Factors affecting privacy protection behavior in e-learning based on the extended protection motivation theory

Le Nhat Tung[1,*], Huynh Thai Linh[2], Ho Gia Thanh[2], Truong Minh Khoa[2]

[1]Dong Nai Technology University, Dong Nai, Vietnam
[2]HUTECH University, Ho Chi Minh City, Vietnam

**Corresponding author. Email: lenhattung@dntu.edu.vn*

Received: dd/mm/yyyy

ABSTRACT

Privacy protection on E-learning systems has become increasingly important as students must share extensive personal information during online learning. This study applies the Extended Protection Motivation Theory (PMT) to model factors influencing students' privacy protection behavior. Data from 158 students were analyzed using PLS-SEM. Results showed that measurement scales achieved good reliability and convergent validity (Composite Reliability: 0.837–0.941; AVE > 0.5), and discriminant validity was confirmed through HTMT, except for the RC–CO pair reflecting conceptual similarity between security costs and convenience levels. The structural model revealed that Attitude toward security behavior (ATT) is the strongest determinant of Privacy Protection Behavioral Intention (BI) ($\beta = 0.713$; $p < 0.001$). Response Efficacy (RE) and Trust in the system (TR) both positively impact attitude, with RE having stronger influence. Perceived Risk (PR) strongly affects Privacy Concerns (PC), and Perceived Severity (SE) significantly impacts Perceived Vulnerability (PV). However, PC, PV, and Social Influence (SI) do not directly affect attitude. The study emphasizes that enhancing confidence in security measures' effectiveness and strengthening system trust are key to promoting positive attitudes and students' privacy protection intentions on E-learning platforms.

Keywords: *privacy protection, e-learning, protection motivation theory, student behavior, information security*

1. INTRODUCTION

Therapid expansion of E-learning systems within higher education has facilitated flexible, convenient, and accessible learning opportunities for students across diverse contexts, particularly in the aftermath of the COVID-19 pan demic, when online classes became common and firmly established [1]. However, the increased reliance on digital platforms has also precipitated escalating concerns regarding data security and students privacy. Numerous studies indicate that students frequently disclose personal information, academic data, and behavioral metrics, and even conduct critical transactions via E-learning platforms [2]; consequently, this renders them increasingly vulnerable to risks such as unauthorized data collection, behavioral tracking, and the leakage of sensitive information [3]. In this context, students' privacy-protective behaviors have emerged as a critical topic for higher education institutions, educational organizations, and platform developers [4]. Privacy is not merely a technical issue involving encryption, system security, or data policies; rather, it is a multifaceted psychological and behavioral matter, heavily predicated upon risk perception, privacy concerns, attitudes, and users' trust in the system [5]. Consequently, investigating individual security behaviors within online learning environments necessitates a robust theoretical framework to elucidate the underlying motivations of students. Rogers' (1975) Protection Motivation Theory (PMT) [6] represents one of the most widely utilized theoretical frame works for investigating security and privacy behaviors within digital environments. PMT suggests that an individual's

self-protective behavior is shaped through two distinct cognitive processes: threat appraisal (encompassing risk perception, perceived severity, and perceived vulnerability) and coping appraisal (comprising response efficacy, self-efficacy, as well as response cost and convenience) [7]. Within various cyber security contexts, PMT has demonstrated significant explanatory power regarding password hygiene, device protection, and the adoption of per sonal information security measures [8].

However, when applied to E-learning con texts, recent studies suggest that PMT requires extension to accurately capture the nuances of the online educational environment where students are faced not only with the risk of data exposure but also with system reliability, convenience, and the influence of the learning community [9]. Furthermore, while attitude is recognized as a pivotal mediating variable [10] bridging cognitive determinants and security behavioral intentions, it remains under-investigated within the framework of original PMT studies. Accordingly, numerous researches have proposed an extension of the PMT framework by integrating variables such as trust [11], privacy concerns, social influence, or the trade-off between security response cost and convenience, and have reported consistent results [12]. Nevertheless, comprehensive research within the E-learning landscape, specifically in developing nations like Vietnam, remains scarce. Discrepancies in technological infrastructure, students' digital literacy, the transparency of privacy policies, and platform usage habits may lead to divergent behavioral models. Addressing the gaps identified above, this study aims to model the factors influencing students' privacy protection behaviors within E-learning systems based on an extended PMT framework. The research objectives are as follows: (1) to examine the impact of cognitive, psychological, and social factors on privacy protection attitudes and intentions; (2) to propose a theoretical model more aligned with the specificities of online learning environments; and (3) to provide practical implications that help universities and E-learning providers understand how to enhance security awareness, bolster trust, and promote privacy protection behaviors among students. Theoretically, this study contributes to the extension of PMT within the domain of digital education. Practically, the results can support the design of privacy policies, the improvement of user interfaces, and the enhancement of information security in the implementation of E learning systems.

2. RESEARCH MODEL AND HYPOTHE-SES

2.1. Theoretical Framework

The research model is based on Rogers' (1975) Protection Motivation Theory (PMT) [6], which has been extensively utilized to elucidate security behaviors in online environments. According to PMT, an individual's protective behavior is determined by two cognitive appraisal processes: threat appraisal which include perceived severity (SE) and perceived vulnerability (PV); and coping appraisal, comprising of response efficacy (RE), self-efficacy (SEF), and response costs (RC), which represent the barriers to implementing protective measures [13]. Numerous studies have validated the efficacy of PMT in predicting information security behaviors and risk management within digital contexts [14], [15]. In addition to PMT, this study incorporates variables that reflect the specific characteristics of the E learning environment. Convenience (CO) may either facilitate or hinder the adoption of security measures, particularly in contexts where students prioritize a seamless learning experience [16]. Social Influence (SI), adapted from the UTAUT framework [17], represents the impact of peers, instructors, and the overall learning environment on personal information protection behavior.

