International Journal of Safety and Security Engineering
Vol. 15, No. 9, September, 2025, pp. 1971-1981
Journal homepage: http://iieta.org/journals/ijsse

Evaluating AI-Based Learning Platform to Increase Cybersecurity Awareness: Case Study of Indonesian Students

Puspita Kencana Sari[1*], Hasiva Amalia Dewi[1], Candiwan Candiwan[1], Puspita Wulansari[1], Achmad Nizar Hidayanto[2], Shinta Oktaviana[3], Hariandi Maulid[1]

[1] School of Economic and Business, Telkom University, Bandung 40257, Indonesia
[2] Faculty of Computer Science, University of Indonesia, Depok 16424, Indonesia
[3] Faculty of Information Technology, Nusa Mandiri University, Jakarta 13620, Indonesia

Corresponding Author Email: puspitakencana@telkomuniversity.ac.id

https://doi.org/10.18280/ijsse.150920

Received: 14 August 2025
Revised: 14 September 2025
Accepted: 24 September 2025
Available online: 30 September 2025

Keywords:
cybersecurity, AI-based learning platform, PMT, SDT, TAM

ABSTRACT

In the digital age, cybersecurity threats to educational institutions are increasing. The increasing number of academics and students falling victim to phishing attacks highlights the severity of the issue. This research investigates the impact of Artificial Intelligence (AI)-based learning platforms on cybersecurity awareness, revealing a focus on threat detection rather than education. Some constructs from Protection Motivation Theory (PMT), Self-Determination Theory (SDT), and Technology Acceptance Model (TAM) were examined to understand the factors that influence intention to use and cybersecurity awareness. This study involved 212 students at a private university in Indonesia to learn cybersecurity topics and take an assessment on an AI-based learning platform. The students then filled out questionnaires to measure their perceptions of those factors. The results showed that perceived severity (PS) and intention to use significantly impact cybersecurity awareness, with intention to use playing a key role in enhancing awareness. Perceived autonomy and usefulness also significantly influence students' intention to use. Furthermore, AI demonstrably increases students' cybersecurity awareness. These findings support AI-based cybersecurity education through personalized, interactive tools and provide valuable insights for improving awareness programs.

1. INTRODUCTION

Cybersecurity threats are growing in complexity and pose significant risks to individuals, organizations, and academic institutions [1]. Educational institutions offer a vast repository of valuable data—student records, research, and financial information—that is highly attractive to cybercriminals. In this sense, data is like gold to cybercrooks, and universities resemble a modern-day Fort Knox [2]. Among the most vulnerable groups within these institutions are university students, who, due to their frequent internet use and limited awareness of cybersecurity best practices, are often easy targets. Studies have shown that students frequently fall victim to phishing, malware, ransomware, cyberbullying, and cyberstalking, with over 20% of faculty and 25% of students reportedly targeted by phishing attacks [3, 4].

Artificial Intelligence (AI) technologies have gained attention in education [5]. AI helps prepare learning materials that align with learning styles, making learning more personalized [6, 7]. In the learning process, AI is used in the learning assessment [7, 8]. The learning process becomes more adaptive so that the learning goals are more personal [9]. Recent efforts explore how AI can be leveraged in cybersecurity education to raise awareness and preparedness [10, 11]. However, current research primarily focuses on AI's technical ability to detect cyber threats, leaving a gap in understanding how students perceive and adopt AI-based cybersecurity learning tools [12].

This study aims to address this gap by developing an integrative theoretical perspective that explains how threat perception, intrinsic motivation, and technology evaluation jointly influence students' intention to use AI-based learning platforms and their cybersecurity awareness outcomes. By combining Protection Motivation Theory (PMT), Self-Determination Theory (SDT), and the Technology Acceptance Model (TAM), this study goes beyond single-theory applications and conceptualizes a multi-layered mechanism in which PMT captures threat cognition, SDT explains motivational processes, and TAM operationalizes technology acceptance. Specifically, the model examines the roles of perceived vulnerability (PV), perceived severity (PS), perceived response efficacy (PRE), perceived self-efficacy (PSE), autonomy, competence, relatedness, and perceived usefulness.

This study occupied Quizalize as an AI-based learning platform, including features such as personalized feedback, real-time hints, and adaptive learning content. These capabilities enable students to independently explore cybersecurity concepts, learn from their mistakes, and receive tailored support, making the platform more responsive to individual learning styles and needs.

Focusing on students from a private university in Indonesia, this research does not evaluate the technical performance of the AI platform, but rather aims to provide insights for educators, developers, and policymakers to design more effective, engaging, and user-friendly cybersecurity training tools.

2. THEORETICAL THEORY AND HYPOTHESIS

PMT is a way of explaining how people react to perceived threats and what makes them want to protect themselves [13]. According to PMT, individuals are more likely to engage in protective actions when they perceive the threat to be significant and believe that their actions will effectively reduce the threat [14]. The theory identifies four main components that influence protective behavior: PV, PS, PRE, and PSE [15].

In the context of cybersecurity awareness, PMT provides a useful lens for understanding students' intention to use AI-based learning platforms designed to measure and enhance cybersecurity awareness through training [16]. PV refers to the extent to which students believe they are vulnerable to cyber threats, while PS reflects their assessment of the potential consequences of such threats. PRE captures students' belief in the effectiveness of AI-based platforms in reducing cybersecurity risks through training, and PSE represents their confidence in their ability to use such platforms effectively to improve their cybersecurity awareness [16].

Previous empirical studies show that PMT is effective in predicting cybersecurity behavior. For example, Alneyadi and Normalini [17] found that the variables PV, PS, PRE, and PSE all had a statistically significant and positive influence on the intention to use AI-based. While their study focused on behavioral intention, these PMT constructs are also foundational to cybersecurity awareness (CSA), as awareness is a precursor to action [13]. Supporting this, a study confirmed [18] that PV, PS, PRE, and PSE significantly enhance cybersecurity awareness, particularly in organizational settings. Similarly, Almansoori et al. [19] demonstrated that PV and PSE directly influence cybersecurity practices. Based on these findings, the following hypotheses are proposed:

H1: PV has a positive impact on CSA.

H2: PS has a positive impact on CSA.

H3: PRE has a positive impact on CSA.

H4: PSE has a positive impact on CSA.

SDT is a psychological theory stating that human motivation depends on fulfilling three core needs: autonomy (control over actions), competence (mastering skills), and relatedness (meaningful connections) [20]. Autonomy refers to having control and the freedom to make one's own choices, competence signifies confidence in one's ability to complete tasks successfully, and relatedness pertains to the sense of connection with others [21]. In the context of technology adoption, SDT suggests that users are more likely to engage with a platform when it meets these psychological needs [22, 23].

