Volume 5 Issue 2 (2025) Pages 1638-1656
Amkop Management Accounting Review (AMAR)
ISSN: 2828-2248 (Online)

The Gap Between Cybersecurity Experience and Behavior: A Case Study of Digital Native Students at the University of Papua

Camelia Lusandri Numberi ✉ Marlina Malino [2] Redemptus Numba Nitu Nua [3] Jenita Sumari [4]

✉[2,3,4] *Program Studi Akuntansi, Universitas Papua, Indonesia*

Abstract

The purpose of this study is to analyze the influence of awareness, knowledge, experience, and compliance on students' digital security behavior at the University of Papua, in the context of social media use. This study conceptualizes digital security behavior as a behavioral phenomenon shaped by psychological factors and social norms within the Theory of Reasoned Action. A quantitative approach with a survey method was employed. Data were collected through a structured questionnaire distributed to active students who regularly use social media and were analyzed using multiple linear regression. The research instrument was developed based on indicators validated in previous studies and was subjected to validity and reliability testing before the primary analysis. The findings indicate that awareness, knowledge, and compliance have a positive and significant effect on students' digital security behavior, whereas experience does not. These results reinforce the relevance of the Theory of Reasoned Action, particularly the role of attitudes and subjective norms in shaping digital security actions. Although students exhibit a relatively high level of awareness, gaps remain in terms of applied knowledge and practical skills. This study offers important implications for the development of digital security literacy in higher education institutions. Universities are encouraged to design practice-oriented, norm-based educational interventions and to integrate digital security into curricula and systematic training programs to foster sustainable digital security behavior among students.

Keywords: *Cybersecurity Awareness; Digital Behavior; Social Media Security; Information Security Literacy; Cybersecurity Education.*

✉ Corresponding author :
Email Address: camelialusandri@gmail.com

INTRODUCTION

Advances in information and communication technology over the past two decades have driven a significant transformation in how individuals interact, communicate, and build social relationships, particularly through social media. In Indonesia, social media has become a primary social space that serves not only as a means of communication but also as a medium for identity formation, network expansion, and public opinion expression. The growing intensity of social media use

DOI: 10.37531/amar.v5i2.3464

has serious consequences, including increased cybersecurity risks. Threats such as phishing, account hacking, online fraud, and personal data leaks are becoming more frequent and leaving social media users vulnerable, especially students who belong to the digital-native generation with very high levels of digital activity (Bada et al., 2021; Ifinedo et al., 2022). The relevance of this phenomenon is further reinforced by national data showing that Indonesia had 167 million active social media users as of January 2023, reflecting the public's high exposure to potential cyber threats in their daily lives (We Are Social, 2023). On the other hand, the increase in the number of users and the intensity of digital interactions is not matched by adequate security preparedness. Although digital literacy in general shows an upward trend, awareness and practices of digital security, particularly in terms of personal data protection, the use of secure authentication, and digital identity management, are still uneven among social media users (Iskandar et al., 2025). Students are often not fully aware of the consequences of their actions in the digital space, such as the use of weak passwords and low awareness of social engineering tactics, thereby increasing their vulnerability to cybercrime (Taha et al., 2025). This phenomenon points to a practical and theoretical problem: a gap between the intensity of social media use and cybersecurity readiness.

Therefore, this research is necessary to gain a deeper understanding of the basis of students' cybersecurity behavior as active social media users. The state of the art in cybersecurity research on digital users reveals a consistent paradox: a gap between awareness and protective behavior. Several studies confirm that cybersecurity awareness variables are often at an adequate level, but do not automatically result in commensurate protective actions.

Zwilling et al. (2022) found that internet users understand cyber threats but only apply minimal protection tools. A similar pattern is seen in the digital-native group, as Kovačević et al. (2020) noted that even technologically active students "do not behave safely" despite their identity as the digital generation. These findings clarify that awareness, as a cognitive variable, can stand apart from behavior, as an implementative variable. On the variable of knowledge or understanding of threats, empirical evidence also shows that sufficient understanding does not always trigger decisive preventive actions. Shukla et al. (2022) show that although internet users have an adequate understanding of cyber threats, they still take only minimal preventive measures. In fact, Barth et al. (2022) found that cybersecurity experts exhibit behavior patterns similar to those of laypeople, confirming that this gap extends beyond technical knowledge. Cross-population studies reinforce the generalization of this phenomenon, including among 579 business professionals by Li et al. (2019) and 268 respondents from various age groups by Cain et al. (2018), as well as a cross-country sample highlighting the main barriers of perceived response costs, lack of practical guidance, and limited organizational support. Another important nuance emerges in the individual factors that influence behavior: Branley-Bell et al. (2022) emphasize the roles of age and self-efficacy in security practices, while Kannelønning & Katsikas (2023) highlight the limitations of subjective self-reporting, which can obscure the mapping of behavioral gaps.

Although recent studies have successfully identified gaps between awareness, knowledge, and cybersecurity behavior, they still face significant limitations from both empirical and theoretical perspectives. Empirically, most previous studies have tested cybersecurity variables separately, such as awareness and knowledge, without simultaneously integrating them with personal experience and compliance with

DOI: 10.37531/amar.v5i2.3464

security practices. This partial approach has led to a fragmented understanding of the mechanisms that shape cybersecurity behavior, making it difficult to explain why individuals who are aware of and understand the risks continue to exhibit unsafe behavior. In addition, many studies rely on survey designs that rely on subjective self-reporting, which can lead to perception bias and undermine the accuracy of describing users' actual behavior in the digital space. From a theoretical perspective, the existing literature is still relatively limited in linking cybersecurity behavior gaps to a comprehensive behavioral theory framework. Many studies are descriptive and focus on identifying barriers, such as perceived costs or limited organizational support, without explaining the cognitive and social processes underlying the transition from awareness to action. In addition, the context of social media use as the primary environment for digital interaction has often not been the focus of in-depth analysis, even though its characteristics entail distinct risk dynamics compared to other digital activities. This gap is even more apparent in the local context, especially in universities in eastern Indonesia, which have rarely been explored in cybersecurity research.

