Student Attitude Toward Cybersecurity Awareness Training in Universities

Tan Quang Duong[1*] and Luan Trong Nguyen[2]

[1]Department of Information Assurance, FPT University, Vietnam, *tandqce180272@fpt.edu.vn
[2]Department of Entrepreneurship, FPT University, Vietnam, luannt73@fe.edu.vn

Abstract. This study used the Technology Acceptance Model to investigate undergraduate perceptions of cybersecurity awareness training (CAT) at Vietnamese institutions. A total of 250 full-time students from institutions across the Mekong Delta completed the survey. Results showed moderately positive attitudes, with strong scale reliability. Perceived usefulness and perceived ease of use scored similarly high, yet intention to practice safe online behavior stayed lukewarm. One-way ANOVA indicated substantial variations across academic years, with final-year students exhibiting the highest receptivity. Behavioral intention, however, remained unchanged across years, exposing a clear awareness–action disconnect. The evidence suggests that current knowledge-focused efforts fall short; universities should therefore introduce compulsory, practical, and regionally tailored cybersecurity units into the regular curriculum to foster genuine and durable behavioral change.

Keywords: Cybersecurity awareness training (CAT) · Higher education · Information security education · Student attitude · Behavioral change · Technology Acceptance Model

1 Introduction

As universities increasingly rely on digital platforms—e-learning systems, cloudbased research databases, and shared storage services—both students and staff have unintentionally created a much larger attack surface for cyber threats [2]. Despite growing attention to the problem, many higher education institutions still lack systematic, campus-specific cybersecurity awareness programs [4]. Previous studies have repeatedly found that university students possess reasonable theoretical knowledge of basic concepts such as strong passwords, phishing recognition, and personal data protection, yet they rarely put this knowledge into practice in everyday life [3,7]. The main reason appears to be that most existing training initiatives remain too generic, lecture-style, and disconnected from the apps and online habits students actually use (e.g., Zalo, TikTok, Shopee), resulting in little or no behavioral change [1,7].

Because today's university students will soon become the main users of technology in the workforce, understanding their real perceptions is crucial for developing effective cybersecurity awareness programs. Previous studies have shown that perceived rele-

C. V. Garces et al. (eds.), *Proceedings of the 6th International Conference on Internet, Education and Information Technology (IEIT 2026)*, Atlantis Highlights in Social Sciences, Education and Humanities 53,
https://doi.org/10.2991/978-94-6239-733-0_44

vance, clarity, and delivery format are key factors shaping attitudes toward cybersecurity education [3]. Among technology acceptance models, the Technology Acceptance Model (TAM) [5] remains one of the most widely validated frameworks across diverse technologies and user populations. It was therefore selected as a suitable lens for examining why students may acknowledge the value of cybersecurity awareness training while still failing to apply recommended practices in their daily digital lives. The present study applies TAM to explore Vietnamese undergraduate students' perceived usefulness, perceived ease of use, attitude, and behavioral intention regarding CAT, aiming to propose more engaging and contextually suitable training approaches for the Vietnamese higher education setting.

2 Literature Review

2.1 Importance of Cybersecurity Awareness in Higher Education

Higher education institutions are exposed to substantial cyber risks owing to their open network architecture, the widespread use of personal devices, and the sensitive nature of academic and research data [2]. Empirical evidence indicates that universities suffer a higher incidence of successful attacks—particularly phishing and ransomware—than many commercial organizations of comparable size [1]. In Vietnam, the abrupt shift to online teaching and administration during the COVID-19 pandemic significantly increased these vulnerabilities while awareness and training initiatives lagged behind [4].

2.2 Student Attitudes and Behavioral Factors

Empirical work across different countries reveals a persistent pattern: undergraduate students typically possess adequate declarative knowledge of core security practices—password complexity, phishing cues, data encryption—but translate this knowledge into routine behavior only rarely [3,7]. Explanations center on low perceived personal vulnerability and the perceived cost (time and effort) of adopting protective habits. Direct experience of a successful attack emerges as the factor most consistently associated with stronger attitudes and improved compliance.

2.3 Effectiveness of Cybersecurity Awareness Training Programs

Evidence from earlier work shows that conventional one-off training sessions achieve little beyond a temporary knowledge increase [6]. Follow-up measurements typically reveal rapid decay of any gains. Programs that rely on repeated exposure, active participation, and elements such as gamified simulations or credit-linked completion, however, generate measurable and lasting improvements in security behavior [1]. In studies that have employed TAM in this domain, perceived usefulness has emerged as the most consistent predictor of participant acceptance, followed by perceived ease of use [4].