In the context of AI-based learning, the integration of intelligent features such as real-time adaptive feedback aligns directly with the three pillars of SDT [24]. Autonomy is fostered through personalized content selection. Competence is enhanced by instant feedback that reinforces learning, helping users understand and retain cybersecurity concepts. Relatedness is supported when users perceive emotional resonance and personal relevance in the learning content [25].

For the AI-based cybersecurity training platform, SDT provides insight into how students' intrinsic intention to use the platform is influenced by their perceptions of autonomy, competence, and relatedness. Research has shown that meeting these psychological needs increases user engagement and technology adoption [26]. For example, a previous study found that PAUT, PCOMP, and PREL significantly influence self-determined motivation in cybersecurity training [27]. When individuals feel competent in acquiring cybersecurity knowledge, have control over their learning process, and develop an emotional connection to the subject, their motivation to learn increases. These factors enhance engagement and commitment, ultimately leading to better learning outcomes [27]. Based on SDT, the following hypotheses are proposed:

H5: Perceived autonomy (PAUT) has a positive influence on the intention to use (IU) an AI-based learning platform for cybersecurity awareness.

H6: Perceived competency (PCOMP) has a positive influence on the intention to use an (IU) AI-based learning platform for cybersecurity awareness.

H7: Perceived relatedness (PREL) has a positive influence on the intention to use (IU) an AI-based learning platform for cybersecurity awareness.

TAM is a well-established framework that explains technology adoption through two key factors: perceived usefulness and perceived ease of use [28, 29]. While TAM traditionally considers both factors, this study focuses specifically on perceived usefulness (PU) as it directly reflects students' belief that the AI-based learning platform will effectively measure and enhance their cybersecurity awareness through training [30].

Empirical studies consistently show that PU is a strong predictor of technology adoption [31]. For example, Davis [29] found that PU significantly influences users' intention to use a new technology. Similarly, Venkatesh and Davis [32] showed that PU is an important determinant of technology acceptance across multiple contexts. Velli and Zafiropoulos [33] also found that PU is the most significant predictor of intention to use AI-based learning platforms. The emphasis on PU (rather than perceived ease of use) is especially relevant in cybersecurity education, because the platform's effectiveness in raising awareness surpasses interface simplicity considerations, and where ease of use usually has only indirect impacts mediated by PU [34]. Based on TAM, the following hypotheses are proposed:

H8: PU has a positive influence on the intention to use (IU) an AI-based learning platform for cybersecurity awareness.

IU is based on TAM, which states that the intention to use technology is a precursor to actual usage behavior [35]. In the context of this research, the AI-based learning platform is designed to measure and improve cybersecurity awareness through training. Therefore, if students have a strong intention to use the platform, they are more likely to engage, take the training, and ultimately improve their cybersecurity awareness [36].

The connection between the intention to use and the desired outcome (in this case, increased cybersecurity awareness) has been demonstrated in various studies [37]. Research conducted in the maritime context found that the intention to use a learning platform significantly increased users' cybersecurity awareness. The study suggests that when users have a strong intention to use the platform, they are more motivated to apply the knowledge gained in a real-world context, thus increasing their awareness of cyber threats [38].

This study further extends prior models by positioning intention to use as a mediating construct that connects psychological and technological perceptions with learning outcomes. While previous research often treats intention to use as the final dependent variable, this study conceptualizes IU as a mechanism through which AI-based learning engagement leads to increased cybersecurity awareness. Based on IU, the following hypotheses are proposed:

H9: IU positively increases CSA.

3. MATERIALS AND METHODS

This research employs a quantitative research design to explore the factors influencing university students' intention to use an AI-based learning platform for cybersecurity awareness learning. The research framework integrates three theoretical models: PMT, SDT, and TAM. These models are used to examine the relationships between PV, PS, PRE, PSE, PAUT, PCOMP, PREL, PU, intention to use, and cybersecurity awareness, as illustrated in Figure 1.

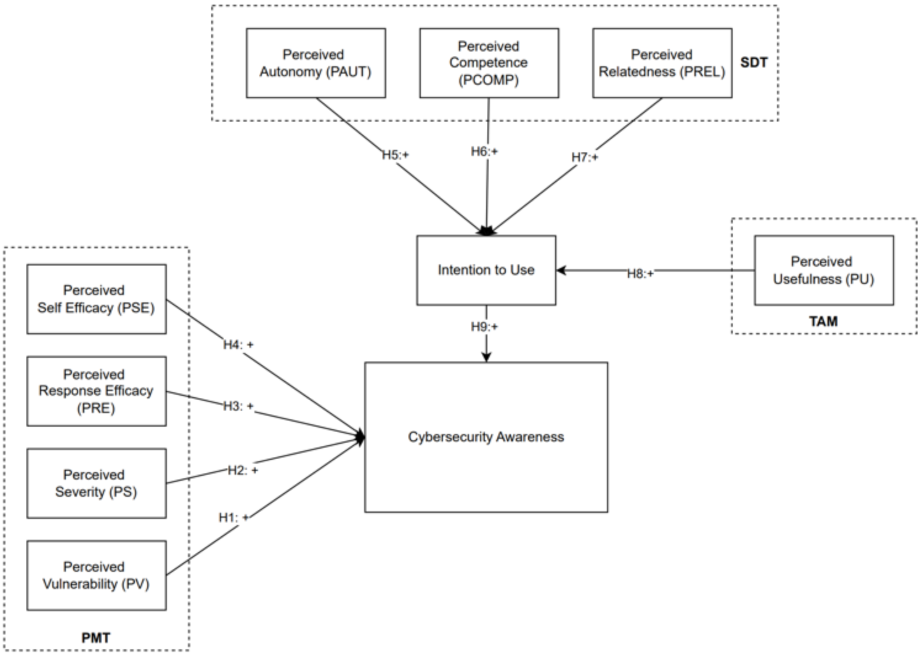
Perceived Autonomy (PAUT)
Perceived Competence (PCOMP)
Perceived Relatedness (PREL)
SDT
H5:+
H6:+
H7:+
Intention to Use
H8:+
Perceived Usefulness (PU)
TAM
H9:+
Perceived Self Efficacy (PSE)
H4: +
Perceived Response Efficacy (PRE)
H3: +
Cybersecurity Awareness
Perceived Severity (PS)
H2: +
H1: +
Perceived Vulnerability (PV)
PMT

Figure 1. Research framework

The AI-based learning platform utilized in this study, Quizalize, includes adaptive learning pathways and instant feedback mechanisms. These AI features aim to enhance learner autonomy by allowing students to progress at their own pace and receive tailored guidance.

3.1 Participant and sample description

Table 1. Respondents' characteristics

Demographic	Group	Frequency	Percentage
Gender	Male	96	45.3%
	Female	116	54.7%
Age	< 18 years	3	1.4%
	18-22 years	192	90.6%
	> 22 years	17	8%
Academic qualifications	Diploma	26	12.3%
	Bachelor	182	85.8%
	Master/Doctoral	4	1.9%
Faculty	Engineering	115	54.2%
	Non-Engineering	97	45.8%

This study involved 212 undergraduate students from a private university in Indonesia. The sample was dominated by respondents aged 18–22 years and mainly consisted of bachelor's degree students. A slightly higher proportion of female participants was observed, and the distribution across Engineering and non-Engineering faculties was relatively balanced. These characteristics ensured the sample's diversity and representativeness for evaluating the adoption of AI-based cybersecurity awareness training. Further details are presented in Table 1.

