommestad et al., 2015), the high desired-state scores indicate positive attitudes and supportive social norms, whereas the low actual-state scores indicate low perceived behavioral control.

RQ2. Prioritized Behavioral Needs

Two dimensions – mobile device security ($PNI_{modified}$ = 0.371) and email security ($PNI_{modified}$ = 0.366) – ranked highest. This ordering reflects the current threat landscape, in which social engineering attacks increasingly target mobile and email channels. According to the Verizon (2026) data breach investigations report in 2026, mobile phishing simulations (via SMS and voice channels) recorded median click rates approximately 40% higher than those for email-based simulations. Pollini et al. (2022) likewise call for greater attention to human factors in mobile cybersecurity research. Because all observed p-values were below .001, the Bonferroni correction did not alter any inferential conclusion; it is reported to make the family of six tests explicit.

Several explanations may account for the gaps in these two domains. In mobile device security, the intimacy paradox leads people to feel that their personal devices are secure (Hadlington, 2017), while small screen size makes it difficult to verify URLs and permissions (Beyer, 2014). In email security, young adults underestimate their susceptibility to phishing because of optimism bias (Dodel & Mesch, 2017), while attackers can readily imitate the urgent tone typical of academic emails. Most importantly, the perceived need for mobile and email security exceeded that for password security.

Security incident reporting ranked third ($PNI_{modified}$ = 0.364). It is particularly important because it is an organizational rather than an individual behavior. Students recognize the significance of reporting but do not know which process to follow or where to report. They also fear reputational damage—a concern especially relevant in collectivist societies such as Thailand (Yang & Chuenterawong, 2025)—and may experience diffusion of responsibility. Unlike password and application security, incident reporting requires infrastructure that students cannot establish on their own.

Password security ranked last ($PNI_{modified}$ = 0.298), substantially below the overall index of 0.354. This finding runs counter to much of the cybersecurity literature, which treats password management as foundational (Kovačević et al., 2020; McCormac et al., 2017). Three explanations are possible. First, controls such as complex passwords, regular password changes, and multi-factor authentication may have instilled good password habits without students' awareness. Second, habit may foster a sense of competence that is not matched by actual competence. Third, the measure assesses perceived rather than observed competence. The practical implication is that educational resources may yield greater returns when directed toward mobile and email security, where the perceived gap is largest.

RQ3. Most Urgent Targets and Relative Magnitude of Need

To address **RQ3** regarding the most urgent targets, the results demonstrated high overall needs as all six $PNI_{modified}$ scores exceeded 0.29, with five above 0.35, though variations in magnitude did exist. Mobile device security ($PNI_{modified}$ = 0.371) and email security (0.366) constituted the top-priority tier. These were followed by a closely grouped middle cluster. These included security incident reporting (0.364), application security (0.363), and social media activity security (0.359).

The spread across these five domains is narrow (0.359-0.371), indicating that they are of broadly comparable urgency, whereas password security (0.298) sits clearly apart as the lowest priority. The practical implication is that an intervention should not treat the six domains as equally weighted: mobile and email security justify the largest share of instructional time, the three middle-tier domains can be addressed together, and password security warrants proportionally less attention than conventional awareness curricula allocate to it.

Practical Recommendations

These findings support three recommendations for curriculum designers and institutional policymakers:

Prioritize mobile and email security in cybersecurity education, replacing or supplementing conventional password-awareness content. Simulation-based training—phishing and smishing exercises with immediate feedback—can address the self-efficacy deficit identified in **RQ1**.

Select experience-based teaching over lectures. As the topic concerns behaviors rather than data, the educational approach should incorporate simulations, reflections about cognitive biases, and gamification based on security topics.

Develop an effective reporting system with reporting portals and policies that protect reporters from reputational damage. Cybersecurity education, including orientation, should be an additional component of the classroom curriculum.