Based on the empirical and theoretical gaps identified, the novelty of this study lies in its integrative approach, which simultaneously analyzes the relationships among awareness, knowledge, experience, and compliance with digital security practices to explain students' cybersecurity behavior when using social media. Unlike previous studies, which tend to be partial and descriptive, this study frames cybersecurity behavior as the result of structured cognitive and social processes by adopting the Theory of Reasoned Action as its main conceptual framework. This approach allows for a more in-depth explanation of how attitudes, subjective norms, and behavioral intentions shape students' actual actions in the face of cyber threats. In addition, this study specifically examines the local context of Papuan University students, which has received minimal attention in cybersecurity studies to date, thereby providing contextual empirical contributions and enriching the literature, which has been dominated by studies in urban areas and developed countries. The purpose of this study is to identify the dominant factors that influence students' cybersecurity behavior in the use of social media and to explain the gap between experience and digital security behavior, so that the results can be used as a basis for developing more effective cybersecurity education and policy strategies that are in line with the characteristics of digital native users in a university environment.

Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA) is a behavioral theory that explains individual actions as the result of rational reasoning, in which behavior is seen as a direct consequence of consciously formed behavioral intentions. Within the TRA framework, behavioral intentions are influenced by two main determinants: individuals' attitudes toward the behavior and the subjective norms perceived from the social environment. Gopinathan et al. (2025) emphasize that TRA views individuals as rational agents who systematically evaluate the consequences of an action before deciding to act, so that behavior does not arise spontaneously, but rather through structured cognitive and social considerations. This view positions intention as a conceptual bridge between internal factors and actual behavior, making TRA widely used to predict planned behavior, including in the context of technology adoption and digital practices. In their empirical study, Gopinathan et al. (2025) show

DOI: 10.37531/amar.v5i2.3464

that relationships among attitudes, subjective norms, and behavioral intentions can significantly explain behavioral variation, confirming the TRA's predictive power in understanding consciousness-based actions. Similar findings are reinforced by Concari et al. (2023), who explain that attitudes toward a behavior and normative pressure from the social environment are the primary motivators of intention formation, both in environmental and technological contexts.

The development of TRA studies after 2018 shows that this theory continues to have high explanatory power and is still used in various modern behavioral contexts, especially those related to technology and digital communication. Paraskevi et al. (2023) demonstrate that TRA is effective in modeling individual behavioral intentions regarding the use of digital services, emphasizing that attitudes toward technology and social norms surrounding users play a central role in shaping these intentions. This study confirms that TRA remains relevant amid the complexity of contemporary digital behavior, as it continues to capture the social and cognitive dynamics that influence individual decisions. Conceptually, Prachaseree et al. (2021) expand on TRA by emphasizing that, although this theory is parsimonious, its structure is flexible enough to be elaborated without losing the core of behavioral rationality. This elaboration shows that TRA can serve as a solid theoretical foundation for understanding various forms of human action, provided the primary focus remains on the relationships among attitudes, subjective norms, and intentions. In the context of digital behavior, umbrella articles discussing the use of TRA as a framework for analyzing technological behavior confirm that this theory is well-suited to explain behaviors involving conscious consideration, such as the use of information systems and digital interactions (Rachmadana et al., 2024). This body of literature shows that TRA is not merely a classical theory but a continually updated conceptual framework applied to understand human behavior in the digital age.

Cybersecurity Awareness

Cybersecurity awareness is the level of understanding, vigilance, and preparedness of individuals to recognize cyber threats and implement appropriate protection practices to maintain the security of information and digital identities. This concept emphasizes that cybersecurity is not merely a technical issue but also a human one, related to how individuals perceive risks, assess consequences, and form habits in their interactions with digital technology. Within this framework, cybersecurity awareness includes recognizing threats such as phishing, malware, and identity theft, understanding the basic mechanisms of attacks, and recognizing the importance of preventive measures in daily digital activities. Taherdoost (2024) emphasizes that cybersecurity awareness must be understood as a continuous learning process, in which individuals actively build a conceptual understanding of cyber risks and relate them to the real situations they encounter. This view places awareness as a cognitive foundation that enables individuals to make rational judgments about digital threats.

In line with this, Shillair et al. (2022) view cybersecurity awareness as an integral part of a broader digital security ecosystem. In this education, awareness campaigns, and the institutional environment shape how individuals understand and respond to risks. Furthermore, cybersecurity awareness has a behavioral dimension that is closely related to human factors and organizational context.

DOI: 10.37531/amar.v5i2.3464

Awareness does not stop at conceptual understanding, but develops into a mental readiness to act safely in various digital situations. Neri et al. (2024) explain that the core of cybersecurity awareness lies in individuals' ability to align security knowledge with real habits and practices, so that security policies or guidelines are not only understood normatively but also implemented consistently. In this context, awareness serves as an internal mechanism that guides individuals to comply with information security principles without relying solely on external supervision. Kavak (2024) reinforces this understanding by showing that cybersecurity awareness is closely related to compliance with digital security rules and procedures, as risk-aware individuals tend to view security practices as a necessity rather than a burden. In an educational environment, cybersecurity awareness is also related to an individual's ability to perceive threats as personally relevant and closely tied to their digital activities. Khan et al. (2023) emphasize that awareness built through risk understanding and protection motivation will increase an individual's readiness to address cyber threats proactively.

Cybersecurity Knowledge

Cybersecurity knowledge is an individual's conceptual and technical understanding of the principles, mechanisms, and practices for protecting information systems and digital data from various cyber threats. This knowledge includes an understanding of threat types such as malware, phishing, network-based attacks, and vulnerability exploitation, as well as mitigation measures such as password management, multi-factor authentication, encryption, and privacy settings. Švábenský et al. (2021) assert that cybersecurity knowledge is not singular but instead comprises conceptual knowledge that explains "why" a threat occurs and procedural knowledge that explains "how" to protect oneself and one's systems. In this framework, knowledge functions as a cognitive map that helps individuals interpret digital situations and make appropriate decisions when faced with risks. Khan et al. (2023) place cybersecurity knowledge as the result of a process of threat evaluation and protection capability assessment, in which individuals build understanding through cognitive mechanisms that weigh the severity of risks and the effectiveness of responses. Thus, knowledge is not only static information, but is also formed through a reasoning process that allows individuals to connect security concepts with the dynamic context of technology use. An et al. (2023) add that the structure of cybersecurity knowledge is influenced by cognitive capacity and educational background, leading to differences in depth and breadth of understanding across individuals.

