ANALYSIS OF CYBERSECURITY AWARENESS AND BEHAVIOR AMONG STUDENTS OF IPB UNIVERSITY: AN INTEGRATION OF PROTECTION MOTIVATION THEORY AND THEORY OF PLANNED BEHAVIOR

Muhammad Gustara[1]
Institut Pertanian Bogor, Bogor, Indonesia
muhammadgustara@apps.ipb.ac.id

Eko Ruddy Cahyadi[2]
Institut Pertanian Bogor, Bogor, Indonesia
ekocahyadi@apps.ipb.ac.id

Bagus Sartono[3]
Institut Pertanian Bogor, Bogor, Indonesia
bagusco@apps.ipb.ac.id

Abstract

This study aims to analyze the factors influencing cybersecurity awareness and behavior among students of IPB University by integrating the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB). Data were collected through an online survey involving 255 students and analyzed using Partial Least Squares Structural Equation Modeling (PLS-SEM). The findings reveal that behavioral intention and awareness significantly influence cybersecurity behavior. Variables such as attitude, subjective norms, response efficacy, and perceived severity contribute significantly to shaping intention and awareness, whereas perceived vulnerability and self-efficacy do not directly affect intention. These results reinforce the validity of integrating PMT and TPB in explaining cybersecurity behavior determinants and offer practical implications for developing evidence-based cybersecurity literacy programs in academic settings.

Keywords: Cybersecurity, Students, Protection Motivation Theory, Theory of Planned Behavior, PLS-SEM

INTRODUCTION

Cybersecurity is a major concern in the digital era, significantly affecting organizations, including academic institutions such as Bogor Agricultural University (IPB). Cyberattacks can disrupt operations, damage institutional reputations, and result in substantial financial losses. Institutions that handle sensitive data—such as students' personal information, research documents, and administrative systems—are particularly vulnerable to these threats. According to the BSSN (2024), the education sector has experienced various disruptions caused by cyberattacks. Nationally, there were 514,508 ransomware incidents, 26.7 million phishing activities, and 56.1 million data records exposed on the darknet. Alarmingly, 58% of reported incidents received no response from the affected institutions. The National Cyber Security Index (NCSI, 2024) ranked Indonesia 49th, with only 64% fulfillment of cybersecurity capacity indicators. Particularly low scores were recorded in digital service protection (20%) and global contribution (17%), indicating a lack of national readiness to respond to cyber threats. The education sector, being part of this national landscape, is therefore at considerable risk.

Data from SAFEnet (2024) further highlight that students are among the most frequent victims of cyber incidents. This aligns with findings by (Alqahtani, 2022), who reported low cybersecurity awareness among students, particularly regarding the use of social media and personal data protection. At IPB, information technology is deeply embedded in academic, research, and administrative processes. While this integration enhances efficiency, it also increases vulnerability to cyber threats such as ransomware and system breaches. Despite the global importance of cybersecurity, awareness and understanding of digital threats among students may still be limited. This situation is often exacerbated by risky digital behaviors, including the use of weak passwords and neglecting software updates.

In light of these concerns, this study seeks to identify the factors that influence cybersecurity awareness and behavior among IPB students, examine the levels of their awareness and secure practices, and offer strategic recommendations to strengthen protection. The findings are intended to support IPB in enhancing digital resilience within the education sector. Cybersecurity itself is defined as the discipline that safeguards hardware, software, and information (Patterson & Winston, 2019; Solms & Solms, 2018). Cybersecurity awareness refers to an individual's understanding of potential risks and the preventive actions required to mitigate them (Zadeh et al., 2018). It plays a foundational role in protection motivation by reducing perceived vulnerability and severity while increasing self-efficacy (Conetta, 2019; Kovacevic et al., 2020; Ifinedo, 2012; Bekkers et al., 2023). Cybersecurity behavior includes preventive actions such as using strong passwords, regularly updating software, and backing up data (Hadlington, 2017; Kovacevic et al., 2020; Verkijika, 2020).

This study applies an integrated framework combining Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB). PMT explains that protection motivation is determined by individuals' assessments of threat severity, vulnerability, and their coping abilities (Rogers, 1975; Bekkers et al., 2023; Ifinedo, 2012). Meanwhile, TPB posits that behavior is primarily predicted by intention, which is shaped by behavioral beliefs, normative beliefs, and perceived behavioral control (Ajzen, 1991). Within this theoretical framework, the study explores how factors such as self-efficacy, response efficacy, perceived severity, perceived vulnerability, attitude, subjective norms, and perceived behavioral control influence students' cybersecurity awareness and intention to behave securely. It also

examines how both awareness and intention affect actual cybersecurity behavior. Ultimately, this research aims to formulate strategic recommendations to enhance cybersecurity awareness, intention, and behavior among IPB students.