2.4 Gaps in Current Research

Most published studies on cybersecurity awareness training originate from North America, Europe, India, and a few Middle Eastern countries, while empirical evidence from Southeast Asia remains scarce, and no previous work has applied TAM to Vietnamese university students. This gap is particularly significant because Vietnam constitutes a unique sociotechnical environment: students rely heavily on local platforms such as Zalo and Shopee that rarely appear in Western training materials; the rapid shift to online education during COVID-19 occurred with limited investment in security infrastructure [4]; most Vietnamese universities offer no compulsory cybersecurity courses and depend on ad-hoc awareness activities; and, as a fast-growing developing economy with constrained resources, Vietnam faces distinct challenges compared with both developed nations and other developing regions.

In the surveyed institutions—FPT University Can Tho, Can Tho University, and Tra Vinh University—CAT currently consists of one-time, lecture-style sessions or sporadic optional online modules, with no integration into creditbearing curriculum [4]. This approach, lacking repetition, active participation, or simulation elements, likely explains the limited behavioral impact observed and confirms that delivery format is critical when interpreting the awareness–behavior gap.

3 Methodology

3.1 Theoretical Framework

The study employed the Technology Acceptance Model (TAM) proposed by Davis [5]. TAM remains one of the most robust and parsimonious frameworks for predicting user acceptance of new systems. It postulates that two primary beliefs—perceived usefulness (PU) and perceived ease of use (PEOU)—determine an individual's attitude toward using the system, which in turn affects behavioral intention. For the present research, cybersecurity awareness training (CAT) was conceptualized as the target "system". This approach allowed examination of why students may recognize the importance of cybersecurity yet fail to translate awareness into sustained behavioral change.

3.2 Research Design and Participants

A cross-sectional, descriptive quantitative design was adopted. The sample included 250 undergraduate students attending higher education institutions in the Mekong Delta area of Vietnam (FPT University Can Tho, Can Tho University, Tra Vinh University). Participants' ages ranged from 18 to 24 years. Convenience sampling, augmented by snowball approaches, was employed: the questionnaire link was originally disseminated by professors and class representatives via Zalo and university Facebook groups, with respondents urged to share it with their classmates.

For the qualitative phase, three participants were intentionally chosen to guarantee diversity in academic year and discipline: a fourth-year Information Technology student, a second-year Economics student, and a third-year Graphic Design student. Semi-structured interviews, lasting 20–30 minutes each, were conducted face-to-face in Vietnamese. All participants gave informed consent and were guaranteed anonymity. Given the small sample size ($n = 3$), these interviews were designed to provide illustrative examples of the mechanisms underlying quantitative findings rather than to achieve thematic saturation or produce generalizable qualitative themes.

Table 1. Descriptive Statistics and Reliability of TAM Constructs.

Construct	M	SD	Items	Cronbach's α
Perceived Usefulness (PU)	3.54	0.77	7	0.946
Perceived Ease of Use (PEOU)	3.52	0.87	7	0.934
Attitude Toward Using (ATT)	3.51	0.82	6	0.906
Behavioral Intention (BI)	3.50	0.95	6	0.881

3.3 Research Instrument

The questionnaire contained 26 items measuring the four core TAM constructs:

Perceived Usefulness (7 items), Perceived Ease of Use (7 items), Attitude Toward Using (6 items), and Behavioral Intention (6 items). Items were adapted from the original TAM instrument [5] and subsequent information-security studies. Responses were recorded on a five-point Likert scale (1 = strongly disagree, 5 = strongly agree). Demographic questions and items on prior cybersecurity training and victimization experience were also included.

The six Behavioral Intention items captured self-reported likelihood of adopting safe practices (e.g., "I intend to regularly update my passwords"; "I plan to enable two-factor authentication"). This self-report approach, standard in TAM research, is a recognized limitation. Future studies should complement intention measures with objective proxies such as phishing-simulation click rates or multi-factor authentication enrollment logs.

3.4 Data Analysis

Data were analyzed using IBM SPSS Statistics 27. Descriptive statistics and Cronbach's α were computed first. Pearson correlations analyzed the links among the TAM dimensions. One-way ANOVA with Tukey HSD post-hoc tests assessed differences across academic years. Assumptions of normality (Q-Q plots, skewness/kurtosis within ±1.0) and homogeneity of variance (Levene's test, $p > .05$) were met; group sizes > 30 and the Central Limit Theorem further supported the use of parametric tests [9].

4 Results

4.1 Demographic Characteristics

The 250 respondents were distributed across all academic years, with fourth-year students comprising the largest group (34.0%). Gender distribution was 38.4% male, 29.6% female, and 32.0% either selected "other" or preferred not to disclose.