2.2. Proposed Model

The research model is based on Rogers' (1975) Protection Motivation Theory (PMT) [6], recognized as a pivotal theoretical framework for elucidating security behaviors and risk management in digital environments. PMT suggests that protective behavioral intention arises from two cognitive mechanisms: (1) Threat Appraisal and (2) Coping Appraisal [13]. In this study, five main PMT variables are incorporated: Perceived Severity (SE), Perceived Vulnerability (PV), Response Efficacy (RE), Self-Efficacy (SEF), and Response Cost (RC). These factors have been empirically validated to significantly influence information security behaviors within the do mains of user security, system safety, and online privacy [14], [15]. Furthermore, the model is ex tended with structures that capture the nuances of the E-learning context and students' behavioral traits. Convenience (CO) accounts for the requirement of user experience optimization, acknowledging that security measures may sometimes be perceived as inconvenient interruptions to the learning process [16]. Lastly, Social In fluence (SI), adapted from the UTAUT model, reflects the influence of instructors, peers,

and the broader academic environment on security related behaviors [17]. Not only that, three ex tended privacy-related variables: Perceived Risk (PR), Privacy Concern (PC), and Trust (TR) are integrated to comprehensively reflect the factors influencing personal data protection behavior in online environments. Prior studies have indicated that risk perception and trust levels are significant predictors of security-related attitudes and behaviors [18], [19]. These factors influence Attitude toward security behavior (ATT)– a pivotal mediating variable in behavioral models such as the Theory of Planned Behavior (TPB) and UTAUT [20], [17]– shaping Privacy Protection Behavioral Intention (BI). Collectively, the research model extends PMT by incorporating privacy-related and E-learning usage constructs to establish a holistic framework for explaining students' intentions to safeguard personal data within online learning environments.

2.3. Research Hypotheses

Formulated on the extended PMT model and incorporating variables tailored to the privacy protection context of E-learning systems, this study proposes 14 hypotheses to examine the relationships between threat appraisal, coping appraisal, attitude, and students' behavioral intentions. These hypotheses are formulated according to PMT logic, wherein threat and coping appraisals are expected to influence attitude and trust, which in turn drive security behavioral intentions.

The proposed research hypotheses are as follows:

H1: Attitude (ATT) has a positive influence on Behavioral Intention (BI).

H2: Convenience (CO) has a positive in fluence on Trust (TR).

H3: Privacy Concern (PC) has a positive influence on Attitude (ATT).

H4: Perceived Risk (PR) has a positive in fluence on Privacy Concern (PC).

H5: Perceived Risk (PR) influences Trust (TR).

H6: Perceived Vulnerability (PV) has a positive influence on Attitude (ATT).

H7: Response Cost (RC) has a positive in fluence on Convenience (CO).

H8: Response Efficacy (RE) has a positive influence on Attitude (ATT).

H9: Response Efficacy (RE) has a positive influence on Self-Efficacy (SEF).

H10: Perceived Severity (SE) has a positive influence on Perceived Vulnerability (PV).

H11: Self-Efficacy (SEF) influences Perceived Vulnerability (PV).

H12: Social Influence (SI) has a positive influence on Attitude (ATT).

H13: Social Influence (SI) has a positive influence on Trust (TR).

H14: Trust (TR) has a positive influence on Attitude (ATT).

3. RESEARCH METHODOLOGY

3.1. Research Design

This study employs a quantitative research approach to examine the relationships among variables in the proposed research model. The research methodology follows a structured process: (1) literature review to establish the theoretical foundation and develop the extended PMT model; (2) questionnaire design and validation; (3) data collection from university students who actively use e-learning systems; (4) data analysis using Partial Least Squares Structural Equation Modeling (PLS-SEM); and (5) interpretation of findings and formulation of recommendations. The proposed research model is presented in Figure 1. The model extends the original PMT framework by incorporating privacy-related con structs (Perceived Risk, Privacy Concern, Trust) and e-learning specific variables (Convenience, Social Influence) to comprehensively capture the factors influencing students' privacy protection intentions in online learning environments.