REVIEW OF LITERATURE

Cybersecurity

Cybersecurity has become a critical concern in the digital era, particularly within academic institutions that manage sensitive data and operate in open network environments. According to Patterson and Winston (2019), cybersecurity is the scientific discipline that protects all elements of computing, including hardware, software, and the data they store. Solms and Solms (2018) emphasize that safeguarding digital information assets in cyberspace has become increasingly vital as technological systems grow more complex and cyber threats more sophisticated.

Higher education institutions are among the primary targets of cyberattacks due to their decentralized structures and the volume of valuable data they process, such as student records, financial transactions, and research outputs. Common cybersecurity threats in academic settings include phishing, which manipulates human behavior to steal sensitive data (Aldawood & Skinner, 2020); malware, including ransomware and spyware, which damages systems or exfiltrates information (Erendor, 2022); and brute-force attacks that exploit weak password practices, particularly among students (Alqahtani, 2022). In addition, data theft and denial-of-service (DoS) attacks further expose academic networks to operational disruption and reputational damage (Kalhoro et al., 2021).

The lack of cybersecurity awareness and technical skills among users especially students is a significant contributing factor to institutional vulnerability. Hong et al. (2023) found that individuals from low-education environments tend to demonstrate weaker awareness of cyber risks. Similarly, the exploitation of third-party software vulnerabilities remains a common attack vector for unauthorized access (Kont, 2024). Despite their familiarity with digital technologies, many students lack the foundational knowledge required to implement effective security practices (Alzahrani, 2021).

Addressing cybersecurity in higher education requires a collective, multidisciplinary effort encompassing user education, robust institutional policies, and reliable technological infrastructure. Cybersecurity should not be viewed solely as an individual responsibility but as a shared obligation to ensure data protection, operational resilience, and the development of a security-aware culture in academic environments.

Cybersecurity Awareness

Cybersecurity awareness is the understanding of information security risks and the necessary actions to prevent cyber threats, shaped by knowledge, attitudes, behaviors, and self-perceptions (Zadeh et al., 2018; Chandarman & Van Niekerk, 2017). It enhances protective motivation by reducing perceived vulnerability and increasing self-efficacy (Ifinedo, 2012; Bekkers et al., 2023). Awareness is influenced by various factors, including demographics (age, gender, education), psychological traits (knowledge, self-efficacy, threat perception), situational aspects (time pressure, training access), and social dynamics (peer influence, organizational culture) (Fatokun et al., 2019; Chowdury et al., 2020; McAlaney & Benson, 2020). In academic settings, fostering a cybersecurity-aware culture is crucial, as students, faculty, and staff face risks that threaten data security and institutional integrity.

Understanding these multifaceted influences enables targeted strategies to build resilient cybersecurity behavior in educational environments.

Cybersecurity Behavior

Cybersecurity behavior refers to individual actions and habitual practices aimed at protecting personal or organizational data from cyber threats, encompassing both immediate threat responses and routine cyber hygiene (Verkijika, 2020; Conetta, 2019). These behaviors include identifying phishing attempts, using strong passwords, updating software, avoiding suspicious links, and minimizing exposure of personal information online (Hadlington, 2017; Kovacevic et al., 2020). Effective cybersecurity behavior also involves responsible use of social media, device security, and awareness of secure network practices (Ibrahim et al., 2024). While knowledge and skills contribute to the formation of secure habits (Zwilling et al., 2020), human factors such as motivation and personality also play a role (Patterson & Winston, 2019). Despite this, many students still engage in risky behaviors like using weak passwords or ignoring software updates (Alqahtani, 2022). Therefore, cybersecurity education and training remain essential in fostering both awareness and protective behavior to mitigate risks in increasingly digitalized environments.