3.2 Materials of the study

This study employs a quantitative methodology, using an online survey distributed to students at a private university in Indonesia. Data collection was conducted using convenience sampling to obtain responses from participants. Before filling out the questionnaire, students were first asked to interact with an AI-based learning platform designed to assess their knowledge and understanding of cybersecurity concepts through ten multiple-choice questions in a pre-test and post-test session.

The use of a simple random sampling method (convenience sampling) has some limitations. Because participants were recruited from one private university and participated voluntarily in the study, the sample may not be fully representative of the Indonesian student population. This sampling approach can lead to self-selection bias, as students who are more interested in technology or cybersecurity topics may be more likely to participate. As a result, generalizations of results are limited, and findings should be interpreted as context-specific rather than universally applicable.

Nonetheless, this method is considered appropriate for exploratory studies researching new technologies, as it allows for initial empirical insights and theoretical testing in a controlled educational environment.

The pre-test was taken before using the platform, and the post-test was taken after usage, as shown in Figure 2. As students answered the questions, the platform actively supported their learning by providing real-time hints and brief explanations whenever they selected an incorrect answer. These hints served as micro-learning interventions, fostering awareness and immediate knowledge reinforcement. Instead of merely identifying wrong answers, the platform aimed to cultivate cybersecurity awareness by clarifying misconceptions and guiding students toward correct reasoning. This approach enabled dynamic learning, as students received immediate feedback and support to deepen their understanding of cybersecurity concepts. After learning from mistakes in the pre-test session, the students were asked to take the post-test with the same questions. The questions used in the pre-test and post-test are presented in Table 2.

After completing the pre-test and post-test, students were instructed to complete a questionnaire. The questionnaire was designed to capture their perceptions and intentions regarding AI-based platforms, focusing on constructs such as PV, PS, PRE, PSE, PAUT, PCOMP, PREL, PU, IU, and CSA.

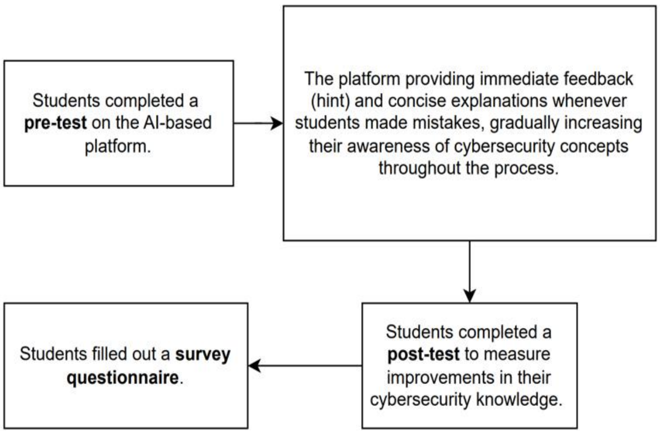
Students completed a **pre-test** on the AI-based platform.
The platform providing immediate feedback (hint) and concise explanations whenever students made mistakes, gradually increasing their awareness of cybersecurity concepts throughout the process.
Students completed a **post-test** to measure improvements in their cybersecurity knowledge.
Students filled out a **survey questionnaire**.

Figure 2. Data collection process

Table 2. Pre-test and post-test questions

No.	Questions
1.	In the context of cybersecurity, what is the most appropriate definition of 'virus'?
2.	What distinguishes a 'worm' from a computer virus?
3.	What are the common characteristics of a program that is a 'Trojan horse'?
4.	Which of these options are programs that look like legitimate apps, utilities, games, or screensavers, but are secretly performing malicious activities?
5.	An IT professional works in a company that uses an operating system that does not get updates. What is the possible impact on the company's network system?
6.	A student downloaded software from an unverified source to support his academic activities. After installing the software, the device's performance slowed down, and various unwanted pop-up windows appeared. The most appropriate action to address this situation is:
7.	A company overlooked the importance of installing a firewall and suffered a DDoS attack. What immediate impact might the company experience because of this attack?
8.	A finance professional lost important financial report data after a computer crash. If he did not back up beforehand, what actions should be taken to prevent the risk of data loss in the future?
9.	What are the main objectives of an organization's cybersecurity policy?
10.	What is 'two-factor authentication' (2FA) in cyber security policy?

Table 3. Measurement items

Construct	Code	Item	Reference
Perceived vulnerability (PV)	PV1	“I am vulnerable to losing data or files on my computer as a result of a cybersecurity breach.	[13]
	PV2	“I could potentially lose data or files on my computer due to a cybersecurity incident.	
	PV3	“It's possible that a cyber security issue caused me to lose files or information on my computer.	
Perceived severity (PS)	PS1	“If I lose my data/files due to a cyber security incident, it will cost me a lot.”	[13]
	PS2	“If I experience data/file loss due to a cyber security incident, this will be a serious problem.”	
	PS3	“If I lose my data/files due to a cybersecurity incident, this will have a huge impact.”	
Perceived response efficacy (PRE)	PRE1	“This AI-based learning platform serves to solve the problem of cyber threats.”	[13]
	PRE2	“This AI-based learning platform is effective in solving the problem of cyber threats.”	
	PRE3	“When using this AI-based learning platform, resolving cyber threat issues is more assured.”	
Perceived self-efficacy (PSE)	PSE1	“I believe that I can use this AI-based learning platform to reduce the cyber threats that attack me.”	[13]
	PSE2	“I am confident that I can use this AI-based learning platform to reduce the cyber threats that attack me.”	
	PSE3	“I am confident in my ability to use this AI-based learning platform even without instructions on how to use it.”	
Perceived autonomy (PAUT)	PAUT1	“I have the freedom to choose how I want to learn cybersecurity.”	[23]
	PAUT2	“I'm free to study cybersecurity however I see fit.”	
	PAUT3	“I believe I have the power to decide what I want to learn about cybersecurity.”	
Perceived competence	PCOMP1	“I believe I am capable of handling difficult cybersecurity duties.”	[23]