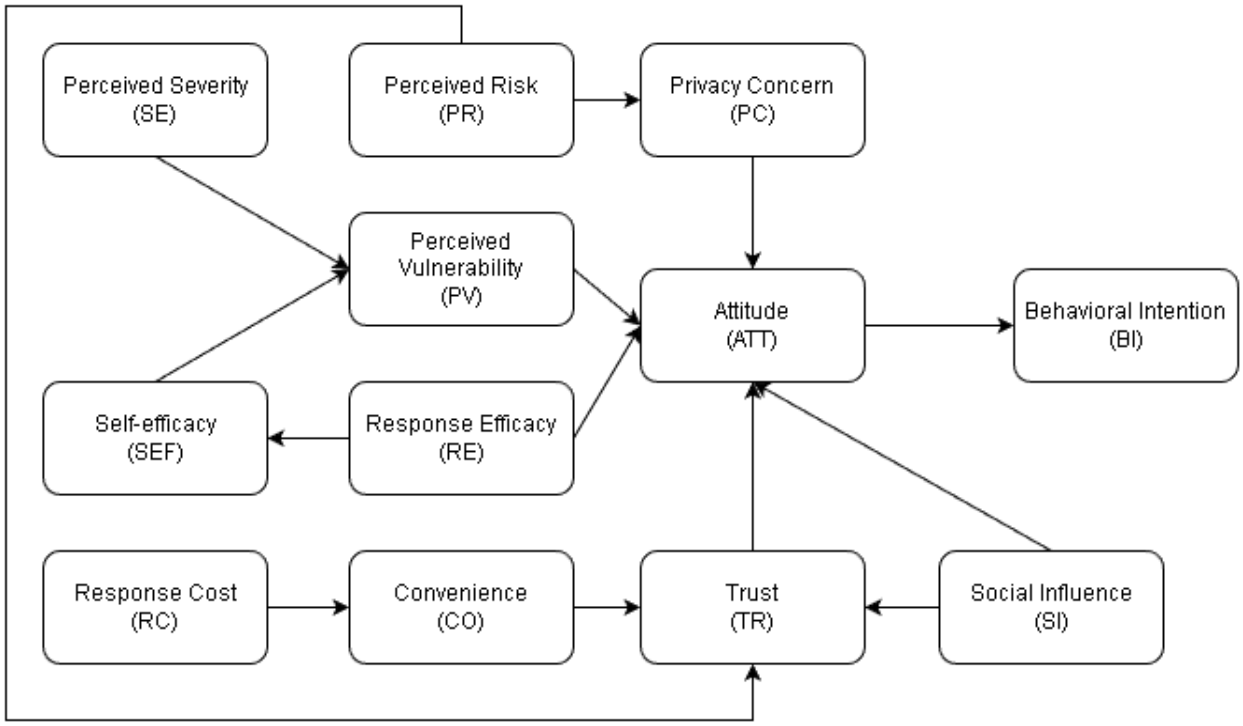

Figure 1. Extended PMT Research Model for E-Learning Privacy Protection

The quantitative approach is appropriate for this study as it allows for systematic testing of hypothesized relationships and enables generalization of findings across the target population [21]. PLS-SEM was selected as the primary analytical technique due to its capability to handle complex models with multiple constructs, its minimal restrictions on sample size and data distribution assumptions, and its suitability for exploratory research that aims to extend existing theories [22].

3.2. Data Collection

Data were collected through an online survey questionnaire distributed to university students in Vietnam who had experience using e-learning platforms. The survey was conducted over a period of four weeks, from December 2025 to January 2026. A convenience sampling approach was employed, targeting students from multiple universities who actively engaged with e learning systems for their coursework. The questionnaire consisted of three main sections: (1) screening questions to ensure respondents had relevant e-learning experience; (2) measurement items for all constructs in the research model; and (3) demographic information. All measurement items were adapted from validated scales in prior literature and modified to fit the e-learning privacy protection context. A five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) was used for all items. Prior to the main survey, a pilot test was conducted with 30 students to assess the clarity and comprehensibility of the questionnaire. Based on feedback from the pilot test, minor wording adjustments were made to improve item clarity. The final sur vey was distributed through online channels including email, social media groups, and learning management systems. A total of 158 valid responses were collected after removing incomplete or inconsistent responses.

3.3. Measurement Scales

All constructs in the research model were measured using multi-item scales adapted from established literature. The measurement scales for PMT constructs (Perceived Severity, Perceived Vulnerability, Response Efficacy, Self-Efficacy, and Response Cost) were adapted from prior PMT studies [23], [24]. Extended constructs including Perceived Risk, Privacy Concern, Trust, Convenience, and Social Influence were adapted from relevant privacy and technology acceptance studies [25], [26]. Attitude and Behavioral Intention scales were adapted from the Theory of Planned Behavior literature [27]. Each construct was measured using 3-5 items to ensure adequate content coverage while minimizing respondent fatigue. All items were carefully translated into Vietnamese and then back-translated to English to ensure semantic equivalence and cultural appropriateness. The Vietnamese version was used for data collection to ensure respondent comprehension.

3.4. Data Analysis Method

The collected data were analyzed using Smart PLS4.0 software following a two-stage approach recommended for PLS-SEM analysis [28]. The first stage involved assessment of the measurement model to evaluate reliability and validity of the constructs. The second stage involved assessment of the structural model to test the hypothesized relationships.

For the measurement model, the following criteria were evaluated: (1) internal consistency reliability using Cronbach's alpha and Composite Reliability (CR), with values above 0.70 considered acceptable [29]; (2) convergent validity assessed through Average Variance Extracted (AVE), with values above 0.50 indicating adequate convergence [30]; (3) indicator reliability examined through outer loadings, with values above 0.70 preferred; and (4) discriminant validity evaluated using the Heterotrait-Monotrait (HTMT)ratio, with values below 0.85 indicating adequate discriminant validity [31].

For the structural model, the following aspects were evaluated: (1) path coefficients and their statistical significance using bootstrapping with 5,000 resamples; (2) coefficient of determination (R^2) values to assess the explanatory power of the model; (3) effect sizes (f^2) to evaluate the relative impact of predictor constructs; and (4) predictive relevance (Q^2) using blindfolding procedures. The significance level was set at $p < 0.05$ for all hypothesis tests.

Prior to hypothesis testing, the data were screened for missing values, outliers, and response patterns. No significant issues were identified that would compromise the validity of the analysis. Common method bias was assessed using Harman's single-factor test, which revealed that no single factor accounted for more than 50% of the variance, suggesting that common method bias was not a significant concern in this study [32]. Additionally, the variance inflation factor (VIF) values for all constructs were below 3.0, indicating no severe multicollinearity issues among the predictor variables [33].

4. RESULTS

4.1. Sample Characteristics

The final sample consisted of 158 respondents. Table 1 presents the demographic profile of the participants.

Table 1. Demographic profile of repondents (n=158)

Characteristic	Frequency	Percentage (%)
Gender		
male	75	47.5
female	83	52.5
Age		
18-22 years	124	78.5
23-25 years	28	17.7
Above 25 years	6	3.8
Academic Year		
Second year	72	45.6
Third year	52	32.9
Fourth year	34	21.5

Beyond demographic characteristics, the survey examined students' e-learning usage pat terns and password security practices. Figure 2 illustrates the frequency of e-learning system usage, revealing that 55.8% of respondents accessed e-learning platforms only when necessary for assignments or tests, 31.3% used them 2-3 times per week for regular study activities, and 12.9% were daily users. This usage pattern suggests that while e-learning has become an integral part of students' academic lives, the majority still adopt a task-oriented approach to platform engagement.