Protection Motivation Theory

Protection Motivation Theory (PMT), first introduced by Rogers (1975), serves as a conceptual framework for understanding how individuals are motivated to protect themselves from threats. The theory posits that protection motivation is influenced by two primary cognitive processes: threat appraisal and coping appraisal. Threat appraisal refers to an individual's assessment of the severity of a threat and their perceived vulnerability to it, while coping appraisal includes self-efficacy (confidence in one's ability to perform protective actions) and response efficacy (belief that those actions will be effective). PMT has been widely applied in information security research. For instance, Meso et al. (2013) used PMT to assess how knowledge and direct experience affect students' cybersecurity behavior, finding that hands-on experiences, such as information security projects, can enhance both threat perception and coping capacity, thus promoting preventive actions. In a cross-cultural study, Ameen et al. (2020) applied PMT to examine cybersecurity behavior across the UK, USA, and UAE, revealing that cultural factors significantly influence both threat and coping appraisals, highlighting the need for culturally contextualized cybersecurity strategies. Farooq et al. (2019) integrated PMT with the Theory of Planned Behavior (TPB) to investigate student behavior in Kenya, discovering that among PMT constructs, only self-efficacy significantly influenced students' intentions to adopt protective behavior, underscoring the importance of strengthening belief in personal capabilities. Similarly, Li et al. (2022) emphasized the role of threat severity and vulnerability in shaping personal information protection behaviors, a finding supported by Bekkers et al. (2023), who noted that individuals perceiving high risk were more motivated to engage in secure behavior. Ifinedo (2012) further confirmed that both self-efficacy and response efficacy positively affect behavioral intentions, suggesting that individuals who feel competent and trust the effectiveness of protective actions are more inclined to adopt them. In the academic context, Alqahtani (2022) found that knowledge about cybersecurity practices—such as password strength, browser security, and social media management—significantly enhances students' cybersecurity awareness, indicating that education and training are effective strategies for improving coping appraisal. Overall, PMT provides a comprehensive framework for understanding the psychological drivers of protective behavior in the face of

cybersecurity threats and serves as a robust foundation for designing interventions aimed at enhancing security practices.

Theory of Planned Behavior

The Theory of Planned Behavior (TPB), introduced by Ajzen (1991), provides a theoretical framework for understanding and predicting human behavior, including cybersecurity-related actions. TPB posits that behavioral intention is the primary predictor of actual behavior and is shaped by three key constructs: attitude toward the behavior, subjective norms, and perceived behavioral control. Attitude refers to an individual's evaluation of the outcomes associated with a behavior; subjective norms involve perceived social pressure from others to perform or refrain from the behavior; and perceived behavioral control reflects the perceived ease or difficulty of performing the behavior, influenced by available resources and potential obstacles. In the cybersecurity context, TPB has been widely applied to explain how these factors influence individuals' intentions to adopt protective measures. For example, Zadeh et al. (2018) found that attitude, subjective norms, and perceived behavioral control positively affected students' intentions to use anti-malware software.

Similarly, Chandarman and Van Niekerk (2017) identified a gap between student attitudes and actual cybersecurity practices in South Africa. Farooq et al. (2019) reported that in Kenya, attitude significantly influenced students' intentions to engage in secure behaviors, while Ameen et al. (2020) demonstrated the role of attitude and subjective norms in shaping employees' intentions to implement cybersecurity measures in the UK, US, and UAE. McAlaney and Benson (2020) emphasized the critical role of social norms in influencing cybersecurity behavior, aligning with Ajzen's assertion that perceived behavioral control is essential for overcoming barriers to protective action. Zadeh et al. (2018) also highlighted that awareness, attitude, and subjective norms significantly contribute to students' intentions to adopt security software. Furthermore, Parikh and Nimbekar (2023) noted that students in India exhibited low levels of cybersecurity awareness, knowledge, and perception, indicating a need for greater education and outreach. By targeting positive attitudes, reinforcing supportive social norms, and enhancing perceived control, TPB offers a practical and flexible framework for promoting secure cybersecurity behaviors across diverse populations and cultural contexts.