We have also added a sentence to the Limitations section acknowledging that, because sampling was stratified by faculty rather than by program, the study cannot report program-specific needs for the computer technology subgroup; this is identified as a direction for future research

Limitations and Future Research

There are four limitations of these results. First, self-report tools may be affected by social desirability bias. Second, the sample was drawn from a single Thai university and does not reflect other educational establishments and regions; in addition, because sampling was stratified by faculty rather than by program, the study cannot report program-specific needs for the computer technology subgroup, which is identified as a direction for future research. Third, the cross-sectional nature of this study means that results can be observed only at a single point in time, and no causal inference can be drawn. Finally, although participation was voluntary and responses were anonymous, the sample was drawn from a class taught by the author of this research, which could affect participants' behavior. Further research should replicate this study using behavioral rather than self-report measures, adopt longitudinal designs to examine behavior change, test self-efficacy as a mediator, and collect program-level samples sufficient to compare the computer technology subgroup with other students.

CONCLUSIONS

This study identified the cybersecurity behavioral needs of 190 Thai undergraduate students using the $PNI_{modified}$ framework across six dimensions. Large gaps between current and desired behaviors were found across all dimensions, with effect sizes (Cohen's $d > 0.90$) indicating practical significance. The prioritization order, from highest to lowest, was mobile device security ($PNI_{modified}$ = 0.371), email security (0.366), security incident reporting (0.364), application security (0.363), social media activity security (0.359), and password security (0.298).

These priorities offer a data-driven basis for allocating scarce instructional resources. An intervention targeting mobile and email security—the two domains with the largest perceived gaps—is likely to yield the

greatest return. By contrast, password security, which conventional awareness programs often emphasize, ranked lowest, suggesting that institutional controls have already normalized much of the required behavior.

The research contributes to the field in three ways. First, the study is the first empirical analysis, to the authors' knowledge, of the cybersecurity behavioral needs of Thai undergraduates, an area where existing research has mainly focused on raising their awareness. Second, it illustrates how the $PNI_{modified}$ model could be used for cybersecurity education and thus provides a replicable model for cybersecurity needs assessment. Third, the study reveals a larger perceived behavioral gap in mobile and email security than in password security.

Author contributions: JC: conceptualization, data curation, formal analysis, investigation, methodology, project administration, resources, software, validation, visualization, writing – original draft, writing – review & editing; **TK:** conceptualization, data curation, formal analysis, investigation, methodology, resources, software, validation, visualization, writing – original draft, writing – review & editing; **PP:** conceptualization, data curation, formal analysis, methodology, project administration, resources, supervision, validation, visualization, writing – original draft, writing – review & editing; **KB:** investigation, project administration, resources, supervision, writing – original draft, writing – review & editing; **MC:** data curation, methodology, project administration, software, supervision, validation, writing – original draft. All authors approved the final version of the article.

Funding: The authors received no financial support for the research and/or authorship of this article.

Ethics declaration: This study was approved by the Research Ethics Committee at King Mongkut's Institute of Technology Ladkrabang on 5 August 2026 with approval number EC-KMITL_69_169. This study involved only non-vulnerable adult participants (aged 18-22) and did not require the collection of sensitive personal data (Techagaisiyavanit et al., 2025). Participation was voluntary, and informed consent was obtained electronically prior to survey completion. The study complies with the ethical standards of the Declaration of Helsinki (revised 2013) and National Research Council of Thailand's (2024) national policy on ethical principles and guidelines for research involving humans, under which anonymous, low-risk social and behavioral research is exempt from formal institutional ethics review. No personally identifying data was collected, and all participant data was secured in password-protected files.

AI statement: Generative AI and AI-assisted tools were used in the preparation of this manuscript for the following purposes: (1) translation from Thai to English using ChatGPT Open AI, (2) figure enhancement and (2) language editing and proofreading using Grammarly Premium. All AI-generated content was critically reviewed, edited, and validated by the authors, who assume full responsibility for the accuracy, integrity, and originality of the final manuscript. No AI tool was used as a substitute for the authors' own intellectual contribution, critical analysis, interpretation, or scientific judgment.