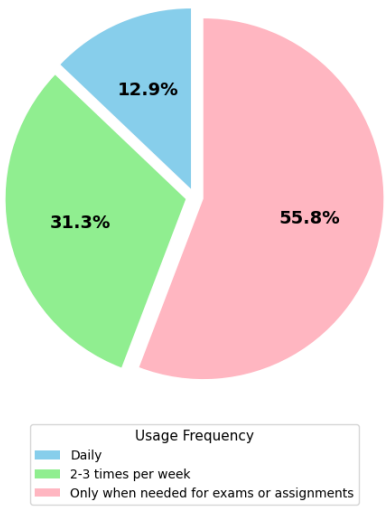

Figure 2. Frequency of e-learning system usage

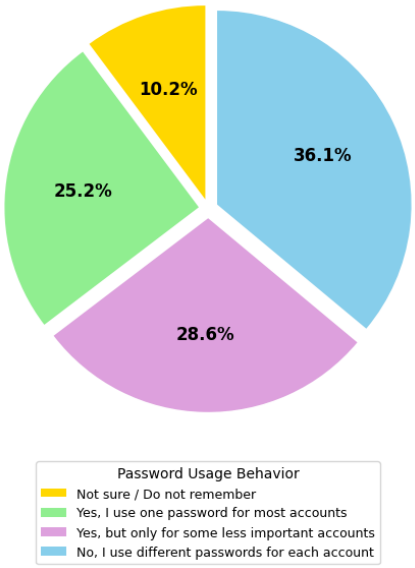

Figure 3. Password reuse patterns

Figure 3 presents password management practices among respondents, revealing significant security vulnerabilities. The analysis shows that 36.1% of students reported never remembering or not knowing whether they reuse pass words across platforms, indicating low pass word awareness. Another 28.6% acknowledged having a few identical or very similar pass words for most accounts, while 25.2% admit ted to not using the same password but selecting similar passwords across different plat forms. Only 10.2%ofrespondents reported using completely unique passwords for each account. These concerning patterns highlight the prevalence of weak password hygiene practices, which pose substantial risks to personal data security. Taken together, approximately 64.7% of respondents demonstrate insecure password behaviors through password reuse or highly similar credentials across platforms, indicating suboptimal security practices among students and emphasizing the need to strengthen cybersecurity awareness and promote safer password management within E-learning environments.

4.2. Measurement model evaluation

The measurement model was evaluated based on a set of reliability and validity criteria to ensure the psychometric robustness of the constructs prior to the structural model analysis. As mentioned in Table 2, the assessment focused on examining factor loadings, composite reliability, and convergent validity of the variables within the extended PMT framework

Table 2. Measurement model evaluation result

Construct / Indicators		**CR**	**AVE**	**α**	**FL**
Perceived Severity (SE)		**0.8078**	**0.5997**	**0.6196**	
SE1	If my personal data is leaked on E-learning, the impact could be severe.				0.8879
SE2	Information leakage will have a negative impact on me.				0.8885
SE3	I do not believe that the disclosure of personal data on E-learning is a serious issue.				**0.4705**
Perceived Vulnerability (PV)		**0.8136**	**0.5997**	**0.6512**	
PV1	I feel that my E-learning account is at risk of unauthorized access.				0.8659
PV2	I believe I could be a target of security risks.				0.8454
PV3	I do not think my E-learning account is likely to be attacked.				**0.5784**
Response Efficacy (RE)		**0.7819**	**0.5623**	**0.5731**	
RE1	Security measures help protect my privacy.				0.8869
RE2	Using strong passwords reduces the risk of being attacked.				0.8381
RE3	Security measures do not contribute significantly to protecting my data.				**0.4449**
Self-efficacy (SEF)		**0.8593**	**0.6710**	**0.7548**	
SEF1	I am confident in modifying security settings as necessary.				0.8596
SEF2	I am capable of detecting unusual activities on my account.				0.8272
SEF3	I possess sufficient skills to protect my personal information.				0.7680
Response Cost (RC)		**0.8465**	**0.6478**	**0.7286**	
RC1	Changing passwords frequently is time-consuming.				0.7843
RC2	Additional authentication steps cause inconvenience during login.				0.8287
RC3	Security measures require extra effort on my part.				0.8010
Convenience (CO)		**0.8681**	**0.6884**	**0.7704**	
CO1	I prefer E-learning usage to be rapid and straightforward.				0.7326
CO2	I feel that security procedures hinder my learning process.				0.8818
CO3	Multi-step verification processes cause disruptions.				0.8665
Social Influence (SI)		**0.8369**	**0.6319**	**0.7073**	