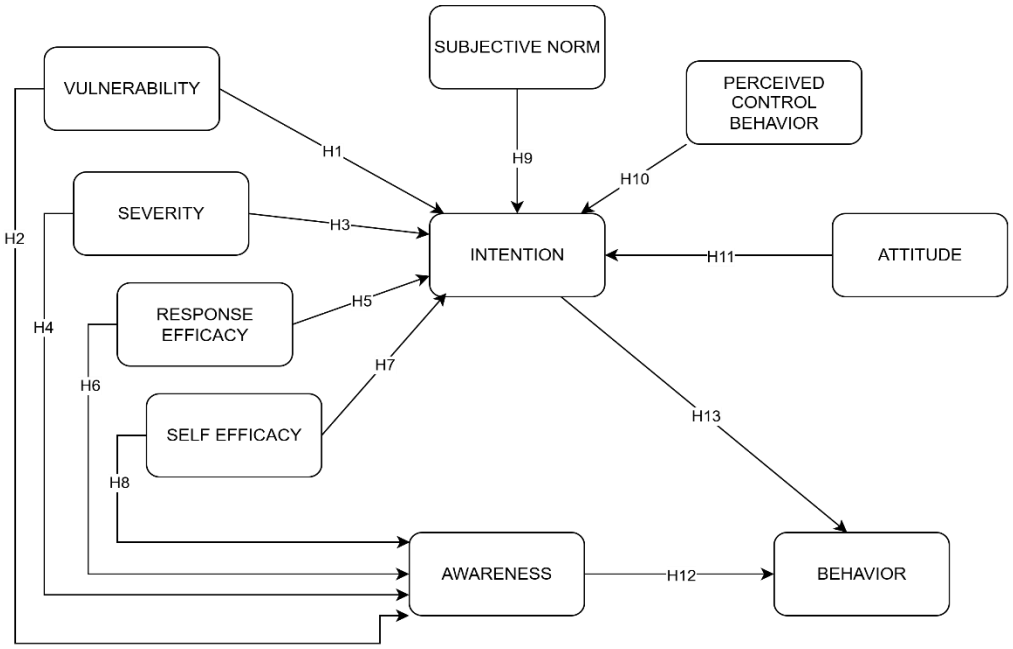

Figure 1
Integration Model of PMT and TPB

RESEARCH METHOD

This study was conducted at IPB University, Dramaga Campus, Bogor, from December 2024 to April 2025. Data were collected through an online survey using Google Forms, which was distributed to all faculties between February and March 2025. The instrument employed a 5-point Likert scale questionnaire to measure constructs such as cybersecurity awareness, threat perception, efficacy, attitude, and behavior. The Likert scale was chosen to allow respondents to express varying levels of agreement, including neutrality (Albaum, 1997). The sample was obtained using non-probability sampling with a voluntary response approach.

After data verification, 255 responses were deemed valid, exceeding the minimum respondent requirement based on the guideline of 5 to 10 times the number of structural paths in the SEM model (Hair et al., 2019). Descriptive analysis of respondents' characteristics—such as gender, age, faculty affiliation, and duration of digital device usage—was conducted using Microsoft Excel. Further analysis employed the Partial Least Squares Structural Equation Modeling (PLS-SEM) technique using SmartPLS 3.

The measurement model (outer model) was evaluated based on convergent validity (with AVE and outer loadings ≥ 0.7), reliability (Composite Reliability and Cronbach's Alpha ≥ 0.7), and discriminant validity using the Heterotrait-Monotrait ratio (HTMT), with a threshold of < 0.90. The structural model (inner model) was then analyzed through path coefficients, t-values, p-values (from bootstrapping), and R-squared values. Model fit was assessed using the Standardized Root Mean Square Residual (SRMR), with values below 0.08 indicating a good model fit.

RESULTS AND DISCUSSION

Respondent Characteristics

This study involved 255 IPB University students with diverse demographic and digital characteristics. The majority of respondents were under the age of 20 (61%) and predominantly enrolled in undergraduate programs (85.5%). In terms of gender, females made up 60.8% of the sample. The distribution across faculties was relatively balanced, with the Faculty of Economics and Management (FEM) and the Faculty of Forestry and Environment (FAHUTAN) contributing the largest shares of respondents (14.9% each). Most students reported high daily usage of digital devices, with 40% using them for 4–6 hours and 53% for more than 7 hours. Smartphones were the primary device used by 89% of participants, indicating a strong mobile-centric digital engagement. However, only 34.9% of respondents were aware of the university's cybersecurity policy, and 74.9% stated that they rarely received information on cybersecurity from IPB. This reveals a gap between the intensity of technology use and awareness of digital security issues, underscoring the need for systematic efforts to enhance cybersecurity literacy and communication among students.

Outer model evaluation

Based on the factor loadings presented in Table 1, all indicators demonstrated satisfactory convergent validity for their respective constructs. The Awareness construct (AWR1–AWR3) showed loading values ranging from 0.791 to 0.867, with AWR3 being the weakest but still above the acceptable threshold of 0.70. The Self-Efficacy and Response Efficacy constructs exhibited excellent indicator strength, with all loadings exceeding 0.80 and some, such as RE1 and RE2, surpassing 0.90. Similarly, the Severity and Vulnerability constructs reflected strong consistency, with loading values ranging from 0.777 to 0.886 and 0.830 to 0.929, respectively. For the Intention construct, all indicators showed loadings above 0.700. Indicators for Subjective Norms, Behavior, Perceived Behavioral Control, and Attitude also demonstrated strong contributions, with all loadings above 0.750. These results confirm that all indicators exhibit adequate convergent validity and are appropriate for use in further analyses, including construct reliability assessment and testing of relationships among latent variables in the structural model.