4.2 Descriptive Statistics and Reliability

Means of the TAM constructs ranged from 3.50 to 3.54 (slightly above neutral), with standard deviations between 0.77 and 0.95 (Table 1). All scales demonstrated excellent internal consistency (Cronbach's $\alpha = 0.881–0.946$), well above the 0.70 threshold [9].

Table 2. One-Way ANOVA Results for TAM Constructs by Academic Year.

Construct	Source	SS	df	MS	F	p
PU	Between	23.45	4	5.86	8.71	< .001
	Within	164.89	245	0.67		
PEOU	Between	11.81	4	2.95	4.81	.001
	Within	150.39	245	0.61		
ATT	Between	38.28	4	9.57	12.62	< .001
	Within	185.88	245	0.76		
BI	Between	1.25	4	0.31	0.52	.722
	Within	147.06	245	0.60		

4.3 Descriptive Statistics by Academic Year

The analysis demonstrates the disconnect between awareness and action: Perceived Usefulness (PU), Perceived Ease of Use (PEOU), and Attitude (ATT) exhibited a progressive increase from Year 1 to Year 5+, while Behavioral Intention (BI) remained relatively stable, ranging from 3.43 to 3.64. This divergence indicates that cognitive and affective improvements do not result in enhanced behavioral commitment.

4.4 Correlation Analysis

Correlation analysis indicated moderate positive associations between PU, PEOU, and ATT ($r = .213$ to $.316$, $p < .01$). Nevertheless, perceived utility (PU) and behavioral intentions (BI) demonstrated a non-significant association ($r = .120$, $p = .058$), suggesting that perceived usefulness did not have a significant impact on behavioral intentions.

4.5 One-Way ANOVA Results

One-way ANOVA indicated significant differences across academic years for PU ($F(4,245) = 8.71$, $p < .001$), PEOU ($F(4,245) = 4.81$, $p = .001$), and ATT ($F(4,245) =$

12.62, $p < .001$), but not for BI ($F(4,245) = 0.52$, $p = .722$) (Table 2). Tukey HSD post-hoc tests showed that Year 5+ students scored significantly higher than Year 1 students on PU (mean difference ≈ 1.06, $p < .001$), PEOU, and ATT. No year-based differences were found for BI.

4.6 Illustrative Interviews: Understanding the Awareness–Behavior Gap

Semi-structured interviews with three students (Information Technology, Economics, and Graphic Design majors) revealed that direct exposure to cyber incidents was the main driver of heightened awareness, while adoption of secure behaviors was impeded by time pressure, academic demands, and convenience tradeoffs. Participants strongly advocated for discipline-specific, platform-relevant training (e.g., GitHub for IT, Shopee/Zalo for Economics, Behance/WeTransfer for Graphic Design) delivered via short, interactive, gamified formats instead of generic lectures.

Interviewees highlighted inconvenience (e.g., security steps perceived as disruptive during deadlines) and the absence of immediate consequences as key barriers, consistent with distrust in generic institutional guidance not perceived as contextually relevant. Future studies could supplement surveys with focus groups to examine whether such distrust and convenience norms systematically suppress behavioral change in Vietnamese higher education.

5 Discussion

5.1 Principal Findings

The results are broadly consistent with international studies but highlight a pattern especially evident in Vietnamese universities. The perceived utility and general attitude towards cybersecurity awareness training dramatically improve with academic advancement, as senior students score nearly one full scale point better in perceived usefulness than first-year students (mean difference = 1.06, $p < .001$). However, behavioral intention shows no significant variation across academic years ($F = 0.52$, $p = .722$), and the correlation between perceived usefulness and behavioral intention is weak and non-significant ($r = .120$, $p = .058$). This complete decoupling of improving perceptions from stagnant intention raises serious questions about the applicability of TAM to preventive security behaviors, which impose immediate costs for uncertain future gains.

5.2 Mechanisms Underlying the Awareness–Behavior Gap

The qualitative interviews reveal four principal mechanisms contributing to the disparity: (i) temporal discounting of prospective risks; (ii) convenience–security trade-offs under time constraints or creative momentum; (iii) lack of contextual pertinence in training (generic examples not related to Zalo, Shopee, GitHub, or Behance); and (iv) absence of explicit implementation intentions or habitformation prompts. Personal experience with real incidents (internship phishing, portfolio hijacking) was unanimously

cited as the only factor that genuinely shifted attitudes, far outweighing formal training sessions.