SI1	The university encourages students to protect their E-learning accounts.				0.8479
SI2	Instructors frequently remind me about security issues.				0.7914
SI3	I observe that people around me are indifferent to information security.				0.7418
Trust (TR)		**0.7982**	**0.5847**	**0.6030**	
TR1	I trust the university's E-learning system to protect my personal information.				0.9001
TR2	I believe the university has clear policies regarding privacy protection.				0.8503
TR3	I doubt that the university prioritizes the protection of students' personal data.				**0.4699**
Perceived Risk (PR)		**0.9178**	**0.7884**	**0.8657**	
PR1	I believe using E-learning carries potential privacy risks.				0.9011
PR2	I am concerned that academic data (assignments, grades) could be disclosed or misused.				0.8735
PR3	I think there is a possibility that my information could be accessed without authorization due to system vulnerabilities.				0.8888
Privacy Concern (PC)		**0.8447**	**0.5885**	**0.7479**	
PC1	I am concerned that my personal data on E-learning could be used for improper purposes.				0.8712
PC2	I feel uncomfortable when the E-learning system collects extensive information from me.				0.7945
PC3	I am worried that the university or the system could share my data with third parties.				0.8678
PC4	I am not overly concerned about my privacy when using E-learning.				**0.4589**
Attitude (ATT)		**0.8265**	**0.5809**	**0.6885**	
ATT1	I believe that protecting personal data is essential.				0.8674
ATT2	I find that implementing information security measures is beneficial to me.				0.8915
ATT3	I consider securing my account to be a positive habit.				0.8550
ATT4	I feel that protecting personal information is bothersome and relatively unimportant.				**0.2126**
Behavioral Intention (BI)		**0.8785**	**0.6441**	**0.8166**	
BI1	I intend to enhance my account security in the near future.				0.8349
BI2	I plan to change my password periodically.				0.7904
BI3	I intend to avoid using the same password for multiple accounts.				0.7737
BI4	I am willing to adopt the security measures recommended by the university.				0.8100
Note: FL = Factor loadings, CR = Composite reliability, AVE = Average variance extracted, α = Cronbach's alpha.					

The initial assessment of the measurement model indicated an overall acceptable level of fit; however, several indicators exhibited low outer loadings that necessitated refinement. In terms of internal consistency reliability, most constructs achieved Cronbach's α values ranging from ap proximately 0.65 to over 0.86, either exceeding or closely approaching the recommended thresh old of 0.7, thereby suggesting general consistency across the scales. The Composite Reliability (CR) for all structures surpassed the 0.78 threshold while the majority exceeded 0.84, con firming robust composite reliability. Addition ally, the AVE values fluctuated between 0.56 and 0.79, mostly surpassing 0.5, which demonstrates that the convergent validity of the scales is satisfactory.

Nevertheless, the results for outer loadings indicated that several indicators did not meet the 0.7 threshold, thereby impacting the model's convergent quality. Indicators such as ATT4 (0.2126), PC4 (0.4589), PV3 (0.5784), RE3 (0.4449), SE3 (0.4705), and TR3 (0.4699) all exhibited low loadings and significant deviations relative to the remaining items within their respective constructs. These indicators di minished the AVE and CR values of the associated variables and demonstrated a limited contribution to the conceptual measurement. Conversely, the majority of the remaining items dis played strong factor loadings, ranging from ap proximately 0.73 to over 0.89, reflecting a robust relationship between the observed variables and their latent constructs.

In general, while the initial measurement model achieved acceptable levels of reliability and convergent validity, the prevalence of indica tors with low outer loadings suggested the necessity of model refinement through the

exclusion of items failing to meet the required threshold.

The results of the discriminant validity assessment using the HTMT ratio indicate that most construct pairs within the model reached an acceptable level, with the majority of HTMT values falling below the recommended threshold of 0.85–0.90. Constructs such as ATT–CO, PV–PC, RE–PC, and TR–PC exhibited low-to-moderate correlations (HTMT ranging from 0.28 to 0.70), confirming their status as distinct and independent concepts. However, the model identified several pairs with relatively high correlations, specifically RC–CO (0.990) and PC–PR (0.923). Despite slightly exceeding the standard thresh olds, these relationships remain theoretically justifiable, as concepts pertaining to inconvenience and required effort (RC–CO) or privacy concerns and perceived risk (PC–PR) possess an inherent and strong conceptual linkage within privacy protective behavior. Concurrently, the remaining constructs maintained clear distinctiveness, and prior reliability and convergent validity tests were satisfactory, suggesting that the model over all demonstrates adequate discriminant validity and is sufficiently robust for subsequent structural model analysis.

4.3. Structural Model Assessment

Following the confirmation that the measurement model's properties are suitable, the structural model was evaluated to test the hypothesized relationships among the constructs within the extended PMT theoretical framework. The structural model analysis focuses on examining path coefficients, statistical significance levels, and the model's explanatory power, thereby vali dating the proposed theoretical relationships and elucidating the factors that influence students' privacy-protective behaviors when utilizing E learning systems. Detailed results are presented in Table 3.

The structural model assessment result in table 4 reveals that only a subset of the hypotheses within the extended PMT framework were supported. Notably, Attitude (ATT) continues to play a central role, exerting a substantial impact on Privacy Protection Behavioral Intention (BI)

Table 3. HTMT Correlation matrix (Discriminant Validity Assessment)

	ATT	**BI**	**CO**	**PC**	**PR**	**PV**	**RC**	**RE**	**SE**	**SEF**	**SI**
ATT											
BI	0.838										
CO	0.516	0.600									
PC	0.528	0.617	0.783								
PR	0.526	0.627	0.791	**0.923**							
PV	0.546	0.593	0.698	0.613	0.668						
RC	0.483	0.548	**0.990**	0.762	0.703	0.667					
RE	0.834	0.713	0.699	0.481	0.547	0.564	0.558				
SE	0.703	0.542	0.597	0.494	0.463	0.709	0.483	0.712			
SEF	0.667	0.820	0.616	0.532	0.560	0.457	0.632	0.745	0.481		
SI	0.737	0.804	0.707	0.654	0.648	0.670	0.560	0.783	0.706	0.698	
TR	0.628	0.701	0.429	0.401	0.446	0.287	0.361	0.592	0.439	0.618	**0.870**

Note: HTMT = Heterotrait-Monotrait Ratio. Values < 0.85 are considered satisfactory for establishing discriminant validity. Although the HTMT ratios for the RC–CO (0.990) and PR–PC (0.923) pairs exceeded this threshold, they remain theoretically justifiable: the RC–CO pair reflects the inherent conceptual overlap between response cost and convenience, while the PR–PC pair represents the strong theoretical link between perceived risk and privacy concerns.