Table 1
Cross Loading

Variable	Indicator	Loading Factor	Status
Self-efficacy (SE)	SE1	0,808	Valid
	SE2	0,851	Valid
	SE3	0,840	Valid
Response Efficacy (RE)	RE1	0,915	Valid
	RE2	0,934	Valid
Severity (SVR)	SVR1	0,822	Valid
	SVR2	0,777	Valid
	SVR3	0,886	Valid
Vulnerability (VLR)	VLR1	0,929	Valid
	VLR2	0,830	Valid
	AWR1	0,791	Valid

Awareness (AWR)	AWR2	0,867	Valid
	AWR3	0,758	Valid
Intention (INT)	INT1	0,841	Valid
	INT2	0,850	Valid
	INT3	0,772	Valid
Subjective Norms (SN)	SN1	0,772	Valid
	SN2	0,771	Valid
	SN3	0,835	Valid
Behavior (BHV)	BHV1	0,819	Valid
	BHV2	0,834	Valid
	BHV3	0,827	Valid
Perceived Control Behavior (PBC)	PCB1	0,784	Valid
	PCB2	0,832	Valid
	PCB3	0,807	Valid
Attitude (ATT)	ATT1	0,787	Valid
	ATT2	0,833	Valid
	ATT3	0,774	Valid

The Composite Reliability (CR) values for all constructs exceeded 0.8, as shown in Table 2, indicating strong internal consistency and reliability in measuring the intended latent variables. Similarly, most Cronbach's Alpha (CA) values were above the acceptable threshold of 0.7, suggesting satisfactory internal consistency among indicators within each construct. Although the CA value for the Subjective Norm construct was relatively low (0.514), it remains acceptable due to the adequate CR value (0.803) and satisfactory Average Variance Extracted (AVE). According to Hair et al. (2019), CR is generally preferred over CA in the context of Structural Equation Modeling (SEM), particularly for reflectively measured constructs, as CR provides a more accurate assessment by accounting for the actual indicator loadings, which are often unequal. Furthermore, all constructs demonstrated AVE values above the minimum threshold of 0.50, indicating that more than half of the variance in the observed indicators is explained by their respective latent constructs.

Table 2
Construct Reliability

Variabel	Cronbach Alpha	rho_A	Composite Reliability	AVE	Ket.
Self-efficacy (SE)	0,782	0,793	0,872	0,694	Valid and Reliable
Response efficacy (RE)	0,831	0,84	0,922	0,855	Valid and Reliable
Severity (SVR)	0,779	0,832	0,868	0,688	Valid and Reliable
Vulnerability (VLR)	0,721	0,805	0,873	0,776	Valid and Reliable

Awareness (AWR)	0,73	0,74	0,848	0,650	Valid and Reliable
Intention (INT)	0,76	0,77	0,862	0,675	Valid and Reliable
Subjective norms (SN)	0,706	0,716	0,835	0,629	Valid and Reliable
Behavior (BHV)	0,77	0,773	0,866	0,684	Valid and Reliable
Perceived Control Behavior (PCB)	0,739	0,76	0,849	0,652	Valid and Reliable
Attitude (ATT)	0,716	0,716	0,840	0,637	Valid and Reliable

Based on the results of the Heterotrait-Monotrait Ratio (HTMT) analysis, all inter-construct values fell below the recommended thresholds—0.90 for conceptually distinct constructs and 0.85 for more conceptually similar constructs. This indicates that all constructs in the model exhibit adequate discriminant validity, confirming that each construct measures a unique conceptual domain without significant overlap. The highest HTMT values were observed between Intention (INT) and Attitude (ATT) at 0.672, and between Intention and Subjective Norms (SN) at 0.732.

Although these constructs are theoretically interrelated within the Theory of Planned Behavior (TPB), the HTMT values remain below the critical thresholds, supporting their discriminant distinction. Conversely, very low HTMT values, such as between Severity (SVR) and Self-Efficacy (SE = 0.126) or Vulnerability (VLR = 0.128) suggest a clear empirical separation between those constructs. These findings confirm that discriminant validity has been established, providing a solid foundation for subsequent structural path analysis**.**

Table 3
Heterotrait-Monotrait Ratio

	SE	**RE**	**SVR**	**VLR**	**AWR**	**INT**	**SN**	**BHV**	**PCB**	**ATT**
SE										
RE	0.409									
SVR	0.126	0.105								
VLR	0.680	0.320	0.128							
AWR	0.598	0.318	0.200	0.246						
INT	0.292	0.456	0.214	0.208	0.589					
SN	0.390	0.438	0.359	0.394	0.423	0.665				
BHV	0.522	0.427	0.243	0.310	0.690	0.707	0.547			
PCB	0.650	0.557	0.118	0.427	0.642	0.489	0.450	0.496		
ATT	0.232	0.322	0.368	0.113	0.364	0.631	0.584	0.540	0.413	