(PCOMP)	PCOMP2	"I believe I am capable of completing activities comparable to those shown in this AI-based learning platform."	
	PCOMP3	"I have faith in my capacity to understand cybersecurity principles."	
Perceived relatedness (PREL)	PREL1	"I sense that this AI-based learning platform emotionally engages me."	[23]
	PREL2	"The ideas I learned on this AI-based learning platform resonated with me personally."	
	PREL3	"The ideas presented in this AI-based learning platform resonate with me."	
Perceived usefulness (PU)	PU1	"My learning performance will be enhanced by using this AI-based learning platform."	[29]
	PU2	"I will learn more effectively if I use this AI-based learning platform."	
	PU3	"I will learn more effectively if I use this AI-based learning platform."	
	PU4	"This AI-based learning platform is helpful to me when I want to learn about cybersecurity."	
Intention to use (IU)	IU1	"I would like to use this AI-based learning platform for other learning in the future. (This digital learning platform can be used for other learning, such as Math, English, etc.)"	[35]
	IU2	"I would advise people to use the online learning environment."	
	IU3	"Compared to traditional learning, I would rather use digital learning platforms."	
	IU4	"I believe that educators should keep using this online learning environment."	
Cybersecurity awareness (CSA)	CSA1	"I understand that in order to combat cybersecurity threats, effective security procedures are required."	[36]
	CSA2	"I am aware that protecting my personal information from cyberattacks requires adherence to safe security procedures."	
	CSA3	"I am knowledgeable and capable of recognizing and addressing cybersecurity risks and threats."	
	CSA4	"I am conscious of the risks and hazards to cybersecurity that could arise from my regular activity."	
	CSA5	"I realize how important it is to establish security measures to protect my sensitive data from online threats."	

Data collection occurred on-site, with students personally approached by a team of researchers to participate in the study. This approach ensured a controlled environment, enabled efficient data collection, and allowed the researchers to promptly assist participants with questions or issues encountered while using the AI-based platform or completing the questionnaires. The research instruments included an introduction consent form that explained the study's goals, the voluntary and anonymous nature of participation, data protection procedures, and the absence of risks, expenses, or benefits. The pre-test, post-test, and questionnaire were part of a process planned to take about 20 minutes. The research instrument was created based on previous related studies [17, 29, 33]. For the convenience of the participants, the questionnaire was translated into Indonesian and tailored to the study's specific setting.

The measurement items in Table 3 were rated on a 5-point Likert scale, ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). This approach ensures the instrument is reliable and valid for assessing factors influencing students' intention to use an AI-based learning platform for cybersecurity awareness training.

3.3 Statistical analysis

Partial Least Squares Structural Equation Modelling (PLS-SEM) was used to analyse the data in this study, with SmartPLS version 4.1.0.8. The analytical procedure was divided into two phases: first, the measurement model was evaluated to assess reliability and validity; second, the structural model was assessed to examine the hypothesized linkages. With 34 indicators in the model, 212 participants were considered sufficient. Cronbach's alpha and composite reliability (CR) were used to assess reliability, while Average Variance Extracted (AVE) and discriminant validity using the Fornell-Larcker criterion were used to ensure validity. To test the importance of path coefficients, a bootstrapping approach with 5,000 resamples was used, with p-values < 0.05 considered evidence supporting the hypotheses.

3.4 Reliability and validity of the measurement model

The study evaluated the reliability and validity of the measurement model to ensure the constructs were both accurate and dependable. Reliability, reflecting the consistency of the measurement tools, was examined using Cronbach's Alpha (α), Composite Reliability (rho_a and rho_c), and AVE. As presented in Table 4, all constructs satisfied the established criteria, with Cronbach's Alpha and Composite Reliability scores exceeding 0.7, and AVE values surpassing 0.5—indicating strong internal consistency and solid convergent validity. For instance, the construct CSA demonstrated a Cronbach's Alpha of 0.930, a Composite Reliability of 0.931, and an AVE of 0.783. Similarly, PU achieved a Cronbach's Alpha of 0.925, Composite Reliability of 0.928, and an AVE of 0.816. These results confirm that the measurement instruments were highly reliable and consistent, reinforcing the validity of the constructs employed in the research.

Table 4. Construct reliability and validity

	Cronbach's Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	AVE
CSA	0.93	0.931	0.947	0.783
IU	0.905	0.909	0.934	0.779
PAUT	0.881	0.882	0.927	0.809
PCOMP	0.863	0.863	0.916	0.785
PRE	0.911	0.911	0.944	0.849
PREL	0.893	0.895	0.934	0.824
PS	0.888	0.893	0.93	0.816
PSE	0.875	0.886	0.923	0.8
PU	0.925	0.927	0.947	0.817
PV	0.903	0.911	0.939	0.838

The analysis results, as shown in Table 5, prove that all constructs meet the discriminant validity requirements. For example, the CSA construct has an AVE of 0.885, higher than its correlations with other constructs such as PAUT (0.814) or

IU (0.857). Similarly, PV has an AVE of 0.915, which is much higher than its correlations with other constructs, such as CSA (0.453) and PU (0.363). A similar pattern is observed across all variables: PREL (0.908) is higher than its correlation with PCOMP (0.827), and PS (0.904) exceeds its correlation with PSE (0.662).

Table 5. Discriminant validity model based on the Fornell-Larcker criterion

	CSA	IU	PAUT	PCOMP	PRE	PREL	PS	PSE	PU	PV
CSA	0.885									
IU	0.857	0.883								
PAUT	0.814	0.751	0.899							
PCOMP	0.71	0.738	0.75	0.886						
PRE	0.704	0.694	0.687	0.685	0.921					
PREL	0.749	0.745	0.741	0.827	0.706	0.908				
PS	0.69	0.598	0.651	0.508	0.698	0.49	0.904			
PSE	0.708	0.708	0.724	0.742	0.858	0.764	0.662	0.895		
PU	0.749	0.85	0.709	0.754	0.681	0.746	0.554	0.687	0.904	
PV	0.453	0.418	0.467	0.423	0.444	0.433	0.508	0.44	0.363	0.915

4. RESULTS

4.1 Test analysis

The study compared participants' pre-test and post-test scores to assess the impact of the AI-based cybersecurity learning platform. Figure 3 reveals a significant improvement, with the average score rising from 76.37 to 87.97, indicating that the platform effectively enhanced participants' understanding and awareness of cybersecurity.

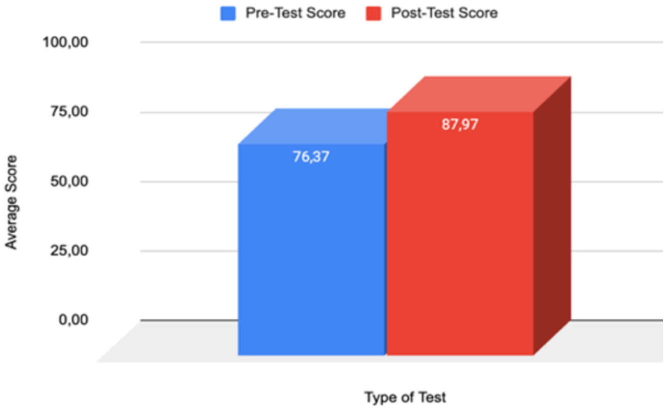

Figure 3. Comparison of average test scores

4.2 Structural model analysis

To evaluate the structural model, hypothesis testing was performed using the hypotheses given in this study. Table 6 shows the results of the direct link between the variables investigated with the PLS-SEM approach. The results show that of the nine hypotheses proposed, four hypotheses are accepted because they have a positive and significant relationship, while the other five are rejected because they do not show a significant relationship.