Declaration of interest: The authors declared no competing interest.

Data availability: Data generated or analyzed during this study are available from the authors on request.

REFERENCES

Akeiber, H. J. (2025). The evolution of social engineering attacks: A cybersecurity engineering perspective. *Al-Rafidain Journal of Engineering Sciences, 3*(1), 294-316. https://doi.org/10.61268/r9c49865

Alqahtani, M. A. (2022). Factors affecting cybersecurity awareness among university students. *Applied Sciences, 12*(5), Article 2589. https://doi.org/10.3390/app12052589

Alsaad, A., & Al-Okaily, M. (2022). Acceptance of protection technology in a time of fear: The case of COVID-19 exposure detection apps. *Information Technology & People, 35*(3), 1116-1135. https://doi.org/10.1108/ITP-10-2020-0719

Aroonsiwagool, A., Tuntiwongwanich, S., Pimdee, P., Meedee, C., & Moto, S. (2025). Assessing instructors' perceptions of critical skills in computational thinking and block-based programming: A needs assessment approach. *International Journal of Instruction, 18*(2), 245-260. https://doi.org/10.29333/iji.2025.18214a

Bandura, A. (2023). Cultivate self-efficacy for personal and organizational effectiveness. In E. A. Locke, & C. Pearce (Eds.), *Principles of organizational behavior: The handbook of evidence-based management* (3rd ed., pp. 113-135). Wiley. https://doi.org/10.1002/9781394320769.ch6

Beyer, C. (2014). Mobile security: A literature review. *International Journal of Computer Applications, 97*(8), 9-11. https://doi.org/10.5120/17025-7315

Bland, J. M., & Altman, D. G. (1995). Multiple significance tests: The Bonferroni method. *BMJ, 310*(6973), Article 170. https://doi.org/10.1136/bmj.310.6973.170

Borriraklert, A., & Kiattisin, S. (2021). User experience design (UXD) competency model: Identifying well-rounded proficiency for user experience designers in the digital age. *Archives of Design Research, 34*(3), 61-79. https://doi.org/10.15187/adr.2021.08.34.3.61

Chaihanchanchai, P., & Anantachart, S. (2024). Unveiling the uses and gratifications of social media: A comparative study of Thai generation Y Internet users in Bangkok and upcountry. *Journal of Mekong Societies, 20*(1), 48-72.

Chimnoy, W., Xupravati, P., & Siribanjitak, P. (2023). Academic management strategies of private elementary schools based on the concept of quality citizenship attributes in the 21st century. *Kasetsart Journal of Social Sciences, 44*(4), 1039-1050. https://doi.org/10.34044/j.kjss.2023.44.4.08

Civaner, M. M., Uncu, Y., Bulut, F., Chalil, E. G., & Tatli, A. (2022). Artificial intelligence in medical education: A cross-sectional needs assessment. *BMC Medical Education, 22*, Article 772. https://doi.org/10.1186/s12909-022-03852-3

Datta, P., & Acton, T. (2025). Promises and perils of generative AI in cybersecurity. *MIS Quarterly Executive, 24*(2), 167-184. https://doi.org/10.17705/2msqe.00115

Daudi, M. (2024). Exploiting human trust in cybersecurity: Which trust development process is predominant in phishing attacks? *Applied Cybersecurity & Internet Governance, 3*, 1-22. https://doi.org/10.60097/acig/199452

Dodel, M., & Mesch, G. (2019). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior, 94*, 107-117. https://doi.org/10.1016/j.chb.2016.11.044

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), Article e00346. https://doi.org/10.1016/j.heliyon.2017.e00346

Hoonsopon, D., Ketkaew, C., Puriwat, W., Viriyasitavat, W., & Tripopsakul, S. (2025). How digital health literacy affects willingness to adopt telemedicine in an emerging country: The case of Thailand. *SAGE Open, 15*(3), Article 21582440251378068. https://doi.org/10.1177/21582440251378068

House, N. (2026). Phishing statistics [2026]: Latest attack data & trends. *StationX*. https://app.stationx.net/articles/phishing-statistics

Hunsapun, N. (2023). *Exploring trends and insights of information literacy education in Asian countries* [PhD thesis, National Taiwan Normal University].