Inner Model Evaluation

Table 4
Path Coefficient

Hypothesis	Path	Coefficient (O)	T-Statistic	P-Value	Significant
H1	Perceived Vulnerability → Intention	-0.018	0.351	0.726	Not Significant
H2	Perceived Vulnerability → Awareness	-0.068	1.057	0.290	Not Significant
H3	Perceived Severity → Intention	-0.013	0.261	0.794	Not Significant
H4	Perceived Severity → Awareness	0.143	3.019	0.003	**Significant**
H5	Response Efficacy → Intention	0.146	2.438	0.015	**Significant**
H6	Response Efficacy → Awareness	0.105	1.527	0.127	Not Significant
H7	Self-Efficacy → Intention	-0.016	0.252	0.801	Not Significant
H8	Self-Efficacy → Awareness	0.458	6.606	0.000	**Significant**
H9	Subjective Norm → Intention	0.295	4.768	0.000	**Significant**
H10	Perceived Behavioral Control → Intention	0.144	2.285	0.022	**Significant**
H11	Attitude → Intention	0.277	4.150	0.000	**Significant**
H12	Cybersecurity Awareness → Cybersecurity Behavior	0.354	6.938	0.000	**Significant**
H13	Intention → Cybersecurity Behavior	0.392	6.828	0.000	**Significant**

The structural model analysis revealed several significant relationships among the latent variables. Within the Theory of Planned Behavior (TPB) framework, attitude ($\beta = 0.277$; $t = 4.150$; $p < 0.001$), subjective norms ($\beta = 0.295$; $t = 4.768$; $p < 0.001$), and perceived behavioral control ($\beta = 0.144$; $t = 2.285$; $p = 0.022$) significantly influenced intention. In the Protection Motivation Theory (PMT) domain, response efficacy ($\beta = 0.146$; $t = 2.438$; $p = 0.015$) had a significant effect on intention, while self-efficacy ($\beta = 0.458$; $t = 6.606$; $p < 0.001$) and perceived severity ($\beta = 0.143$; $t = 3.019$; $p = 0.003$) significantly predicted cybersecurity awareness. However, perceived vulnerability showed no significant effect on either awareness or intention ($p > 0.05$), and neither did self-efficacy and response efficacy in their direct paths to intention. These results suggest that although not all PMT components (e.g., vulnerability and self-efficacy) directly influence intention, they remain vital by enhancing awareness, which plays a crucial mediating role.

This aligns with the core premise of PMT (Rogers, 1975), which emphasizes the importance of threat appraisal and coping appraisal in motivating protective behavior. Intention was found to have a strong effect on cybersecurity behavior ($\beta = 0.392$; $t = 6.828$; $p < 0.001$), reinforcing its central role in behavioral execution. Notably, the non-significant effect of self-efficacy on intention may reflect overconfidence, where individuals believe they have already taken sufficient protective actions and thus lack further motivation—a finding consistent with Bekker et al. (2023). Similarly, the non-significance of perceived vulnerability contrasts with Hassandoust and Techatassanasoontorn (2020), who suggested a

reciprocal link between awareness and vulnerability perception. In this study, vulnerability failed to drive greater awareness or preparedness for cyber threats. Overall, the findings underscore the key roles of awareness, attitude, subjective norms, and perceived severity in shaping cybersecurity intentions and behaviors, while indicating that factors such as self-efficacy, perceived control, and vulnerability may have more complex or indirect influences.

Table 5
Coefficient Determination

Variable	R^2	R^2 Adjusted
Awareness	0,247	0,235
Intention	0,376	0,359
Behavior	0,399	0,394

The coefficient of determination (R^2) reflects the explanatory power of the model toward the dependent variables. In this study, constructs from the Protection Motivation Theory (PMT) account for 24.7% of the variance in cybersecurity awareness ($R^2 = 0.247$), which is categorized as weak to moderate (Chin, 1998). This implies that awareness is influenced not only by perceptions of threat and self-efficacy but also by external factors such as prior experience, education, or institutional policies. The intention to engage in secure behavior has a moderate R^2 value of 0.376, indicating the significant predictive contribution of TPB constructs—namely, attitude, subjective norms, and perceived behavioral control. Furthermore, the cybersecurity behavior variable shows an R^2 of 0.399, suggesting that awareness and intention collectively explain nearly 40% of its variance, while the remainder may be attributed to unmeasured external factors such as environmental constraints, habitual behavior, or lack of enforcement.