Table 4. Structural Model Assessment Result

Theory	**Relationship**	**β**	**t-value**	**p-value**	**Result**
H1	ATT → BI	0.713	11.255	0.000	Accept
H2	CO → TR	-0.067	0.718	0.473	Reject
H3	PC → ATT	0.118	1.469	0.142	Reject
H4	PR → PC	0.782	16.988	0.000	Accept
H5	PR → TR	0.089	0.856	0.392	Reject
H6	PV → ATT	0.113	1.336	0.182	Reject
H7	RC → CO	0.749	16.284	0.000	Accept
H8	RE → ATT	0.447	5.327	0.000	Accept
H9	RE → SEF	0.585	8.212	0.000	Accept
H10	SE → PV	0.530	6.594	0.000	Accept

H11	SEF → PV	0.136	1.668	0.095	Reject
H12	SI → ATT	0.055	0.553	0.580	Reject
H13	SI → TR	0.657	7.349	0.000	Accept
H14	TR → ATT	0.220	2.559	0.011	Accept

Note: β denotes the path coefficient; t-value and p-value are used to determine the level of statistical significance for each hypothesis.

With a high coefficient (β=0.713;p=0.000). This confirms that students only genuinely intend to engage in security behaviors — such as creating strong passwords, changing passwords periodically, or enhancing personal information protection — when they maintain a positive attitude toward these actions. These findings are consistent with prior research on online security behavior, indicating that attitude is the most potent predictor of intention.

Two factors significantly influence security attitude: Response Efficacy (RE) and student Trust (TR) in the E-learning system. Both relationships were supported with high statistical significance (RE→ATT: β = 0.447; p = 0.000; TR→ATT: β = 0.220; p = 0.011). This suggests that when students believe protective measures (e.g., two-factor authentication, password updates, security alerts) are effective and when they trust the university's E-learning platform, their attitude toward privacy protection becomes more positive. Conversely, factors such as Privacy Concern(PC), Perceived Vulnerability (PV), and Social Influence (SI)were found to have no direct impact on attitude. Nonetheless, cognitive mechanisms still play an indirect role:

Perceived Risk (PR) strongly influences PC (β = 0.782; p = 0.000), Perceived Severity(SE) impacts PV (β = 0.530; p = 0.000), and RE continues to bolster students' Self-Efficacy(SEF).

Regarding Trust (TR), Social Influence (SI) emerged as the sole factor with a significant impact (β = 0.657; p = 0.000). This indicates that students' trust in the E-learning system is reinforced when they receive security recommendations from professors, peers, or the university. Conversely, perceived convenience (CO) and perceived risk (PR) do not exert a significant influence on TR.

Simultaneously, Response Cost (RC) has a very strong influence on Convenience (CO) (β = 0.749; p = 0.000), reflecting that complex and time-consuming security measures can diminish the perceived ease of use within the E-learning environment. Overall, the model demonstrates that security attitude and trust in the system are the two core determinants driving students' information privacy protection intentions, while perceived risk and cost factors primarily play an indirect role in shaping password security behaviors and account protection practices on E learning platforms.

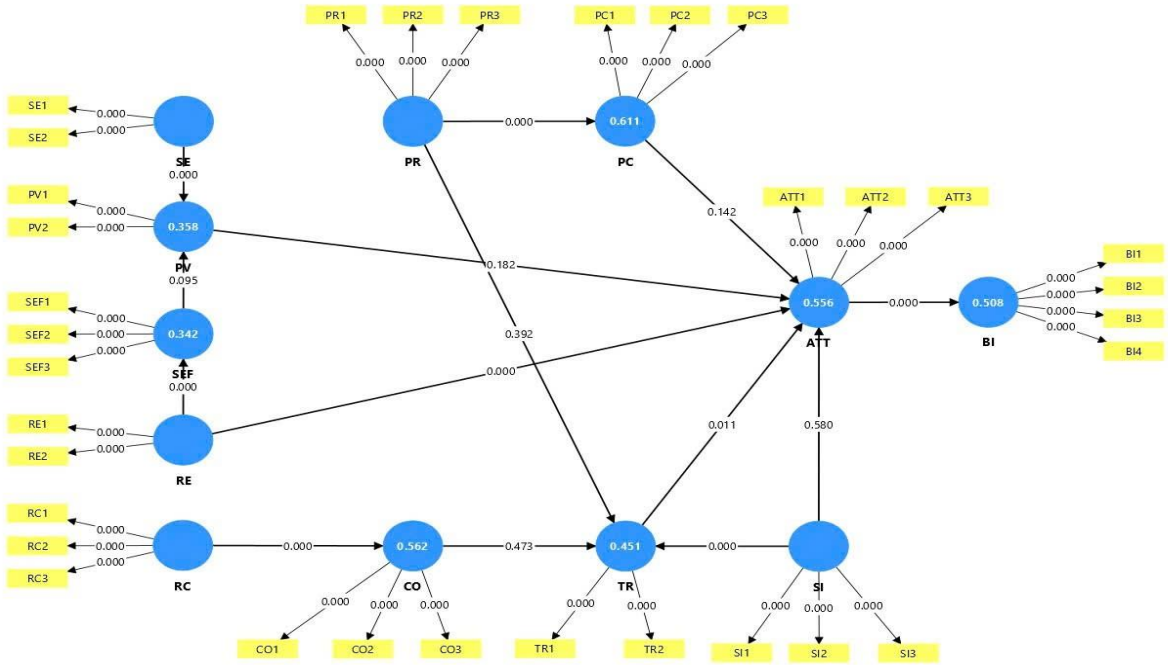

Figure 4. Structural Model Results and Measurement Coefficients

5. CONCLUSION

The findings of this study make a significant contribution to the field of security behavior in E-learning environments by elucidating the factors that shape students' privacy protection intentions through the lens of an ex tended PMT model. The most prominent finding indicates that Attitude toward security behavior is the strongest predictor of the intention to enhance personal information protection, emphasizing that students only proactively employ strong passwords or adopt security measures when they believe such actions are truly beneficial and necessary. Additionally, the study confirms the pivotal role of Response Efficacy and Trust in the E-learning system in fostering positive attitudes, whereas traditional risk perception factors predominantly influence intentions indirectly through threat appraisal mechanisms.