Based on the analysis results presented in Table 6, the data support several hypotheses, and some that are rejected. The accepted hypotheses are H2 (PS → CSA), H5 (PAUT → IU), H8 (PU → IU), and H9 (IU → CSA), as they have a p-value of less than 0.05, indicating a statistically significant relationship. For example, the PS → CSA relationship has a path coefficient of 0.229 with a p-value of 0.000, which indicates that PS has a positive effect on CSA. Similarly, the relationships PU → IU (β = 0.571, p = 0.000) and IU → CSA (b = 0.643, p = 0.000) are also significant, confirming the important role of these variables.

Table 6. Direct hypothesis results

Hypothesis	Relationships	Original Sample (O)	P-Value	Decision
H1	PV → CSA	0.026	0.540	Rejected
H2	PS → CSA	0.229	0.000	Accepted
H3	PRE → CSA	0.032	0.693	Rejected
H4	PSE → CSA	0.062	0.404	Rejected
H5	PAUT → IU	0.232	0.000	Accepted
H6	PCOMP → IU	0.037	0.520	Rejected
H7	PREL → IU	0.117	0.126	Rejected
H8	PU → IU	0.571	0.000	Accepted
H9	IU → CSA	0.643	0.000	Accepted

On the other hand, hypotheses H1 (PV → CSA), H3 (PRE → CSA), H4 (PSE → CSA), H6 (PCOMP → IU), and H7 (PREL → IU) were rejected because the p-value exceeded 0.05, indicating that the relationships between these variables were not significant. For example, the relationship PV → CSA has a path coefficient of 0.026 with a p-value of 0.540, which means there is no significant effect. The same is true for the relationships PRE → CSA (β = 0.032, p = 0.693) and PCOMP → IU (β = 0.037, p = 0.520). Figure 4 depicts the structural model result in this study.

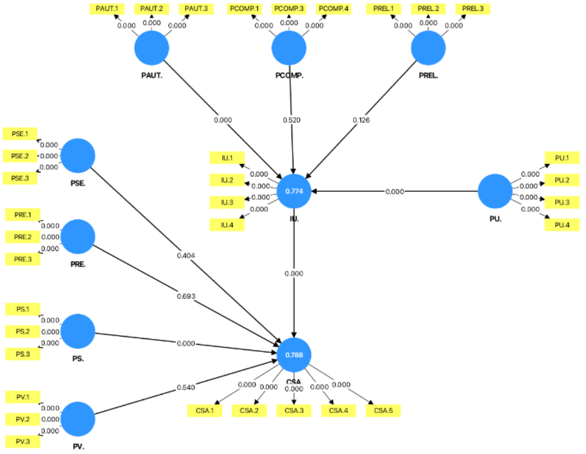

Figure 4. PLS structure model

The findings revealed that only certain factors significantly influenced CSA and IU, while other factors had no meaningful impact. The results of this study can serve as a basis for further studies to identify other variables that are more relevant in the context of CSA and IU.

4.3 Descriptive analysis

To understand the characteristics of students' perceptions and attitudes toward AI-based learning platforms in improving cybersecurity awareness, a descriptive analysis was conducted on all variables measured using a 5-point Likert scale. The results of the descriptive analysis are presented in Table 7.

Table 7. Descriptive analysis of all variables

Variable	Item No.	Mean	Median	Standard Deviation
PV	PV1	3.958	4.000	1.015
	PV2	3.981	4.000	0.995
	PV3	3.995	4.000	1.007
PS	PS1	4.330	5.000	0.821
	PS2	4.321	5.000	0.765
	PS3	4.330	5.000	0.786
PRE	PRE1	4.184	4.000	0.764
	PRE2	4.137	4.000	0.780
	PRE3	4.132	4.000	0.825
PSE	PSE1	4.137	4.000	0.768
	PSE2	4.184	4.000	0.776
	PSE3	4.071	4.000	0.879
PAUT	PAUT1	4.179	4.000	0.787
	PAUT2	4.165	4.000	0.769
	PAUT3	4.241	4.000	0.767
PCOMP	PCOMP1	3.991	4.000	0.841
	PCOMP2	4.047	4.000	0.834
	PCOMP3	4.094	4.000	0.847
PREL	PREL1	4.024	4.000	0.832
	PREL2	4.075	4.000	0.797
	PREL3	4.132	4.000	0.808
PU	PU1	4.175	4.000	0.779
	PU2	4.151	4.000	0.787
	PU3	4.203	4.000	0.753
	PU4	4.189	4.000	0.814
IU	IU1	4.179	4.000	0.768
	IU2	4.160	4.000	0.773
	IU3	4.189	4.000	0.790
	IU4	4.212	4.000	0.744

In addition to maintaining and promoting the variables that showed significant effects, descriptive analysis revealed that certain items within these constructs still require further attention. Although these variables demonstrated statistical significance, some items recorded slightly lower mean scores than others within the same construct, indicating areas that need reinforcement to maximise the platform's effectiveness.

For instance, within PAUT, item PAUT2 ("I'm free to study cybersecurity however I see fit") had the lowest mean (M = 4.165) compared to PAUT1 (M = 4.179) and PAUT3 (M = 4.241). This item reflects students' perceived control over their learning approach. Although autonomy as a construct significantly affects intention to use (IU), this score suggests an opportunity to enhance personalization and flexible learning pathways within the platform.

In PU, the item with the lowest mean was PU2: "I will learn more effectively if I use this AI-based learning platform" (M = 4.151). Despite PU's strong effect on IU, this relatively lower perception indicates that students may not be fully convinced of the platform's learning impact. This could be addressed by incorporating features that visualize progress, demonstrate learning outcomes, and present real-world applications of the content.

For IU, the lowest mean was recorded in IU2: "I would advise people to use the online learning environment" (M = 4.160). Although IU significantly contributes to CSA, this suggests that students may feel confident using the platform themselves but remain hesitant to recommend it to others. To strengthen this dimension, improvements can be made in user experience, community endorsement (e.g., testimonials), and sharing functionalities that allow learners to showcase their achievements.

Interestingly, within PS, the construct with the highest mean overall (M = 4.32), PS2: "If I experience data/file loss due to a cybersecurity incident, this will be a serious problem" scored slightly lower (M = 4.321) than PS1 and PS3 (both M = 4.330). This slight gap may indicate that while students acknowledge the impact of cyber incidents, the practical consequences may not yet feel personally relevant. Strengthening this perception through real-case scenarios or visual representations of cybersecurity breaches could enhance their awareness of potential threats.