Intarakamhang, U., Tuntivivat, S., Pattrawiwat, K., Prasittichok, P., Pichaisamart, N., Thaksin, S., & Wongthong, P. (2025). Validity of measurement and causal model of online scam protection behavior among risk Thai students. *European Journal of Educational Research, 14*(2), 661-675. https://doi.org/10.12973/eu-jer.14.2.661

International Telecommunication Union. (2024). Facts and figures 2024. *ITU*. https://www.itu.int/itu-d/reports/statistics/2024/11/10/ff24-internet-use

Janpirom, C., Tuntiwongwanich, S., Pimdee, P., Kulworatit, C., & Moto, S. (2025). Lecturers' perspectives on undergraduate students' innovative thinking skills and creative problem-solving skills: A comparative needs analysis. *International Journal of Instruction, 18*(3), 121-140. https://doi.org/10.29333/iji.2025.1837a

Jittam, P., Sriwattanarothai, N., Ketpichainarong, W., Chenprakhon, P., & Pichitpornchai, C. (2026). From classroom to online learning during the COVID-19 transition in Thailand: A mixed-methods study of pedagogical transformation and digital resilience in science-based faculties. *Journal of Innovative Learning, 2*(1), 45-57.

Kemp, S. (2025). Digital 2026: Thailand. *DataReportal*. https://datareportal.com/reports/digital-2026-thailand

Khamcharoen, N., Kantathanawat, T., & Sukkamart, A. (2022). Developing student creative problem-solving skills (CPSS) using online digital storytelling: A training course development method. *International Journal of Emerging Technologies in Learning, 17*(11), 17-34. https://doi.org/10.3991/ijet.v17i11.29931

Khong-ngam, S., Wongwanich, S., & Piromsombat, C. (2014). Principals' and teachers' use of evaluation results for student learning in science. *Procedia – Social and Behavioral Sciences, 116*, 1902-1907. https://doi.org/10.1016/j.sbspro.2014.01.492

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors related to cyber security behavior. *IEEE Access, 8*, 125140-125148. https://doi.org/10.1109/ACCESS.2020.3007867

Kraiwanit, T., Limna, P., Sonsuphap, R., & Chutipat, V. (2025). Predictors of digital fraud: Evidence from Thailand. *Journal of Risk and Financial Management, 18*(12), Article 671. https://doi.org/10.3390/jrfm18120671

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and Psychological Measurement, 30*(3), 607-610. https://doi.org/10.1177/001316447003000308

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296. https://doi.org/10.1016/j.cose.2006.02.008

La Barbera, F., & Ajzen, I. (2020). Control interactions in the theory of planned behavior: Rethinking the role of subjective norm. *Europe's Journal of Psychology, 16*(3), 401-417. https://doi.org/10.5964/ejop.v16i3.2056

Lallie, H. S., Thompson, A., Titis, E., & Stephens, P. (2025). Analysing cyber attacks and cyber security vulnerabilities in the university sector. *Computers, 14*(2), Article 49. https://doi.org/10.3390/computers14020049

Lapmak, R. (2025). Industry outlook 2025-2027: Data center industry. *Krungsri Research*. https://www.krungsri.com/en/research/industry/industry-outlook/services/data-center/io/io-data-center-2025-2027

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports, 5*, Article 100165. https://doi.org/10.1016/j.chbr.2021.100165