Cybersecurity knowledge is integrative, as it intersects with organizational practices, policies, and the context of technology use. Pigola et al. (2025) explain that cybersecurity knowledge does not stand alone at the individual level but is integrated into a broader information security management system, where knowledge serves as a strategic resource for decision-making and policy enforcement. In this perspective, knowledge includes an understanding of security standards, procedures, and frameworks that guide the consistent use and protection of technology. Oroni et al. (2025) reinforce this understanding by placing cybersecurity knowledge as an important component in the digital learning environment, where adequate understanding enables individuals to recognize the implications of security policies

DOI: 10.37531/amar.v5i2.3464

and translate them into appropriate practices. Knowledge, thus, acts as a bridge between formal rules and operational actions, as individuals who understand the rationale behind policies tend to interpret security as a functional necessity rather than merely an administrative obligation. On the other hand, Khan et al. (2023) emphasize that the quality of cybersecurity knowledge is determined by its ability to motivate effective protective responses, so that good knowledge must be relevant, contextual, and applicable. This aligns with the mapping by Švábenský et al. (2021), which shows that fragmented knowledge without a complete conceptual understanding can limit an individual's ability to address complex threat scenarios.

Cybersecurity Experience

Cybersecurity experience is defined as the accumulation of individual or organizational involvement in facing, handling, or recognizing events related to digital security threats and incidents, either directly or indirectly. This experience includes exposure to incidents such as phishing, account hacking, data leaks, and privacy violations, as well as routine interactions with security mechanisms, including authentication, warning systems, and incident response procedures. Within a conceptual framework, cybersecurity experience shapes practical understanding that is not always gained through formal learning, but through reflective processes on real events in the digital environment. Bishop et al. (2025) emphasize that practical experience and involvement are core elements in building individuals' understanding of cyber risks, as experience allows individuals to relate security concepts to real consequences they have encountered. In other words, experience serves as a bridge between abstract knowledge and the operational reality of cybersecurity. This view is consistent with the findings of Patterson et al. (2023), who identify incident experience as the primary source of learning in cybersecurity, as direct interaction with incidents encourages the reevaluation of previously held security practices and assumptions. Through experience, cyber threats are no longer perceived as a distant possibility but as a concrete risk that demands attention and preparedness. Reuben-Owoh & Haig (2025) reinforce this understanding by showing that recurring incident patterns, such as phishing and social engineering attacks, shape the collective experience of users and organizations in dealing with dynamic threats.

Cybersecurity experiences have cognitive and affective dimensions that influence how individuals respond to digital security challenges. Experience not only creates practical understanding but also shapes perceptions, awareness, and sensitivity to signs of threats. Baltuttis et al. (2024) show that different security behavior patterns can be traced to variations in professional and prior experience with risky situations, suggesting that experience shapes individuals' response styles to cyber threats. In this context, experience can be active, such as direct involvement in incident handling, or passive, such as witnessing or hearing about the consequences of incidents experienced by others. Acheampong et al. (2025) emphasize that users' experiences with security mechanisms, including interactions with security protocols and protection systems, also influence how individuals perceive the balance between security, usability, and convenience. Experiences perceived as complicated or disruptive can shape perceptions of digital security, while experiences considered relevant and contextual can increase awareness of the importance of protection. Bishop et al. (2025) reiterate that cybersecurity experience must be understood as a continuous

DOI: 10.37531/amar.v5i2.3464

process, in which every interaction with threats or security systems enriches an individual's framework for thinking about future risks. From a broader perspective, cybersecurity experience is also cumulative and contextual, influenced by the technological environment, organizational culture, and the characteristics of the system in use.

Compliance with Digital Security Practices

Compliance with digital security practices is the degree to which individuals follow the rules, policies, procedures, and standards established to protect information systems and digital data from various cyber threats. The concept of compliance emphasizes that digital security depends not only on the existence of formal policies but also on the extent to which these policies are internalized and implemented in daily activities. Alraja et al. (2023) view compliance as a form of behavior that reflects an individual's acceptance of information security policies, arising when individuals understand the purpose of the rules and view them as a rational protection mechanism. In this perspective, compliance is not passive, but rather the result of cognitive and normative processes that shape an individual's orientation towards digital security. Vedadi et al. (2024) expand on this understanding by framing information security compliance as part of organizational citizenship behavior, a voluntary behavior that goes beyond formal obligations. This view emphasizes that compliance should ideally not be driven by fear of sanctions, but rather by an intrinsic commitment to maintaining collective security.

Compliance with digital security practices also has psychological and contextual dimensions that influence how individuals respond to security demands. Yazdanmehr et al. (2023) explain that information security compliance activities can create psychological pressure, especially when procedures are perceived as complex or burdensome. Therefore, compliance cannot be separated from individuals' subjective experiences in implementing security practices, as perceptions of burden and benefits will influence the sustainability of compliant behavior. Xu et al. (2024) emphasize that effective compliance is not only reactive but also proactive, where individuals consciously and voluntarily take security measures even without direct encouragement from formal rules. In this context, compliance is understood as an individual's readiness to act in accordance with security principles in their work habits and digital interactions. Social and leadership factors also play an important role in shaping compliance. Tejay & Winkfield (2025) show that a leadership approach that emphasizes exemplary behavior, support, and communication of security values can create a stronger climate of compliance than a coercive approach. This confirms that compliance with digital security practices is a social construct influenced by norms, expectations, and organizational culture.

METHODOLOGY

This study uses a quantitative approach, with a survey design, as its primary method for collecting empirical data. The quantitative approach was chosen because it allows for objective, structured, and standardized measurement of variables, enabling statistical analysis of their relationships. The survey design was used to capture respondents' perceptions, attitudes, and behaviors regarding digital security

DOI: 10.37531/amar.v5i2.3464

practices in the context of social media use. This study is explanatory in nature, aiming not only to describe the phenomenon but also to explain the cause-and-effect relationships among the variables of awareness, knowledge, experience, and compliance with digital security measures among students. The study's conceptual framework is based on the Theory of Reasoned Action (TRA), which views behavior as the result of attitudes and subjective norms that influence an individual's intentions and actual actions. Thus, this research design aims to empirically examine how cognitive, psychological, and normative factors contribute to students' digital security behavior.

The population in this study consisted of all active students at the University of Papua who regularly use social media for academic and social activities. This population included students from various faculties and study programs, representing diverse academic, social, and cultural backgrounds. The sampling technique used was purposive sampling, which involves selecting respondents based on specific criteria relevant to the research objectives. These criteria included active student status, intensity of social media use, and willingness to participate in the study. The sample size was determined using the Slovin formula with a 5 percent margin of error, resulting in a minimum of 100 student respondents. This sample size was considered adequate for multiple linear regression analysis and capable of reflecting the characteristics of the study population.