5.3 Theoretical Implications

The tenuous connection between perceived utility and behavioral intention indicates that TAM, although helpful for productivity tools that provide immediate advantages, is insufficient by itself for cybersecurity scenarios. Future research should evaluate hybrid models that integrate TAM with constructs from Protection Motivation Theory (threat appraisal, coping appraisal) or the Theory of Planned Behavior (subjective norms, perceived behavioral control). Moreover, because the present study measured intention rather than actual behavior, subsequent work must include objective metrics such as password-complexity audits, phishing-simulation click rates, and multi-factor authentication adoption rates.

Cultural context also shapes TAM dynamics in Vietnam. As a collectivist society [10], Vietnamese students are more influenced by authority endorsement and peer norms than by individual risk appraisal: perceived usefulness may be amplified when CAT is endorsed by instructors or senior peers, while behavioral intention may be suppressed when secure practices are seen as non-conforming—a pattern distinct from individualistic cultures where personal vulnerability drives adoption. The qualitative emphasis on peer-mentoring aligns with these tendencies. Future research should explore hybrid TAM models incorporating Hofstede's collectivism-individualism axis to better capture socio-cultural dynamics in Southeast Asian cybersecurity contexts.

5.4 Practical Implications

To convert rising awareness into sustained secure behavior, Vietnamese universities should: (i) incorporate cybersecurity education as a mandatory, credit-bearing course delivered in regular, short, interactive sessions rather than one-off voluntary seminars; (ii) reduce friction by enforcing two-factor authentication across all university systems and issuing security reminders through Zalo; (iii) create discipline-specific, Vietnamese-language training modules using authentic attack examples from platforms students actually use (GitHub and Discord for IT students, Shopee and Zalo groups for Economics students, Behance for Graphic Design students); (iv) conduct regular, gamified phishing simulations with immediate feedback; and (v) implement peer-mentoring initiatives wherein upperclassmen function as security advocates for subsequent student groups.

6 Conclusion

This mixed-methods study of 250 Vietnamese undergraduates shows that students clearly see the value of cybersecurity awareness training—with high perceived usefulness and positive attitude—yet their behavioral intention to adopt secure behaviors re-

mains modest, confirming the classic awareness–behavior gap. One-way ANOVA revealed that perceived usefulness, ease of use, and attitude all vary significantly across academic years, with upper-year students scoring highest, but behavioral intention shows no significant difference. The correlation between perceived usefulness and behavioral intention was weak and statistically insignificant ($r = .120$, $p = .058$).

Qualitative interviews provided explanatory depth, revealing that direct exposure to cyber incidents drives attitude change, while convenience–security trade-offs prevent behavioral adoption despite growing awareness. Students unanimously demanded discipline-specific, contextually relevant training featuring platforms they actually use—GitHub and Discord for IT, Shopee and business platforms for Economics, Behance and creative tools for Graphic Design—rather than generic Western-focused content. Current one-off, lecture-style programs are simply not enough. To produce real change, universities must embed short, interactive, gamified, and credit-bearing cybersecurity modules into the core curriculum, reduce friction through automatic security integration into existing workflows, and leverage peer influence through upper-year student mentorship. Until training becomes mandatory, relevant, and engaging, human error will remain the weakest link in campus cybersecurity.

References

1. Alqahtani, M.A.: Factors affecting cybersecurity awareness among university students. Applied Sciences 12(5), 2589 (2022)
2. Bóttyan, L.: Cybersecurity awareness among university students. Journal of Applied Technical and Educational Sciences 13(3), Article 363 (2023)
3. Ahamed, B., Polas, M.R.H., Kabir, A.I., Sohel-Uz-Zaman, A.S.M., Fahad, A.A., Chowdhury, S., Dey, M.R.: Empowering students for cybersecurity awareness management in the emerging digital era. SAGE Open 14(1) (2024)
4. Dash, B., Ansari, M.F.: An effective cybersecurity awareness training model: First defense of an organizational security strategy. Int. Res. J. Eng. Technol. 9(4), 2347– 2353 (2022)
5. Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quart. 13(3), 319–340 (1989)
6. Kruger, H.A., Kearney, W.D.: A prototype for assessing information security awareness. Comput. Secur. 25(4), 289–296 (2006)
7. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., Basim, H.N.: Cyber security awareness, knowledge and behavior: A comparative study. J. Comput. Inf. Syst. 62(1), 82–97 (2022)
8. Nunnally, J.C., Bernstein, I.H.: Psychometric Theory, 3rd edn. McGraw-Hill, New York, NY, USA (1994)
9. Hofstede, G.: Culture's Consequences: International Differences in Work-related Values. Sage, Beverly Hills, CA, USA (1980)