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

Mohsin, K. (2025). *Cybercrime and privacy in the digital age: Legal frameworks, emerging challenges, and future trends*. SSRN. https://doi.org/10.2139/ssrn.5169894

Nantha, C., Siripongdee, K., Siripongdee, S., Pimdee, P., Kantathanawat, T., & Boonsomchuae, K. (2024). Enhancing ICT literacy and achievement: A TPACK-based blended learning model for Thai business administration students. *Education Sciences, 14*(5), Article 455. https://doi.org/10.3390/educsci14050455

National Research Council of Thailand. (2024). Research standards & ethics: Strengthening quality, integrity and responsible research in Thailand. *NRCT*. https://en.nrct.go.th/hilghlight/detail/490

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). *Computers & Security, 42*, 165-176. https://doi.org/10.1016/j.cose.2013.12.003

Pimdee, P., Sukkamart, A., Nantha, C., Kantathanawat, T., & Leekitchwatana, P. (2024). Enhancing Thai student-teacher problem-solving skills and academic achievement through a blended problem-based learning approach in online flipped classrooms. *Heliyon, 10*(7), Article e29172. https://doi.org/10.1016/j.heliyon.2024.e29172

Pimsalee, S., Sukkamart, A., Pimdee, P., & Meedee, C. (2026). Prioritizing software development skill needs for Thai pre-service computer technology teachers. *Contemporary Educational Technology, 18*(2), Article ep638. https://doi.org/10.30935/cedtech/18039

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

Prasittichok, P., & Klaykaew, K. K. (2022). Meta-skills development needs assessment among undergraduate students. *Heliyon, 8*(1), Article e08787. https://doi.org/10.1016/j.heliyon.2022.e08787

Pushsapavardhana, N. (2025). Social media usage and cyberbullying: Experiences and coping strategies among secondary school students in Surat Thani, Thailand. *Humanities, Arts and Social Sciences Studies, 25*(3), 550-566. https://doi.org/10.69598/hasss.25.3.278093

Rosenberg, H., Blondheim, M., & Sabag-Ben Porat, C. (2025). Who in the world is generation Z? The rise of mobile natives and their socio-technological identity. *Societies, 15*(11), Article 314. https://doi.org/10.3390/soc15110314

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet, 11*(4), Article 89. https://doi.org/10.3390/fi11040089

Samae, N., Boonmongkol, P., Ojanen, T. T., Samakkeekharom, R., & Guadamuz, T. E. (2014). Youth perceptions on cyberbullying. *Journal of Behavioral Science for Development, 6*(1), 1-14.

Shahid, J., Hameed, M. K., Javed, I. T., Qureshi, K. N., Ali, M., & Crespi, N. (2022). A comparative study of web application security parameters: Current trends and future directions. *Applied Sciences, 12*(8), Article 4077. https://doi.org/10.3390/app12084077

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A study on the psychology of social engineering-based cyberattacks and existing countermeasures. *Applied Sciences, 12*(12), Article 6042. https://doi.org/10.3390/app12126042

Singh, A. S., & Masuku, M. B. (2014). Sampling techniques and determination of sample size in applied statistics research: An overview. *International Journal of Economics, Commerce and Management, 2*(11), 1-22.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information and Computer Security, 23*(2), 200-217. https://doi.org/10.1108/ICS-04-2014-0025

Sureeyatanapas, P., Srisawasdi, N., & Sureeyatanapas, P. (2024). A need analysis of English proficiency in engineering graduates: Perspectives of the world's leading companies in Thailand. *European Journal of Engineering Education, 49*(6), 1179-1202. https://doi.org/10.1080/03043797.2024.2377314

Susyanto, S., Mulyanti, R. Y., & Rini, N. (2026). Extending protection motivation theory for organizational cybersecurity behavior: A systematic literature review. *Jurnal Ilmiah Ilmu Terapan Universitas Jambi, 10*(2), 1114-1131. https://doi.org/10.22437/jiituj.v10i2.54776