Data collection was conducted through the distribution of a closed-ended structured questionnaire. The questionnaire was developed based on indicators validated in previous studies relevant to cybersecurity and student digital behavior. The research instrument consisted of two main sections. The first section contained demographic questions, including age, gender, faculty status, and frequency of social media use. The second section consisted of 25 statements that measured four primary constructs, namely cybersecurity awareness, cybersecurity knowledge, cybersecurity experience, and compliance with digital security practices, as well as digital security action variables as dependent variables. Each item is measured using a five-point Likert scale, ranging from strongly disagree to agree strongly. Before widespread use, the instrument was tested in a pilot study of 30 respondents to ensure its validity and reliability. The validity test results showed that all items met the validity criteria. In contrast, the reliability test showed a Cronbach's Alpha value above the minimum required limit, so the instrument was declared suitable for use.

The collected data were analyzed using multiple linear regression techniques to test the simultaneous and partial effects of independent variables on dependent variables. Before regression analysis, the data were tested using classical assumption tests to assess the validity of the statistical model. A normality test was conducted to ensure the data were normally distributed, a multicollinearity test was used to identify high correlations among independent variables, a heteroscedasticity test was conducted to assess the uniformity of residual variance, and an autocorrelation test was used to assess residual independence. All statistical analyses were performed using the latest version of SPSS software. The coefficient of determination value was used to measure the overall contribution of independent variables to the dependent variable. In contrast, the significance value was used to determine the strength of each variable's partial influence. Through this analytical approach, the study is expected to provide an accurate empirical description of the factors that influence students' digital security actions.

DOI: 10.37531/amar.v5i2.3464

RESULTS AND DISCUSSION

Results

Respondent Description and Data Distribution

This study involved 100 students from the University of Papua, selected through purposive sampling. Table 1 shows that most respondents were 21 years old (31%), followed by 20 years old (26%) and 22 years old (20%). Based on gender, 56% were females and 44% were males (Table 2). In terms of faculty distribution (Table 3), most respondents came from the Faculty of Teacher Training and Education (34%), followed by the Faculty of Engineering (27%), and the Faculty of Agriculture (20%).

Table 1. Characteristics of Research Respondents (n = 100)

Respondent Characteristics	Category	Frequency	Percentage
Age	20 years	26	26%
	21 years	31	31%
	22 years	20	20%
	> 22 years	23	23%
Gender	Man	44	44%
	Man	56	56%
Faculty	Teaching and Education	34	34%
	Technique	27	27%
	Agriculture	20	20%
	Others	19	19%

Based on Table 1, the respondents' characteristics indicate that the majority were in their early twenties. The 21-year-old age group was the largest, accounting for 31 percent, followed by 20-year-olds at 26 percent and 22-year-olds at 20 percent. Meanwhile, respondents aged 22 years or older accounted for 23 percent. This age distribution indicates that the respondents were dominated by students in the active phase of using digital technology and social media, which is relevant to the study's focus on digital security behavior among the digital-native generation.

In terms of gender, the composition of respondents was relatively balanced, with 56 percent female and 44 percent male. This composition shows that female participation in this study was higher, which may reflect their level of involvement in academic activities and online surveys.

However, the significant proportion of male respondents still provides adequate representation to describe the gender perspective in the context of digital security behavior. Based on faculty distribution, most respondents came from the Faculty of Teacher Training and Education (34%), followed by the Faculty of Engineering (27%) and the Faculty of Agriculture (20%).

Meanwhile, respondents from other faculties contributed 19 percent of the total sample. This distribution shows that respondents came from diverse academic backgrounds, including education, technology, and applied sciences.

Description of Research Variable Statistics

Table 2 shows the average values and interpretation categories for the five main variables studied. The results show that the variables Awareness and Action are in the high category, while Knowledge, Experience, and Compliance remain in the moderate category.

DOI: 10.37531/amar.v5i2.3464

Table 2. Average Research Variables

Variable	Mean	Category
Awareness	4.18	Height
Knowledge	3.87	Medium
Experience	3.52	Medium
Compliance	3.78	Medium
Digital Actions	4.01	Height

Instrument Validity and Reliability Test

The validity test shows that all questionnaire items have a calculated correlation coefficient> 0.3, indicating they are valid. Furthermore, the Cronbach's Alpha values for all constructs were above 0.7 (Awareness = 0.801; Knowledge = 0.812; Experience = 0.826; Compliance = 0.793; Action = 0.844), indicating excellent reliability for the instrument.

Classical Assumption Test

The Kolmogorov-Smirnov normality test shows p-values> 0.05 for all variables, indicating that the data are normally distributed. The multicollinearity test shows that the VIF values range from 1.132 to 1.365, and the tolerances are> 0.1. Heteroscedasticity was tested using the Glejser method, and no systematic pattern was found. The Durbin-Watson statistic of 1.895 is close to 2, indicating no autocorrelation.

Multiple Linear Regression Analysis

Regression analysis shows that all four independent variables simultaneously have a significant effect on the dependent variable (F-count = 14.203; p = 0.000 < 0.05). An R^2 of 0.579 indicates that Awareness, Knowledge, Experience, and Compliance can explain 57.9% of the variation in Digital Security Actions.

Table 3. Multiple Linear Regression Test Results

Independent Variable	t-calculated	Sig. (p)
Awareness	2,948	0,004
Knowledge	2,772	0,007
Experience	1,264	0,210
Compliance	3,029	0,003

Based on Table 3, three of the four hypotheses proved to be significant. Awareness, Knowledge, and Compliance were proven to have a positive influence on students' Digital Security Actions. Meanwhile, Experience did not show a significant influence (p > 0.05).

Bar chart showing the average values of the five variables: Awareness, Knowledge, Experience, Compliance, and Digital Action. Scale 1–5. Awareness and Action are close to 4.2 and 4.0; Experience is the lowest. Overall, the results of this study underscore the importance of integrating behavior-based digital literacy, with a focus on practical education, attitude formation, and internalization of digital security norms. Higher education institutions can play a central role in providing training and simulations to improve students' preparedness for cyber threats.