Table 6
Goodness of Fit Index

	Saturated Model	Estimated Model	Note
SRMR	0,068	0,086	< 0,10, Fit

In terms of model fit, the Standardized Root Mean Square Residual (SRMR) value of 0.086 falls below the recommended threshold of 0.10, indicating an acceptable model fit and validating the model's internal consistency for further analysis (Ghozali, 2019). Other fit indices such as d_ULS and d_G support this assessment, although they lack established cutoff values in PLS-SEM.

Implications

The findings of this study offer strategic implications for enhancing cybersecurity behavior among university students, particularly within the context of IPB. Theoretically, the results support the validity of integrating the Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) in explaining the determinants of cybersecurity intentions and behaviors. Constructs such as awareness, attitude, subjective norms, and perceived behavioral control were found to significantly influence intention and behavior, indicating that secure behavior is shaped not only by cognitive assessments but also by social influences and self-belief. Practically, the study highlights three key areas for intervention: (1) fostering positive attitudes toward cybersecurity through educational campaigns emphasizing the importance of personal data protection and digital risk awareness; (2) strengthening

subjective norms by leveraging peer, lecturer, and student organization influences to promote secure practices; and (3) enhancing students' perceived control and self-efficacy through accessible training modules and hands-on cybersecurity exercises.

Additionally, the direct influence of awareness on behavior underscores the need for awareness programs that go beyond merely disseminating information, instead focusing on sustainable and contextualized engagement that can lead to tangible behavioral outcomes. Institutional units such as IPB's LMITD, Directorate of Student Affairs, and faculty-level stakeholders can utilize these findings to design targeted policies, curricula, and training programs grounded in empirical evidence.

CONCLUSION

This study demonstrates that cybersecurity behavior among IPB university students is influenced by a combination of psychological factors and awareness levels. From the perspective of the Theory of Planned Behavior (TPB), attitude, subjective norms, and perceived behavioral control significantly influence the intention to engage in secure behavior. Meanwhile, within the framework of Protection Motivation Theory (PMT), self-efficacy significantly affects cybersecurity awareness, whereas perceived vulnerability does not show a meaningful impact. Both awareness and intention are confirmed as significant predictors of actual cybersecurity behavior. Enhancing self-efficacy and fostering strong behavioral intentions emerge as key strategies in promoting secure digital practices.

Accordingly, it is recommended that IPB develop cybersecurity literacy programs that go beyond informative approaches by incorporating practical training, integrating cybersecurity topics into academic activities, and fostering social norms that support secure behavior. Future research is encouraged to expand the model by including additional variables such as prior cyber incident experience or technological background and to employ qualitative or longitudinal methods to gain deeper insights. Furthermore, exploring alternative theoretical frameworks may offer new perspectives on the determinants of cybersecurity behavior among students.

REFERENCES

Ajzen, I. 1991. *The Theory of Planned Behavior*. Organizational Behavior and Human Decision Processes. 50(2):179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Aldawood, H., dan Skinner, G. 2020. *Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions*. IEEE Access, 8, 67321-67329. DOI: 10.1109/ACCESS.2020.2983280

Alqahtani, M. A. 2022. *Factors Affecting Cybersecurity Awareness among University Students*. Applied Sciences. 12(5):2589. https://doi.org/10.3390/app12052589

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., dan Choudrie, J. 2020. *Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce*. Computers in Human Behavior. 106531. https://doi.org/10.1016/j.chb.2020.106531

Bekkers, L., van Hoff-de G. S., Misana E. Y., Van Y. S., Spithoven, R., dan Leukfeldt, E. 2023. *Protecting your business against ransomware attacks: Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model*. Computers & Security. 127:103099. https://doi.org/10.1016/j.cose.2023.103099

Chandarman, R., dan van Niekerk, B. 2017. *Students Cybersecurity Awareness at a Private Tertiary Educational Institution*. The African Journal of Information and Communication (AJIC). 20:133-155. DOI:10.23962/10539/23572

Chowdhury, N. H., Adam, M. T., dan Teubner, T. 2020. *Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures*. Computers and Security. 97:101963. https://doi.org/10,1016/j.cose.2020,101963

[CNBC] 2022 Des 26. *Hacker Bjorka Tantang Pemerintah RI: Saya Menunggu Digerebek!*. CNBC Indonesia. https://www.cnbcindonesia.com/tech/20221226135118-37-400166/hacker-bjorka-tantang-pemerintah-ri-saya-menunggu-digerebek

[CNN] 2017 Okt 4. *Seluruh Data Pengguna Yahoo Telah Diretas Pada 2013*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20171004084050-185-245977/seluruh-data-pengguna-yahoo-telah-diretas-pada-2013

Conetta, C. 2019. *Individual Differences in Cyber Security*. McNair Research Journal SJSU. 15. https://doi.org/10,31979/mrj.2019,1504