Tanti, R. (2024). Phishing attack: A case study and their prevention techniques. *International Journal for Multidisciplinary Research, 6*(5), 1-43. https://doi.org/10.36948/ijfmr.2024.v06i05.29087

Techagaisiyavanit, W., Mingmontchaikul, B., & Keitleartthum, S. (2026). Navigating ethical challenges in research ethics approval: A case study of social science research in Thailand. *Research Ethics, 22*(1), 81-104. https://doi.org/10.1177/17470161251336573

Verizon. (2026). *2026 data breach investigations report*. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems, 51*(3), 576-586. https://doi.org/10.1016/j.dss.2011.03.002

Wongwanich, S., Sakolrak, S., & Piromsombat, C. (2014). Needs for Thai teachers to become a reflective teacher: Mixed methods needs assessment research. *Procedia – Social and Behavioral Sciences, 116*, 1645-1650. https://doi.org/10.1016/j.sbspro.2014.01.450

Wuttikamonchai, O., Pimdee, P., Ployduangrat, J., & Sukkamart, A. (2024). A needs assessment evaluation of information technology student mobile website design skills. *Contemporary Educational Technology, 16*(1), Article ep494. https://doi.org/10.30935/cedtech/14173

Yang, J., & Chuenterawong, P. (2025). Rethinking crisis response: Cross-cultural insights from comparing American and Korean corporate apologies. *International Journal of Communication, 19*, 47-69.

Yurayat, P., & Seechaliao, T. (2021). Needs assessment to develop online counseling program. *International Education Studies, 14*(7), 59-71. https://doi.org/10.5539/ies.v14n7p59

Zimba, A., Phiri, K., Kashale, C., & Phiri, M. (2025). Unveiling deception: A socio-economic analysis of smishing attacks on mobile money transaction users. *Humanities and Social Sciences Communications, 12*, Article 1880. https://doi.org/10.1057/s41599-025-06141-8

APPENDIX A: CYBERSECURITY BEHAVIOR NEEDS ASSESSMENT QUESTIONNAIRE

Research Questionnaire

Topic: Priority needs for cybersecurity behavior among undergraduate students

Objectives: This questionnaire aims to assess the priority needs for cybersecurity behavior among second-year undergraduate students at DRU, Samut Prakan, who are enrolled in the media literacy course. The questionnaire consists of three sections:

Section 1: Demographic information

Section 2: Cybersecurity behavior needs assessment

Section 3: Additional suggestions

All responses will be kept confidential and used for research purposes only. Please answer all questions honestly and completely. Thank you for your cooperation.

Section 1. Demographic Information

Instructions: Please tick (✓) the box that best describes you.

1.1 Gender

□ 1) Male □ 2) Female □ 3) Other

1.2 Current cumulative grade point average (GPAX)

□ 1) 3.51 - 4.00 □ 2) 3.01 - 3.50 □ 3) 2.51 - 3.00 □ 4) 2.01 - 2.50 □ 5) 2.00 or below

1.3 Faculty

□ 1) Management science □ 2) Science and technology □ 3) Education □ 4) Humanities and social sciences

Table A1. Rating scale

Rating	Current behavior (actual)	Desired behavior (ideal)
5	Strongly agree	Strongly agree
4	Agree	Agree
3	Neutral	Neutral
2	Disagree	Disagree
1	Strongly disagree	Strongly disagree

Section 2. Cybersecurity Behavior Needs Assessment

Instructions: Please indicate your level of agreement with each statement for both your current behavior (D)—what you actually do—and your desired behavior (I)—what you think you should do. Tick (✓) the box that best reflects your opinion for each column.