DOI: 10.37531/amar.v5i2.3464

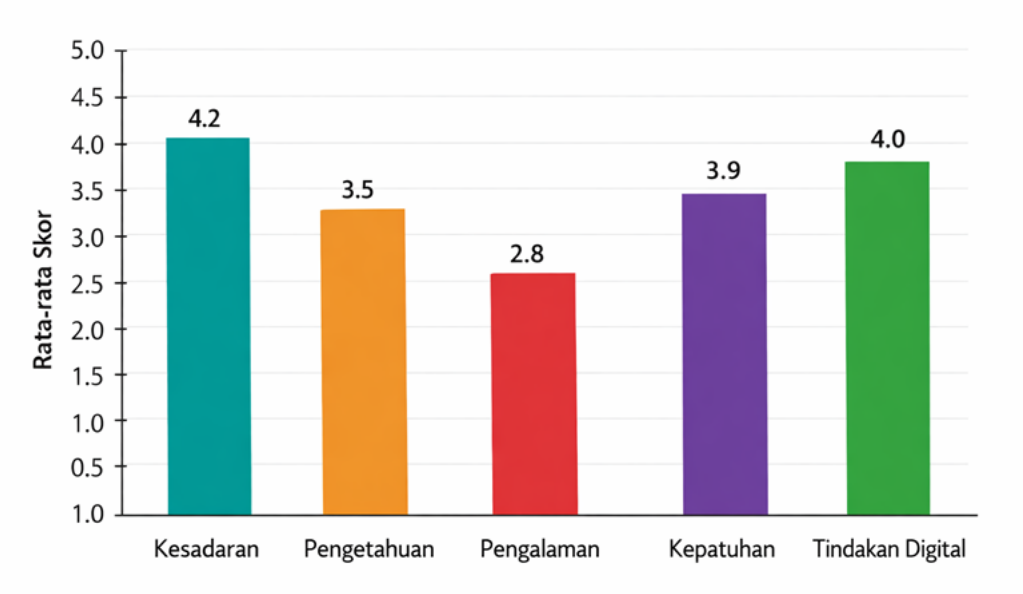

Figure 1. Average Graph of Resea*Discussion*

Discussion

Analysis of the Influence of Awareness on Digital Security Actions

The study's results show that cybersecurity awareness has a positive, significant influence on students' digital security actions. These findings indicate that when individuals have an adequate understanding of cyber risks, potential digital threats, and the consequences of unsafe online behavior, they tend to exhibit more protective behavior in their digital activities. Awareness in this context not only reflects cognitive knowledge of cyber threats but also includes an individual's sensitivity to the importance of maintaining the security of personal data, social media accounts, and digital footprints in general. Thus, awareness serves as the initial foundation that shapes students' behavioral orientation in facing a risky digital environment. These research results reinforce the view that awareness is an important prerequisite for the formation of consistent digital security behavior. Students with a high level of awareness tend to be more cautious in sharing personal information, more alert to the potential for social engineering, and more selective in managing privacy settings on social media. These findings confirm that awareness is not merely an abstract concept, but has real practical implications in everyday digital life. Strong awareness enables individuals to recognize risky situations and make safer decisions before cyber threats actually occur.

These findings are consistent with the Theory of Reasoned Action, which posits that attitudes are the primary determinants of individuals' intentions and actions. In this perspective, awareness of cybersecurity can be understood as an individual evaluative attitude towards digital security behavior. Students who recognize that digital security practices provide tangible protection benefits will develop a positive attitude toward them, which in turn encourages the formation of intentions and the implementation of security measures. In other words, awareness serves as a psychological mechanism that bridges risk perception with protective behavior, thereby reinforcing the Theory of Reasoned Action's relevance in explaining students' digital security behavior (Ajzen & Fishbein, 1975).

In line with this study's results, several previous studies confirm that cybersecurity awareness continues to play an important role in encouraging digital

DOI: 10.37531/amar.v5i2.3464

security actions, even though contextual and individual factors often influence the relationship. Research by Dawn Branley-Bell et al. (2022) shows that cyber risk awareness, accompanied by an adequate level of self-efficacy, contributes to more consistent digital security practices. The study confirms that individuals with high awareness of digital threats tend to exhibit stronger protective behaviors, such as using secure passwords and regularly updating systems, especially when they feel capable of controlling the risks they face. These findings show that awareness is not passive but can be a driver of action when internalized personally. In addition, a cross-population study by Li et al. (2019) among business professionals provides evidence that cybersecurity awareness is positively associated with the implementation of digital security practices. The study shows that individuals with greater awareness of the consequences of cyber threats tend to be more compliant with security procedures and more active in protecting the organization's digital assets.

Knowledge as a Determinant of Cyber Behavior

The study's results indicate that cybersecurity knowledge plays an important role in shaping students' digital security behaviors. These findings suggest that individuals' understanding of basic digital security principles, such as account protection mechanisms, personal information management, and cyber threat identification, directly contributes to their tendency to act protectively in the digital environment. Knowledge in this context is not only the accumulation of information but also a cognitive capacity that enables individuals to assess risky situations and determine an appropriate response. Thus, knowledge serves as an internal resource that strengthens students' ability to translate awareness into concrete security actions. The findings of this study also confirm that applied knowledge plays a stronger role than purely theoretical knowledge. Students who understand digital security concepts in practice, such as how to activate additional protection features and manage privacy settings, tend to be better prepared to address cyber threats. Practical digital security skills are more effective at shaping protective behavior than delivering general information. In other words, knowledge that can be directly applied in real situations is a key factor in encouraging sustainable digital behavior change.

Conceptually, these findings align with the Theory of Reasoned Action, which posits that individual beliefs and understanding serve as the foundation for shaping attitudes toward a behavior. From this theoretical perspective, cybersecurity knowledge shapes fundamental beliefs about the benefits and consequences of safe behavior, which, in turn, influence individuals' attitudes toward digital security practices. When students have an adequate understanding of how cyber threats work and the available protection strategies, they tend to develop positive attitudes toward implementing security practices. These attitudes then encourage the emergence of intentions and actual actions to protect themselves in the digital space. Thus, knowledge acts as a cognitive element that strengthens the path between awareness and action, while clarifying the relevance of the Theory of Reasoned Action in explaining students' digital security behavior.