These findings demonstrate that even among significant constructs, certain dimensions can still be improved. By targeting these specific items, PAUT2, PU2, IU2, and PS2, platform developers and educators can refine learning experiences, increase trust, and further elevate students' engagement and cybersecurity awareness.

4.4 Discussion

Understanding the contextual factors that influence the results is essential for interpreting the relationships between variables in this study. Various psychological and technological factors play a role in shaping students' engagement with the AI-based learning platform. The analysis reveals that some factors significantly contribute to students' CSA and IU platforms, and these will be discussed first. Meanwhile, other factors do not exhibit a meaningful impact, which will be addressed later in the discussion.

PS significantly influences CSA, leading to the acceptance of H2. This indicates that students who perceive cyber threats as severe are more likely to engage with the platform and enhance their cybersecurity awareness. The significance of PS can be attributed to the frequent media coverage of severe data breaches in Indonesia, which heightens public concern [39]. These findings align with previous research [17, 18], which identified PS as a key driver of protective behaviors and cybersecurity awareness in educational and organizational settings.

Similarly, PAUT significantly affects the IU AI-based learning platform, supporting H5. This suggests that students appreciate the flexibility and control provided by the AI-based learning platform, which enhances their motivation to use it. The significance of PAUT, along with PU, reflects the adaptability of Indonesia's younger generation to mobile technology [40]. The results are consistent with references [29, 40] who found that autonomy-supportive educational technologies increase user engagement and adoption intentions.

PU also has a significant positive impact on IU, confirming H8. This implies that students are more likely to adopt the platform if they believe it effectively enhances their cybersecurity knowledge [41]. Similar conclusions were drawn in other research [29, 33], which identified perceived usefulness as a dominant predictor of technology acceptance in educational contexts.

Furthermore, IU significantly increases CSA, supporting H9. This suggests that students who intend to use the platform are more likely to develop higher cybersecurity awareness through active engagement. The strong relationship between IU and CSA reflects the appeal of AI-based learning methods, which remain relatively new in Indonesia. This finding is in line with previous research [42], which demonstrated that the intention to use cybersecurity training tools positively correlates with improved awareness and knowledge retention.

On the other hand, several factors do not significantly influence CSA or IU. PV does not significantly influence CSA, thereby rejecting H1. This suggests that although students recognise their vulnerability to cyber threats, that awareness does not necessarily translate into proactive learning behaviours. One possible explanation for this insignificance is the relatively low level of cybersecurity literacy among the Indonesian population compared to that in developed countries like the UAE, which may lead to minimal awareness of their susceptibility to cyber threats [43]. This finding contrasts with previous studies [16, 18], which reported that PV significantly drives cybersecurity awareness, particularly in high-risk environments.

Similarly, PRE does not significantly affect CSA, thereby rejecting H3. This suggests that students may not fully trust the platform's ability to mitigate cyber threats, possibly due to their limited prior exposure to such tools. The insignificance of PRE can be attributed to Indonesian students' limited experience with cybersecurity training, which makes them more skeptical of the platform's effectiveness. Unlike the study, which was performed in the US [29] and utilised the NICE framework, Indonesia does not yet have an established national standard for cybersecurity education [44].

Likewise, PSE does not significantly impact CSA, resulting in the rejection of H4. This indicates that students' confidence in their ability to use the platform does not directly enhance their cybersecurity awareness. The insignificance of PSE may be due to Indonesia's IT curriculum, which does not emphasize cybersecurity practices, and to limited access to cybersecurity tools. These findings contrast with previous research [19, 27, 45], which identified response efficacy and self-efficacy as key factors in cybersecurity training outcomes, behaviour, and technology adoption in more structured educational environments.

Additionally, PCOMP does not significantly influence IU, leading to the rejection of H6. This suggests that students' belief in their cybersecurity skills does not necessarily increase their intention to use the platform. Another explanation is Indonesia's hierarchical and lecturer-centric educational culture, which may limit students' sense of independent competence [46]. Additionally, the platform's overly technical design for novice users could further hinder engagement.

Finally, PREL does not significantly affect IU, resulting in the rejection of H7. This implies that emotional connection to the platform or subject matter does not play a crucial role in adoption intentions [47]. The insignificance of PREL is attributed to the lack of social features on the platform and the absence of institutional incentives that connect learning to real-world needs [45]. These findings contrast with previous studies [21, 26, 48, 49], which emphasised the importance of competence and relatedness in fostering engagement in technology-enhanced, socially embedded learning environments.

Despite this limitation, as explained in the previous paragraph, post-test scores compared to pre-test scores indicate that the AI-based learning platform, equipped with dynamic feedback mechanisms, effectively improved students' understanding of cybersecurity concepts. This finding underscores the potential of AI-based tools in enhancing cybersecurity education, particularly in developing countries like Indonesia, where cybersecurity awareness is still evolving [50, 51].

5. CONCLUSIONS

This study demonstrated that AI-based learning platforms effectively enhance cybersecurity awareness among Indonesian university students, with post-test results significantly higher than pre-test results. Key findings revealed that the PS of cyber threats and intention to use the platform strongly influenced cybersecurity awareness, while perceived autonomy and usefulness were critical drivers of intention to use the learning platform.

However, several limitations should be carefully considered when interpreting these findings. First, the narrow demographic scope, which focused exclusively on Indonesian university students, may have influenced the non-significant effects of PV, response efficacy, self-efficacy, competence, and relatedness. In contexts where baseline cybersecurity literacy is relatively low, students may not accurately perceive their vulnerability or efficacy, thereby weakening the explanatory power of these constructs. As a result, the findings should not be generalized beyond similar educational and cultural settings without caution.

Second, the study's short-term nature limits the ability to assess whether increased cybersecurity awareness translates into sustained behavioural change. While post-test improvements indicate immediate learning gains, the absence of longitudinal data limits conclusions about long-term retention and real-world cybersecurity practices. This limitation may partially explain why motivational constructs related to competence and relatedness did not exhibit significant effects, as such factors often manifest more strongly over extended learning periods.

Third, the limited use of AI functionalities—primarily for question and hint generation—may have constrained the platform's potential impact on adaptive learning, personalised feedback, and deeper student engagement. Consequently, the observed effects likely underestimate the full educational value of AI-based learning platforms. More comprehensive AI integration could amplify both motivational and behavioural outcomes.

As a practical contribution, this study highlights the need for policymakers, platform developers, and educators to prioritise scalable, ethically designed AI-based solutions to address persistent gaps in cybersecurity awareness. Practical implementation can be operationalized through the integration of scenario-based simulations that replicate real-world cyber threat environments, supported by gamified elements such as achievement badges, progressive challenge levels, and adaptive task difficulty. Furthermore, collaboration with industry stakeholders can strengthen implementation by aligning AI-generated learning content with current threat models, professional skill requirements, and evolving cybersecurity standards. By combining technological scalability with culturally adaptive, learner-centred design, this study provides a concrete pathway for translating AI-driven cybersecurity education research into sustainable, impactful educational practice.