Table A2. Cybersecurity behavior needs assessment

No	Item	Current (D)	Desired (I)
2.1 Password security (CSB-PW)			
1.1	I set passwords that are 8–12 characters long, including uppercase letters, lowercase letters, numbers, and symbols.	5 4 3 2 1	5 4 3 2 1
1.2	I do not use the same password for all websites or applications.	5 4 3 2 1	5 4 3 2 1
1.3	I change my passwords every 3–6 months and do not reuse old passwords.	5 4 3 2 1	5 4 3 2 1
1.4	I keep my passwords confidential and do not share them with others.	5 4 3 2 1	5 4 3 2 1
1.5	I enable two-factor authentication (2FA) for important applications.	5 4 3 2 1	5 4 3 2 1
1.6	I do not use easily guessable personal information (e.g., birthdate, phone number) as passwords.	5 4 3 2 1	5 4 3 2 1
1.7	I do not use sequential keyboard patterns (e.g., 123456, qwerty, asdf) as passwords.	5 4 3 2 1	5 4 3 2 1
1.8	I do not write down passwords on paper or in notebooks that others can easily access or see.	5 4 3 2 1	5 4 3 2 1
1.9	I do not save passwords in web browsers when using public computers.	5 4 3 2 1	5 4 3 2 1
1.10	I always log out of systems when I finish using a shared device.	5 4 3 2 1	5 4 3 2 1
2.2 Social media activity security (CSB-SM)			
2.1	I am cautious when uploading personal photos or information on social media.	5 4 3 2 1	5 4 3 2 1
2.2	I avoid publicly sharing or checking in to my current location.	5 4 3 2 1	5 4 3 2 1
2.3	I am cautious when texting or video-calling with strangers.	5 4 3 2 1	5 4 3 2 1
2.4	I immediately report suspicious activities or accounts on social media.	5 4 3 2 1	5 4 3 2 1
2.5	I adjust privacy settings to limit who can access my information.	5 4 3 2 1	5 4 3 2 1
2.6	I verify the accuracy of information and news before sharing or forwarding it.	5 4 3 2 1	5 4 3 2 1

Table A2 (Continued).