In line with this study's results, previous research has shown that cybersecurity knowledge positively influences digital security actions, though other supporting factors often moderate this influence. A study by Li et al. (2019) among business professionals shows that individuals with greater knowledge of cyber threats and digital protection mechanisms tend to exhibit more proactive security behavior than

DOI: 10.37531/amar.v5i2.3464

those with a limited understanding. Although the study also noted that not all individuals with high knowledge consistently implement all security protocols, the empirical findings still confirm that knowledge serves as an initial foundation that distinguishes individuals who are willing to take protective measures from those who are entirely passive. Thus, knowledge is positioned as an important prerequisite for the emergence of digital security actions. Furthermore, research by Ashley Cain et al. (2018), which involved respondents from various age groups, also provides evidence that the level of understanding of cyber risks and threat mechanisms correlates with an individual's tendency to implement basic security practices. The study shows that respondents with better knowledge of digital threats and how to mitigate them are more likely to take preventive measures, such as password management and vigilance against suspicious activity.

Compliance with Rules as a Socio-Psychological Factor

The study's results show that compliance with digital security practices significantly influences students' digital security actions. These findings indicate that digital security behavior is not solely determined by individual awareness or knowledge, but also by the extent to which individuals internalize the rules, policies, and norms that govern the use of digital technology. Compliance in this context reflects students' readiness to adjust their digital behavior to applicable security standards, both formal and informal. Thus, compliance serves as a behavioral control mechanism that encourages individuals to act consistently in protecting their personal information and digital reputation. The results of this study show that compliance does not arise solely from administrative obligations or the threat of sanctions. Student compliance more reflects a normative awareness of the importance of protecting personal information and managing digital identity responsibly. Social factors and norms influence behavioral intentions, though their influence is often more implicit than that of cognitive factors. Compliance based on understanding and internalization of digital security values tends to be more sustainable than compliance driven solely by formal rules.

In other words, internalized compliance will be more effective in shaping consistent digital security behavior. Conceptually, these findings align with the Theory of Reasoned Action, which posits subjective norms as a key determinant of behavior. Within this theoretical framework, subjective norms refer to individuals' perceptions of significant social expectations, including pressure or support from the social environment towards a behavior.

Compliance with digital security practices can be understood as a manifestation of internalized subjective norms, where students feel that practicing safe behavior is expected and valued in their academic and social environments. When digital security norms are perceived as a collective responsibility, individuals are more motivated to comply with the rules and translate them into concrete actions.

Thus, the results of this study reinforce the relevance of the Theory of Reasoned Action in explaining students' digital security behavior, particularly through the channel of social norms influencing actual actions. In line with this study's results, several previous studies have shown that compliance with digital security practices and policies plays a significant role in encouraging digital security actions, especially when awareness and knowledge alone are not enough to bridge the gap between understanding and behavior.

DOI: 10.37531/amar.v5i2.3464

Research by Alraja et al. (2023) confirms that compliance with information security policies is an important determinant of employees' digital security behavior in various global organizational contexts. The study shows that individuals comply with security policies not only because of formal pressure, but also because they view compliance as a legitimate and relevant protection mechanism. These findings indicate that compliance serves as a link between risk awareness and concrete actions, thereby reducing users' tendency to ignore security protocols even though they understand cyber threats. In addition, research by Vedadi et al. (2024) provides a perspective that reinforces the role of compliance as a normative and prosocial behavioral factor. Vedadi views information security compliance as part of organizational citizenship behavior, which is voluntary behavior that goes beyond formal obligations and is driven by the internalization of shared values and norms. This study shows that individuals who perceive compliance as a collective responsibility tend to be more consistent in implementing digital security practices.

The Minimal Influence of Experience on Actions

The study's results show that cybersecurity experience does not have a significant effect on students' digital security behaviors. These findings indicate that experiencing cyber incidents does not automatically lead individuals to adopt better digital security behaviors. In other words, experiences with cyber risks or incidents do not necessarily translate into consistent protective actions. This fact shows that experiences are ambiguous and depend on how they are processed, interpreted, and integrated into an individual's cognitive framework. Without adequate reflection and learning, experiences can become events that pass without lasting impact on behavior.

The results of this study seem to contradict the view that direct experience is the primary driver of changes in cybersecurity behavior. Bada et al. (2021) emphasize that real experiences with security incidents can increase awareness and encourage users to be more cautious in their digital activities (Bada et al., 2021). However, this difference in results does not necessarily indicate an absolute contradiction; rather, it reflects differences in context and quality of experience. Studies that emphasize the decisive role of experience generally refer to experiences that are intense, reflective, and accompanied by explicit learning. In contrast, students' experiences in this study tended to be passive and were not followed by a structured learning process. Further explanation can be seen in students' experiences. These experiences are often limited to mild exposure, such as receiving suspicious messages or knowing about incidents experienced by others, without active involvement in handling or analyzing the incident. Such experiences are insufficient to form a deep reflective awareness of cyber risks and the consequences of digital behavior. Without strong emotional and cognitive involvement, experiences lose their transformative power and are unable to drive significant behavioral change.

These findings can be explained by the Theory of Reasoned Action, which emphasizes that behavior is influenced by subjective attitudes and norms rather than solely by empirical experiences. From this theoretical perspective, experiences will only influence actions if they shape evaluative attitudes or change individuals' perceptions of social expectations. If cyber experiences are not accompanied by conceptual understanding and internalization of security values, they are not powerful enough to shape behavioral intentions. Thus, the findings of this study indicate that

DOI: 10.37531/amar.v5i2.3464

unstructured experiences that are not cognitively reflected upon tend to fail to determine digital security behavior.

In line with this study's results, previous studies have shown that cybersecurity experiences do not always have a significant effect on digital security actions, especially when they are not followed by adequate learning and internalization. A study by Zwilling et al. (2022) revealed that although internet users have experienced or are aware of various forms of cyber threats, these experiences do not automatically prompt the adoption of stronger protective measures. These findings indicate that experiences are descriptive and passive, and therefore insufficient to trigger behavioral change unless accompanied by practical guidance and normative encouragement. Thus, experiences as exposure to risk can be separate from protective behaviors that are implementative in nature. In addition, research by Kovačević et al. (2020) on groups of students and digital natives also shows a similar pattern. The study found that individuals who are technologically active and have extensive experience with digital devices still exhibit weak security behaviors. High technology use does not correlate with the adoption of digital security practices, reinforcing the argument that experience alone is insufficient to shape security actions. This finding is reinforced by Barth et al. (2022), who show that even cybersecurity experts can exhibit behavior similar to that of ordinary users, despite their extensive experience and exposure to security issues.