[Databoks] 2024. *Teknologi dan Komunikasi*. Databoks Indonesia. https://databoks.katadata.co.id/category/86/teknologi-telekomunikasi

Fatokun, F. B., Hamid, S., Norman, A., dan Fatokun, J. O. 2019. *The Impact of Age, Gender, and Educational level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical investigation on Malaysian Universities*. Journal of Physics: Conference Series. 1339(1):012098. https://doi.org/10,1088/1742-6596/1339/1/012098

[Badan Siber dan Sandi Negara]. 2024. *Lanskap Keamanan Siber Indonesia*. https://www.bssn.go.id/monitoring-keamanan-siber/

Hadlington, L. 2017. *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. Heliyon. 3(7):e00346. https://doi.org/10,1016/j.heliyon.2017.e00346

Hair, J.F., Black, W.C., Babin, B.J., dan Anderson, R.E. 2019. *Multivariate Data Analysis*. Ed ke-8. Cengage.

Hong, W. C. H., Chi, C., Liu, J., Zhang, Y., Lei, V. N., dan Xu, X. 2022. *The influence of social education level on cybersecurity awareness and behaviour: a comparative study of university students and working graduates*. Education and Information Technologies. 28:439–470. https://doi.org/10,1007/s10639-022-11121-5

Ifinedo, P. 2012. *Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory*. Computers & Security. 31(1):83–95. https://doi.org/10,1016/j.cose.2011,10,007

Kalhoro, S., Rehman, M., Ponnusamy, V.A.P., dan Shaikh, F.B. 2021. *Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review*. IEEE Access, 9, 99339-99363. Doi: 10.1109/ACCESS.2021.3097144

Kont, K. R. 2024. *Cybersecurity behaviours of the employees and students at the Estonian Academy of Security Sciences*. Organizational Cybersecurity Journal: Practice, Process and People. https://doi.org/10.1108/OCJ-02-2024-0001

Kovacevic, A., Putnik, N., dan Toskovic, O. 2020. *Factors Related to Cyber Security Behavior*. IEEE Access. 8:125140–125148. https://doi.org/10,1109/ACCESS.2020,3007867

Li, L., Xu, L., dan He, W. 2022. *The effects of antecedents and mediating factors on cybersecurity protection behavior*. Computers in Human Behaviour Reports. 5:100165. https://doi.org/10,1016/j.chbr.2021,100165

McAlaney, J., dan Benson, V. 2020. *Cybersecurity as a social phenomenon*. Dalam: Cruz-Cunha M, editor. Cyber Influence and Cognitive Threats. Academic Press. hlm 1–8. https://doi.org/10,1016/B978-0-12-819204-7,00001-4

Moustafa, A. A., Bello, A., dan Maurushat, A. 2021. *The Role of User Behaviour in Improving Cyber Security Management*. Frontiers in Psychology. 12:561011. https://doi.org/10,3389/fpsyg.2021,561011

Parikh, V., dan Nimbekar, M. 2023. *Socializing the impact: An analysis of the theory of planned behavior's influence on increasing university students' cybersecurity awareness*. Journal of Community Development. 4(2):139-156. https://doi.org/10.47134/comdev.v4i2.162

Patterson, W., dan Winston, C. E. 2019. *Behavioral Cybersecurity: Applications of Personality Psychology and Computer Science*. Taylor and Francis, CRC Pr.

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., dan Guerri, D. 2022. *Leveraging human factors in cybersecurity: An integrated methodological approach*. Cognition, Technology and Work. 24:371–390. https://doi.org/10,1007/s10111-021-00683-y

Rogers, R.W. 1975. *A protection motivation theory of fear appeals and attitude change*. Journal of Psychology. 91(1):93–114.

Solms, B.V., dan Solms, R. V. 2018. *Cybersecurity and information security – what goes where?*. Information and Computer Security. 26(1):2–9. https://doi.org/10,1108/ics-04-2017-0025

Wiechetek, L., dan Medrek, M. 2022. *Human Factors in Security – Cybersecurity Education and Awareness of Business Students*. Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia. 56(1). https://doi.org/10,17951/h.2022,56,1.119-142

Zadeh, A. V., Thurasamy, R., dan Hanifah, H. 2018. *Modeling anti-malware use intention of university students in a developing country using the theory of planned behavior*. Kybernetes. https://doi.org/10,1108/K-05-2018-0226

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., dan Basim, H. N. 2020. *Cyber Security Awareness, Knowledge and Behavior: A Comparative Study*. Journal of Computer Information Systems, 1–13. https://doi.org/10,1080/08874417,2020,1712269