No	Item	Current (D)	Desired (I)
2.7	I do not click on suspicious links in chat messages, even if they are sent by someone I know.	5 4 3 2 1	5 4 3 2 1
2.8	I carefully consider and screen friend requests before accepting them.	5 4 3 2 1	5 4 3 2 1
2.9	I do not comment on or post content that may violate others' privacy or personal information.	5 4 3 2 1	5 4 3 2 1
2.10	I delete or deactivate old social media accounts I no longer use to prevent identity theft.	5 4 3 2 1	5 4 3 2 1
2.3 Application security (CSB-AP)			
3.1	I choose official applications that are properly licensed and owned by the respective organization.	5 4 3 2 1	5 4 3 2 1
3.2	I avoid accessing untrustworthy or suspicious websites.	5 4 3 2 1	5 4 3 2 1
3.3	I avoid downloading files from unsafe peer-to-peer (P2P) file-sharing networks.	5 4 3 2 1	5 4 3 2 1
3.4	I read and understand the Terms of Service before installing applications.	5 4 3 2 1	5 4 3 2 1
3.5	I review and manage app permissions (e.g., camera, microphone access) appropriately.	5 4 3 2 1	5 4 3 2 1
3.6	I regularly update applications and operating systems to the latest versions to patch vulnerabilities.	5 4 3 2 1	5 4 3 2 1
3.7	I install and use antivirus software on my computer devices.	5 4 3 2 1	5 4 3 2 1
3.8	I do not root or jailbreak my devices to install applications from unofficial stores.	5 4 3 2 1	5 4 3 2 1
3.9	I always scan applications with a virus scanner before installing them.	5 4 3 2 1	5 4 3 2 1
3.10	I regularly review and uninstall unused applications from my devices.	5 4 3 2 1	5 4 3 2 1
2.4 Email security (CSB-EM)			
4.1	I reject and delete attachments from emails with unknown or unclear sources.	5 4 3 2 1	5 4 3 2 1
4.2	I do not click links or open attachments from unsolicited emails.	5 4 3 2 1	5 4 3 2 1
4.3	I do not forward chain emails or spam to others.	5 4 3 2 1	5 4 3 2 1
4.4	I verify the sender's email address before replying or clicking any links.	5 4 3 2 1	5 4 3 2 1
4.5	I never send sensitive information, financial data, or passwords via email.	5 4 3 2 1	5 4 3 2 1
4.6	I clearly separate my personal email from my academic/university email.	5 4 3 2 1	5 4 3 2 1
4.7	I look for unusual language or writing patterns commonly found in phishing emails.	5 4 3 2 1	5 4 3 2 1
4.8	I regularly clear my inbox and delete spam or unnecessary emails.	5 4 3 2 1	5 4 3 2 1
4.9	I do not use my personal email to register for untrustworthy websites or applications.	5 4 3 2 1	5 4 3 2 1
4.10	I use the blind carbon copy function when sending mass emails to protect others' email privacy.	5 4 3 2 1	5 4 3 2 1
2.5 Mobile device security (CSB-MD)			
5.1	I am cautious about security when conducting financial transactions via banking applications.	5 4 3 2 1	5 4 3 2 1
5.2	I carefully check the reliability of online stores before making purchases.	5 4 3 2 1	5 4 3 2 1
5.3	I am cautious when using public Wi-Fi to log in to important systems.	5 4 3 2 1	5 4 3 2 1
5.4	I always set a screen lock using a password, fingerprint, or facial recognition.	5 4 3 2 1	5 4 3 2 1
5.5	I enable device-tracking features (e.g., Find My Device) to locate my device if it is lost.	5 4 3 2 1	5 4 3 2 1
5.6	I avoid charging my device via public USB ports to prevent data theft.	5 4 3 2 1	5 4 3 2 1
5.7	I regularly back up important data to the cloud or an external storage device.	5 4 3 2 1	5 4 3 2 1
5.8	I turn off Bluetooth or Wi-Fi when not in use to prevent unwanted connections.	5 4 3 2 1	5 4 3 2 1
5.9	I do not leave my personal mobile device unattended in public places.	5 4 3 2 1	5 4 3 2 1
5.10	I verify the URL and look for the HTTPS padlock symbol when conducting online transactions.	5 4 3 2 1	5 4 3 2 1
2.6 Security incident reporting (CSB-IR)			
6.1	I prevent unauthorized access to my devices or personal information.	5 4 3 2 1	5 4 3 2 1
6.2	I take immediate action or report any anomalies I detect (e.g., viruses, data theft).	5 4 3 2 1	5 4 3 2 1
6.3	I alert relevant parties when I detect a security breach or unauthorized system access.	5 4 3 2 1	5 4 3 2 1
6.4	I preserve evidence (e.g., screenshots) when I encounter suspicious activity or cyber threats.	5 4 3 2 1	5 4 3 2 1
6.5	I know how and where to contact the system administrator or relevant authorities when a security incident occurs.	5 4 3 2 1	5 4 3 2 1
6.6	I cooperate with university staff or authorities by providing information during cybersecurity incident investigations.	5 4 3 2 1	5 4 3 2 1
6.7	I immediately alert friends or close contacts when I discover their accounts have been hacked or show unusual activity.	5 4 3 2 1	5 4 3 2 1
6.8	I change my passwords immediately if I suspect my personal information or passwords have been compromised.	5 4 3 2 1	5 4 3 2 1
6.9	I immediately freeze my credit cards or bank accounts if I notice financial transactions I did not authorize.	5 4 3 2 1	5 4 3 2 1
6.10	I monitor cybersecurity threat alerts to stay prepared and report incidents promptly.	5 4 3 2 1	5 4 3 2 1

Section 3. Additional Suggestions

Instructions: Please provide any additional comments or suggestions regarding cybersecurity behaviors or education at your university. *(Open-ended response space)* End of Questionnaire.