Relevance to the Local Context of Papuan Students

This study makes significant contextual contributions by being conducted with students at the University of Papua, a region that remains relatively unexplored in academic research on digital security. The geographical context of Papua, characterized by technological infrastructure challenges, limited internet access in some areas, and gaps in the availability of digital devices, presents a different dynamic from the urban context in western Indonesia. Nevertheless, students at the University of Papua show a relatively high level of digital participation, especially in the use of social media for communication, information, and social expression. This condition reflects a paradox between structural limitations and the intensity of digital activities, which can increase vulnerability to cybersecurity risks if not balanced with adequate literacy and security practices.

The social and cultural background of Papuan students also shapes distinctive patterns of digital interaction. The values of collectivity, community closeness, and strong social relationships among students can influence how they perceive risk and security in the digital space. In this context, the practice of sharing information, interpersonal trust, and the tendency to follow group behavior can either strengthen or weaken digital security measures. Therefore, the approach to cybersecurity literacy and education in Papua cannot be directly equated with the approach applied in other regions with different social and technological characteristics.

As a result, strategies to improve digital security among Papuan students need to be designed with careful consideration of the local context. A culture-based approach, easy-to-understand language, and visual media and contextual examples familiar to students are important for increasing the effectiveness of cybersecurity messages. In addition, campus community approaches, such as group discussions, student organization-based activities, and direct mentoring, have the potential to be more effective than conventional online learning methods that depend on stable

DOI: 10.37531/amar.v5i2.3464

internet access. By adapting educational strategies to the social, geographical, and cultural realities of Papua, efforts to strengthen students' digital resilience can be carried out in a more inclusive, relevant, and sustainable manner.

The Urgency of Practice- and Norm-Based Educational Strategies

The urgency of practice- and norm-based educational strategies is becoming increasingly evident in strengthening students' digital security behavior. Cybersecurity literature consistently shows that one-way, informative counseling is not enough to shape sustainable protective behavior. This study confirms that awareness and knowledge are meaningful only when translated into practical skills and attitudes internalized in daily digital activities. Thus, an educational approach that emphasizes direct experience, active learning, and critical reflection is key to bridging the gap between cognitive understanding and real action. Cyberattack simulations, such as phishing or social engineering, as well as data security practices, including password management and encryption, can help students understand the consequences of risk in concrete, contextual terms.

Furthermore, effective educational strategies should not only focus on individual aspects but also on fostering collective norms in the academic environment. Social norms that support digital security practices will strengthen the internalization of safe behavior, as students will act not only on personal awareness but also in line with shared expectations and habits. In this context, campuses have a strategic role as social spaces that can shape students' digital values, attitudes, and habits. Practice-based training programs conducted in groups, real-case discussions, and student organization involvement can strengthen the normative dimension of cybersecurity behavior. In the long term, systematic intervention from higher education institutions is an inevitable necessity. Integrating digital literacy and security as a compulsory subject across study programs is a strategic step to ensure that all students acquire the same foundation, regardless of their academic background. In addition, providing technology-based training facilities tailored to the local context will increase the relevance and affordability of learning. By making digital security an integral part of the curriculum and campus culture, the formation of safe behavior is no longer seen as the sole responsibility of individuals but as an institutional commitment to sustainably building the digital resilience of the younger generation.

CONCLUSION

This study conceptually focuses on understanding students' digital security behavior in social media use through a behavioral approach that emphasizes the roles of psychological and normative factors. The research aims to explain how awareness, knowledge, experience, and compliance shape students' digital security actions within the Theory of Reasoned Action framework. By framing digital security behavior as the result of cognitive and social processes, this study provides a comprehensive understanding of the mechanisms underlying the formation of digital security actions in higher education environments, particularly at the University of Papua, which has distinctive social, geographical, and technological characteristics.

Theoretically, this research contributes to the development of behavior-based cybersecurity studies by extending the Theory of Reasoned Action to the context of students in a region that has been relatively underexplored in the literature. The uniqueness of this research lies in integrating the dimensions of attitude, norms, and

DOI: 10.37531/amar.v5i2.3464

local context to explain digital security actions, thereby enriching perspectives that have tended to focus solely on technical aspects. From a practical and managerial perspective, this research provides a basis for higher education institutions to design more comprehensive digital literacy policies and strategies, emphasizing the formation of attitudes and norms of compliance through curriculum, practice-based training, and strengthening the culture of digital security on campus as part of academic governance and student character development.

However, this study has limitations that need to be considered. The use of a cross-sectional design limits the study's ability to capture the dynamics of changes in digital security behavior over time. The study's limited scope, confined to one university, also limits the generalizability of its findings to broader contexts. In addition, reliance on perception-based data can lead to self-reporting bias. Therefore, future research is recommended to adopt a longitudinal approach to observe continuous behavioral changes, expand the participant pool to include students from various educational institutions in Indonesia, and combine quantitative and qualitative methods to explore the deeper psychological, social, and cultural dynamics that shape students' digital security behavior.

Reference:

Acheampong, R., Balan, T. C., Popovici, D.-M., Tuyishime, E., Rekeraho, A., & Voinea, G. D. (2025). Balancing usability, user experience, security and privacy in XR systems: a multidimensional approach. *International Journal of Information Security*, *24*(3), 112. https://doi.org/10.1007/s10207-025-01025-z

Ajzen, I., & Fishbein, M. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Alraja, M. N., Butt, U. J., & Abbod, M. (2023). Information security policies compliance in a global setting: An employee's perspective. *Computers & Security*, *129*, 103208. https://doi.org/https://doi.org/10.1016/j.cose.2023.103208

An, Q., Hong, W. C. H., Xu, X., Zhang, Y., & Kolletar-Zhu, K. (2023). How education level influences internet security knowledge, behaviour, and attitude: a comparison among undergraduates, postgraduates and working graduates. *International Journal of Information Security*, *22*(2), 305–317. https://doi.org/10.1007/s10207-022-00637-z

Bada, A., Sasse, M. A., & Nurse, J. R. (2021). The role of user education and awareness in improving cybersecurity: A review of recent literature. *Computers & Security*, *103*, 102159.