These results suggest that investing in user-friendly, effective security measures combined with increased communication and recommendations from instructors and the university will have a practical impact on bolstering trust and reducing student indifference toward information safety. Given the context where many students still reuse passwords or only access the system when mandatory, the study suggests that E-learning management strategies should focus on: (1) strengthening trust through communication initiatives and social influence; (2) raising awareness regarding the efficacy of security measures; and (3) optimizing the security experience to mitigate perceived costs and inconvenience. These results pave the way for future research into long-term security behaviors, the evolution of password habits over time, and the impact of advanced security mechanisms (such as MFA or intelligent security alerts) on learner attitudes and intentions within the modern E learning ecosystem.

DECLARATION OF CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] D. Turnbull, R. Chugh, and J. Luck, "Transitioning to E-learning during the COVID-19 pandemic: How have higher education institutions responded to the challenge?," Educ. Inf. Technol., vol. 26, no. 5, pp. 6401-6419, Jun. 2021, doi: 10.1007/s10639-021-10633-w

[2] B. Chang, "Student privacy issues in online learning environments," Distance Educ., vol. 42, no. 1, pp. 55-69, Jan. 2021, doi: 10.1080/01587919.2020.1869527

[3] K. El-Khatib, L. Korba, Y. Xu, and G. Yee, "Privacy and security in E-learning," Int. J. Distance Educ. Technol., vol. 1, no. 4, pp. 1-19, Oct. 2003, doi: 10.4018/jdet.2003100101

[4] M. Alier, M. J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca, "Privacy and e-learning: A pending task," Sustainability, vol. 13, no. 16, art. no. 9206, Aug. 2021, doi: 10.3390/su13169206

[5] S. Kokolakis, "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," Comput. Secur., vol. 64, pp. 122-134, Jan. 2017, doi: 10.1016/j.cose.2015.07.002

[6] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," J. Psychol., vol. 91, no. 1, pp. 93-114, Sep. 1975, doi: 10.1080/00223980.1975.9915803

[7] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A meta-analysis of research on protection motivation theory," J. Appl. Soc. Psychol., vol. 30, no. 2, pp. 407-429, Feb. 2000, doi: 10.1111/j.1559-1816.2000.tb02323.x

[8] A. Almansoori, M. Al-Emran, and K. Shaalan, "Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories," Appl. Sci., vol. 13, no. 9, art. no. 5700, May 2023, doi: 10.3390/app13095700

[9] M. Anwar, "Supporting privacy, trust, and personalization in online learning," Int. J. Artif. Intell. Educ., vol. 31, no. 4, pp. 769-783, Sep. 2021, doi: 10.1007/s40593-020-00216-0

[10] M. Siponen, M. Rönkkö, F. Li, S. Haag, and G. Laatikainen, "Protection motivation theory in information security behavior research: Reconsidering the fundamentals," Commun. Assoc. Inf. Sist., vol. 53, art. no. 43, pp. 1136-1165, 2024, doi: 10.17705/1CAIS.05348

[11] H. T. Nguyen and C. W. Tang, "Students' intention to take E-learning courses during the COVID-19 pandemic: A protection motivation theory perspective," Int. Rev. Res. Open Distance Learn., vol. 23, no. 3, pp. 21-42, Sep. 2022

[12] M. Mousavizadeh and D. J. Kim, "A study of the effect of privacy assurance mechanisms on self-disclosure in social networking sites from the view of protection motivation theory," in Proc. Int. Conf. Inf. Syst., Fort Worth, TX, USA, Dec. 2015, pp. 1-18.

[13] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," J. Exp. Soc. Psychol., vol. 19, no. 5, pp. 469-