ACKNOWLEDGMENT

This work is funded by a Regular Fundamental Research Grant from the Ministry of Higher Education, Science, and Technology of the Republic of Indonesia No. Contract: PARENT DPPM-LLDIKTI 125/C3/DT.05.00/PL/2025; Derivative LLDIKTI-PTS 7925/LL4/PG/2025; Derivative PTS-Researcher and 096/LIT07/PPM-LIT/2025.

REFERENCES

[1] Schmitt, M., Koutroumpis, P. (2025). Cyber shadows: Neutralizing security threats with AI and targeted policy measures. IEEE Transactions on Artificial Intelligence, 6(7): 1697-1705. https://doi.org/10.1109/tai.2025.3527398

[2] Candiwan, Sari, P.K., Nurshabrina, N. (2015). Assessment of information security management on Indonesian higher education institutions. In Lecture Notes in Electrical Engineering, pp. 375-385. https://doi.org/10.1007/978-3-319-24584-3_31

[3] Al-Khassawneh, Y.A. (2022). A review of artificial intelligence in security and privacy: Research advances, applications, opportunities, and challenges. Indonesian Journal of Science and Technology, 8(1): 79-96. https://doi.org/10.17509/ijost.v8i1.52709

[4] Morrow, E. (2024). Scamming higher ed: An analysis of phishing content and trends. Computers in Human Behavior, 158: 108274. https://doi.org/10.1016/j.chb.2024.108274

[5] Tang, K.Y., Chang, C.Y., Hwang, G.J. (2021). Trends in artificial intelligence-supported e-learning: A systematic review and co-citation network analysis (1998-2019). Interactive Learning Environments, 31(4): 2134-2152. https://doi.org/10.1080/10494820.2021.1875001

[6] Blažić, A.J., Blažić, B.J. (2024). Teaching and learning cybersecurity for European youth by applying interactive technology and smart education. Education and Information Technologies, 30(7): 9093-9120. https://doi.org/10.1007/s10639-024-13155-3

[7] Dogan, M.E., Goru Dogan, T., Bozkurt, A. (2023). The use of artificial intelligence (AI) in online learning and distance education processes: A systematic review of empirical studies. Applied Sciences, 13(5): 3056. https://doi.org/10.3390/app13053056

[8] Halkiopoulos, C., Gkintoni, E. (2024). Leveraging AI in E-Learning: Personalized learning and adaptive assessment through cognitive neuropsychology—A systematic analysis. Electronics, 13(18): 3762. https://doi.org/10.3390/electronics13183762

[9] Gligorea, I., Cioca, M., Oancea, R., Gorski, A.T., Gorski, H., Tudorache, P. (2023). Adaptive learning using artificial intelligence in e-learning: A literature review. Education Sciences, 13(12): 1216. https://doi.org/10.3390/educsci13121216

[10] Rachmayanti, T.S., Sari, P.K., Candiwan, C. (2024). Understanding what motivates students to use digital platforms for cybersecurity learning and awareness: A conceptual model. In 2024 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung, Indonesia, pp. 517-522. https://doi.org/10.1109/icitsi65188.2024.10929266

[11] Rahim, A.S., Widodo, P., Reksoprodjo, A.H.S., Alsodiq, A. (2023). Identify cyber intelligence threats in Indonesia. International Journal of Humanities Education and Social Sciences, 3(1): 431-440. https://doi.org/10.55227/ijhess.v3i1.426

[12] Dewi, H.A., Candiwan, C., Sari, P.K. (2024). Artificial intelligence in security education, training and awareness: A bibliometric analysis. In 2024 International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA), Bali, Indonesia, pp. 914-919. https://doi.org/10.1109/icicyta64807.2024.10912940

[13] Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. The Journal of Psychology, 91(1): 93-114. https://doi.org/10.1080/00223980.1975.9915803

[14] Mackay, M.I., Klas, A., Fernando, J., Kothe, E.J., Ling, M. (2024). Using protection motivation theory to explain Australian's motivations to engage in individual and collective climate actions. Asian Journal of Social Psychology, 28(1). https://doi.org/10.1111/ajsp.12660

[15] González-Ponce, B.M., Carmona-Márquez, J., Pilatti, A., Díaz-Batanero, C., Fernández-Calderón, F. (2024). The protection motivation theory as an explanatory model for intention to use alcohol protective behavioral strategies among young adults. Alcohol and Alcoholism, 59(5): agae059. https://doi.org/10.1093/alcalc/agae059

[16] Alneyadi, M.R.M.A.H., Normalini, M.K. (2025). Intelligent protection: A study of the key drivers of intention to adopt artificial intelligence (AI) cybersecurity systems in the UAE. Interdisciplinary Journal of Information, Knowledge, and Management, 20: 003. https://doi.org/10.28945/5430

[17] Alneyadi, M.R.M.A.H., Normalini, M.K. (2023). Factors influencing user's intention to adopt AI-Based cybersecurity systems in the UAE. Interdisciplinary Journal of Information, Knowledge, and Management, 18: 459-486. https://doi.org/10.28945/5166

[18] Vafaei-Zadeh, A., Nikbin, D., Teoh, K.Y., Hanifah, H. (2024). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. International Journal of Bank Marketing, 43(3): 476-505. https://doi.org/10.1108/ijbm-03-2024-0138

[19] Almansoori, A., Al-Emran, M., Shaalan, K. (2024). Determinants of users' cybersecurity behavior in the metaverse: A deep learning-based hybrid SEM-ANN approach. International Journal of Human-Computer Interaction, 41(17): 11116-11133. https://doi.org/10.1080/10447318.2024.2440674

[20] Deci, E.L., Ryan, R.M. (1985). Intrinsic Motivation and Self-Determination in Human Behavior. Springer. https://doi.org/10.1007/978-1-4899-2271-7

[21] Zhang, S., Miao, C. (2024). The mediating role of competence, autonomy, and relatedness in the activation and maintenance of sports participation behavior. Scientific Reports, 14(1): 27124. https://doi.org/10.1038/s41598-024-78760-1

[22] Wong, X.J., Tajudeen, F.P. (2024). Factors affecting employees' intention to work through the metaverse

platform. International Journal of Human-Computer Interaction, 41(11): 7058-7075. https://doi.org/10.1080/10447318.2024.2388480

[23] Ryan, R.M., Deci, E.L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. American Psychologist, 55(1): 68-78. https://doi.org/10.1037/0003-066x.55.1.68

[24] Osman, S.A., Ahmed, Z.E. (2024). Navigating AI integration. In Advances in Educational Technologies and Instructional Design, pp. 240-267. https://doi.org/10.4018/979-8-3693-2728-9.ch011

[25] Hensley, L., Sayers, R., Brady, A., Cutshall, J. (2020). Supporting autonomy, competence, and relatedness in a learning-to-learn course: College students' insights into effective instruction. Teaching of Psychology, 48(3): 236-247. https://doi.org/10.1177/0098628320977270

[26] Oppl, S., Stary, C. (2022). Motivating users to manage privacy concerns in cyber-physical settings—A design science approach considering self-determination theory. Sustainability, 14(2): 900. https://doi.org/10.3390/su14020900

[27] Kam, H., Ormond, D.K., Menard, P., Crossler, R.E. (2021). That's interesting: An examination of interest theory and selfdetermination in organisational cybersecurity training. Information Systems Journal, 32(4): 888-926. https://doi.org/10.1111/isj.12374

[28] O'Dea, M. (2025). Editorial: "Are technology acceptance models still fit for purpose?". Journal of University Teaching and Learning Practice, 21(8). https://doi.org/10.53761/1bdbms32

[29] Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3): 319-340. https://doi.org/10.2307/249008

[30] Ortiz-Garcés, I., Govea, J., Sánchez-Viteri, S., Villegas-Ch., W. (2024). CyberEduPlatform: An educational tool to improve cybersecurity through anomaly detection with artificial intelligence. PeerJ Computer Science, 10: e2041. https://doi.org/10.7717/peerj-cs.2041

[31] Shania, F., Paramarta, V. (2024). Analysis of technology acceptance model (TAM) on the use of electronic medical records in hospitals. Jurnal Indonesia Sosial Sains, 5(12): 3190-3196. https://doi.org/10.59141/jiss.v5i12.1520

[32] Venkatesh, V., Davis, F.D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. Management Science, 46(2): 186-204. https://doi.org/10.1287/mnsc.46.2.186.11926

[33] Velli, K., Zafiropoulos, K. (2024). Factors that affect the acceptance of educational AI tools by Greek teachers—A structural equation modelling study. European Journal of Investigation in Health, Psychology and Education, 14(9): 2560-2579. https://doi.org/10.3390/ejihpe14090169

[34] Crabb, J., Izurieta, C., Van Wie, B., Adesope, O., Gebremedhin, A. (2024). Cybersecurity education: Insights from a novel cybersecurity summer workshop. IEEE Security & Privacy, 22(6): 89-98. https://doi.org/10.1109/msec.2024.3473188

[35] Or, C. (2024). Watch that attitude! Examining the role of attitude in the technology acceptance model through meta-analytic structural equation modelling. International Journal of Technology in Education and Science, 8(4): 558-582. https://doi.org/10.46328/ijtes.575

[36] Pramod, D. (2024). Gamification in cybersecurity education; a state of the art review and research agenda. Journal of Applied Research in Higher Education, 17(4): 1162-1180. https://doi.org/10.1108/jarhe-02-2024-0072

[37] Almansoori, A., Al-Emran, M., Shaalan, K. (2023). Exploring the frontiers of cybersecurity behavior: A systematic review of studies and theories. Applied Sciences, 13(9): 5700. https://doi.org/10.3390/app13095700

[38] Becmeur, T., Boudvin, X., Brosset, D., Héno, G., Merien, T., Jacq, O., Kermarrec, Y., Sultan, B. (2017). A platform for raising awareness on cyber security in a maritime context. In 2017 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, pp. 103-108. https://doi.org/10.1109/csci.2017.17

[39] Das, S., Lo, J., Dabbish, L., Hong, J.I. (2018). Breaking! A typology of security and privacy news and how it's shared. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, QC, Canada, pp. 1-12. https://doi.org/10.1145/3173574.3173575

[40] Lisana, L. (2022). Factors affecting university students switching intention to mobile learning: A push-pull-mooring theory perspective. Education and Information Technologies, 28(5): 5341-5361. https://doi.org/10.1007/s10639-022-11410-z

[41] Deng, Y., Zeng, Z., Huang, D. (2021). NeoCyberKG: Enhancing cybersecurity laboratories with a machine learning-enabled knowledge graph. In Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V.1, Germany, pp. 310-316. https://doi.org/10.1145/3430665.3456378

[42] Adouani, Y., Khenissi, M.A. (2024). Investigating computer science students' intentions towards the use of an online educational platform using an extended technology acceptance model (e-TAM): An empirical study at a public university in Tunisia. Education and Information Technologies, 29: 14621-14645. https://doi.org/10.1007/s10639-023-12437-6

[43] De Kimpe, L., Walrave, M., Verdegem, P., Ponnet, K. (2021). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8): 1796-1808. https://doi.org/10.1080/0144929x.2021.1905066

[44] Mulyadi, Rahayu, D. (2018). Indonesia national cybersecurity review: Before and after establishment national cyber and crypto agency (BSSN). In 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, pp. 1-6. https://doi.org/10.1109/citsm.2018.8674265

[45] Shao, C., Nah, S., Makady, H., McNealy, J. (2024). Understanding user attitudes towards AI-enabled technologies: An integrated model of self-efficacy, TAM, and AI ethics. International Journal of Human-Computer Interaction, 41(5): 3053-3065. https://doi.org/10.1080/10447318.2024.2331858

[46] Qurohman, M.T., Zaenuri, Mulyono, Wardono. (2024). Development of the learning model group investigations based academic culture (GIBAC). Evolutionary Studies in Imaginative Culture, 9(1): 52-63.

https://doi.org/10.70082/esiculture.vi.1307

[47] Songkram, N., Chootongchai, S., Osuwan, H., Chuppunnarat, Y., Songkram, N. (2023). Students' adoption towards behavioral intention of digital learning platform. Education and Information Technologies, 28(9): 11655-11677. https://doi.org/10.1007/s10639-023-11637-4

[48] Inan, D.I., Hidayanto, A.N., Juita, R., Hasian, C.Y., Luvian, K., Leonardo, Ian, S.L., Pratama, S. (2023). How personal, technical, social environments affecting generation Z to utilise video-based sharing platform in learning process during crisis? Research and Practice in Technology Enhanced Learning, 19: 003. https://doi.org/10.58459/rptel.2024.19003

[49] Jetten, J., Postmes, T., McAuliffe, B.J. (2002). 'We're all individuals': Group norms of individualism and collectivism, levels of identification and identity threat. European Journal of Social Psychology, 32(2): 189-207. https://doi.org/10.1002/ejsp.65

[50] Astuti, E.F., Hidayanto, A.N., Nurwardani, S., Salsabila, A.Z. (2024). Assessing Indonesian MSMEs' awareness of personal data protection by PDP law and ISO/IEC 27001:2013. International Journal of Safety and Security Engineering, 14(5): 1559-1567. https://doi.org/10.18280/ijsse.140523

[51] Akib, A.A.P.M., Candiwan, C., Ramadhani, D.P. (2025). Cybersecurity compliance and other factors influencing employee protective behavior: A case study of bank X in Indonesia. International Journal of Safety and Security Engineering, 15(6): 1229-1241. https://doi.org/10.18280/ijsse.150613