479, Sep. 1983, doi: 10.1016/0022-1031(83)90023-9
[14] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," Comput. Secur., vol. 31, no. 1, pp. 83-95, Feb. 2012, doi: 10.1016/j.cose.2011.10.007
[15] A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," MIS Quart., vol. 34, no. 3, pp. 549-566, Sep. 2010, doi: 10.2307/25750691
[16] I. Kirlappos and M. A. Sasse, "Security education against phishing: A modest proposal for a major rethink," IEEE Security Privacy, vol. 10, no. 2, pp. 24-32, Mar./Apr. 2012, doi: 10.1109/MSP.2011.179
[17] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quart., vol. 27, no. 3, pp. 425-478, Sep. 2003, doi: 10.2307/30036540
[18] P. A. Pavlou, "Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model," Int. J. Electron. Commerce, vol. 7, no. 3, pp. 101-134, Spring 2003, doi: 10.1080/10864415.2003.11044275
[19] T. Dinev and P. Hart, "An extended privacy calculus model for E-commerce transactions," Inf. Syst. Res., vol. 17, no. 1, pp. 61-80, Mar. 2006, doi: 10.1287/isre.1060.0080
[20] I. Ajzen, "The theory of planned behavior," Organ. Behav. Hum. Decis. Process., vol. 50, no. 2, pp. 179-211, Dec. 1991, doi: 10.1016/0749-5978(91)90020-T
[21] A. Pinsonneault and K. L. Kraemer, "Survey research methodology in management information systems: An assessment," J. Manage. Inf. Syst., vol. 10, no. 2, pp. 75-105, Fall 1993, doi: 10.1080/07421222.1993.11518001
[22] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, "When to use and how to report the results of PLS-SEM," Eur. Bus. Rev., vol. 31, no. 1, pp. 2-24, Jan. 2019, doi: 10.1108/EBR-11-2018-0203
[23] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory," Inf. Manage., vol. 49, no. 3-4, pp. 190-198, May 2012, doi: 10.1016/j.im.2012.04.002
[24] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," Eur. J. Inf. Syst., vol. 18, no. 2, pp. 106-125, Apr. 2009, doi: 10.1057/ejis.2009.6
[25] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model," Inf. Syst. Res., vol. 15, no. 4, pp. 336-355, Dec. 2004, doi: 10.1287/isre.1040.0032
[26] D. Gefen, E. Karahanna, and D. W. Straub, "Trust and TAM in online shopping: An integrated model," MIS Quart., vol. 27, no. 1, pp. 51-90, Mar. 2003, doi: 10.2307/30036519
[27] S. Taylor and P. A. Todd, "Understanding information technology usage: A test of competing models," Inf. Syst. Res., vol. 6, no. 2, pp. 144-176, Jun. 1995, doi: 10.1287/isre.6.2.144
[28] J. F. Hair, G. T. M. Hult, C. M. Ringle, and M. Sarstedt, A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM), 3rd ed. Thousand Oaks, CA, USA: Sage, 2022.
[29] R. P. Bagozzi and Y. Yi, "On the evaluation of structural equation models," J. Acad. Mark. Sci., vol. 16, no. 1, pp. 74-94, Mar. 1988, doi: 10.1007/BF02723327
[30] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," J. Market. Res., vol. 18, no. 1, pp. 39-50, Feb. 1981,
[31] J. Henseler, C. M. Ringle, and M. Sarstedt, "A new criterion for assessing discriminant validity in variance-based structural equation modeling," J. Acad. Mark. Sci., vol. 43, no. 1, pp. 115-135, Jan. 2015, doi: 10.1007/s11747-014-0403-8
[32] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff, "Common method biases in behavioral research: A critical review of the literature and recommended remedies," J. Appl. Psychol., vol. 88, no. 5, pp. 879-903, Oct. 2003, doi: 10.1037/0021-9010.88.5.879
[33] N. Kock, "Common method bias in PLS-SEM: A full collinearity assessment approach," Int. J. e-Collaboration, vol. 11, no. 4, pp. 1-10, Oct./Dec. 2015, doi: 10.4018/ijec.2015100101

Các nhân tố ảnh hưởng hành vi bảo vệ quyền riêng tư trong E-learning theo Thuyết động lực bảo vệ mở rộng

Lê Nhật Tùng[1,*], Huỳnh Thái Linh[2], Hồ Gia Thành[2], Trương Minh Khoa[2]

[1]Trường Đại học Công nghệ Đồng Nai, Đồng Nai, Việt Nam
[2]Trường Đại học Công nghệ TP. Hồ Chí Minh, TP. Hồ Chí Minh, Việt Nam

**Tác giả liên hệ chính. Email: lenhattung@dntu.edu.vn*

Ngày nhận bài: dd/mm/yyyy; Ngày sửa bài: dd/mm/yyyy;
Ngày nhận đăng: dd/mm/yyyy; Ngày xuất bản: dd/mm/yyyy

TÓM TẮT

Bảo vệ quyền riêng tư trên hệ thống E-learning ngày càng quan trọng khi sinh viên phải chia sẻ nhiều thông tin cá nhân trong học trực tuyến. Nghiên cứu này áp dụng lý thuyết Động lực Bảo vệ mở rộng (Extended PMT) để mô hình hóa các yếu tố ảnh hưởng đến hành vi bảo vệ quyền riêng tư của sinh viên. Dữ liệu từ 158 sinh viên được phân tích bằng PLS-SEM. Kết quả cho thấy các thang đo đạt độ tin cậy và giá trị hội tụ tốt (Composite Reliability: 0.837–0.941; AVE > 0.5), giá trị phân biệt được xác nhận qua HTMT, ngoại trừ cặp RC–CO phản ánh sự tương đồng về chi phí bảo mật và mức độ thuận tiện. Mô hình cấu trúc chỉ ra Thái độ (ATT) là yếu tố quyết định mạnh nhất đến Ý định bảo vệ quyền riêng tư (BI) ($\beta = 0.713$; $p < 0.001$). Hiệu quả biện pháp bảo mật (RE) và Sự tin cậy hệ thống (TR) đều tác động tích cực đến thái độ, với RE có ảnh hưởng mạnh hơn. Nhận thức rủi ro (PR) ảnh hưởng mạnh đến Mối quan ngại quyền riêng tư (PC), và Mức độ nghiêm trọng (SE) tác động đáng kể đến Nhận thức khả năng bị đe dọa (PV). Tuy nhiên, PC, PV và Ảnh hưởng xã hội (SI) không ảnh hưởng trực tiếp đến thái độ. Nghiên cứu nhấn mạnh việc nâng cao niềm tin vào hiệu quả biện pháp bảo mật và tăng cường sự tin cậy hệ thống là chìa khóa thúc đẩy thái độ tích cực và ý định bảo vệ quyền riêng tư của sinh viên trên E-learning.

Từ khóa: *Bảo vệ quyền riêng tư, E-learning, lý thuyết PMT mở rộng, PLS-SEM, an toàn thông tin*