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*, 103741. https://doi.org/https://doi.org/10.1016/j.cose.2024.103741

Barth, S., de Jong, M. D. T., & Junger, M. (2022). Lost in privacy? Online privacy from a cybersecurity expert perspective. *Telematics and Informatics*, *68*, 101782. https://doi.org/10.1016/j.tele.2022.101782

Bishop, L. M., Asquith, P. M., & Morgan, P. L. (2025). The employee cybersecurity awareness framework. *Human Behavior and Emerging Technologies*, *2025*(1), 1025045. https://doi.org/10.1155/hbe2/1025045

Branley-Bell, D., Coventry, L., Dixon, M., Joinson, A., & Briggs, P. (2022). Exploring age and gender differences in ICT cybersecurity behaviour. *Human Behavior and Emerging Technologies*, *2022*(1), 2693080. https://doi.org/10.1155/2022/2693080

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36–45.

DOI: 10.37531/amar.v5i2.3464

https://doi.org/10.1016/j.jisa.2018.08.002

Concari, A., Kok, G., Martens, P., & Brink, N. (2023). Investigating the Role of Goals and Motivation on Waste Separation Behavior Through the Lens of the Theory of Reasoned Goal Pursuit. *Environmental Management*, *72*(5), 1019–1031. https://doi.org/10.1007/s00267-023-01820-1

Gopinathan, S., Veeraya, S., Raman, M., & Jambulingam, M. (2025). Role of behavioral intention in implementation of green information systems among Malaysians. *Discover Sustainability*, *6*(1), 139. https://doi.org/10.1007/s43621-025-00873-y

Ifinedo, P., Mengesha, N., & Bekele, R. (2022). Effects of Personal Factors and Organizational Reinforcing Tools in Decreasing Employee Engagement in Unhygienic Cyber Practices: Perspectives From a Developing Country. *Journal of Global Information Management (JGIM)*, *30*(1), 1–27. https://doi.org/10.4018/JGIM.299324

Iskandar, R., Maksum, A., & Marini, A. (2025). Digital citizenship literacy in Indonesia: The role of privacy awareness and social campaigns. *Social Sciences & Humanities Open*, *12*, 101697. https://doi.org/https://doi.org/10.1016/j.ssaho.2025.101697

Kannelønning, K., & Katsikas, S. K. (2023). A systematic literature review of how cybersecurity-related behavior has been assessed. *Information and Computer Security*, *31*(4), 463–477. https://doi.org/10.1108/ICS-08-2022-0139

Kavak, A. (2024). Impact of information security awareness on information security compliance of academic library staff in Türkiye. *The Journal of Academic Librarianship*, *50*(5), 102937. https://doi.org/https://doi.org/10.1016/j.acalib.2024.102937

Khan, N. F., Ikram, N., Murtaza, H., & Javed, M. (2023). Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. *Computers & Security*, *125*, 103049. https://doi.org/https://doi.org/10.1016/j.cose.2022.103049

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

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.10.017

Neri, M., Benevento, E., Stefanini, A., Aloini, D., Niccolini, F., Carducci, A., Federigi, I., & Dini, G. (2024). Understanding information security awareness: evidence from the public healthcare sector. *Information and Computer Security*, *33*(3), 309–319. https://doi.org/10.1108/ICS-04-2024-0094

Oroni, C. Z., Xianping, F., Ndunguru, D. D., & Ani, A. (2025). Enhancing cyber safety in e-learning environment through cybersecurity awareness and information security compliance: PLS-SEM and FsQCA analysis. *Computers & Security*, *150*, 104276. https://doi.org/https://doi.org/10.1016/j.cose.2024.104276

Paraskevi, G., Saprikis, V., & Avlogiaris, G. (2023). Modeling nonusers' behavioral intention towards mobile chatbot adoption: An extension of the UTAUT2 model with mobile service quality determinants. *Human Behavior and Emerging Technologies*, *2023*(1), 8859989. https://doi.org/10.1155/2023/8859989

Patterson, C. M., Nurse, J. R. C., & Franqueira, V. N. L. (2023). Learning from cyber security incidents: A systematic review and future research agenda. *Computers & Security*, *132*, 103309. https://doi.org/https://doi.org/10.1016/j.cose.2023.103309

Pigola, A., da Costa, P. R., Vils, L., & Meirelles, F. de S. (2025). Enhancing information security management and performance through social and relational factors: a structural equation modelling approach. *Behaviour & Information Technology*, 1–23. https://doi.org/10.1080/0144929X.2025.2522206

Prachaseree, K., Ahmad, N., & Md Isa, N. (2021). Applying Theory Elaboration for Theory of Reasoned Action (TRA) and Its Extensions. *GIS-Business*, *16*(2), 35–57.

Rachmadana, S. L., Mufida, N., Rusdy, H., Agung, A., & Masiku, G. (2024). Theory of

DOI: 10.37531/amar.v5i2.3464

Reasoned Action as a Framework for Analyzing Investment Knowledge in Generation Z. *Fundamental and Applied Management Journal (FAMJ)*, *2*(1), 16–21. https://doi.org/10.61220/famj.v2i1.2243

Reuben-Owoh, B., & Haig, E. (2025). A Systematic Review of Voluntary Cybersecurity Standards and Frameworks. *International Journal of Information Security*, *24*(5), 206. https://doi.org/10.1007/s10207-025-01121-0

Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. *Computers & Security*, *119*, 102756. https://doi.org/https://doi.org/10.1016/j.cose.2022.102756

Shukla, S. S., Tiwari, M., Lokhande, A. C., Tiwari, T., Singh, R., & Beri, A. (2022). A comparative study of cyber security awareness, competence and behavior. *2022 5th International Conference on Contemporary Computing and Informatics (IC3I)*, 1704–1709. https://doi.org/10.1109/IC3I56241.2022.10072880

Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security*, *102*, 102154. https://doi.org/https://doi.org/10.1016/j.cose.2020.102154

Taha, I. M., Hussein, R., Ali, A., & Abbas, A. A. (2025). The Impact of Students ' Cybersecurity Vulnerability Behavior on E-Learning Obstacles. *Organizacija*, *58*(1), 85–104. https://doi.org/10.2478/orga-2025-0006

Taherdoost, H. (2024). A Critical Review on Cybersecurity Awareness Frameworks and Training Models. *Procedia Computer Science*, *235*, 1649–1663. https://doi.org/https://doi.org/10.1016/j.procs.2024.04.156

Tejay, G. P. S., & Winkfield, M. (2025). Does Leadership Approach Matter? Examining Behavioral Influences of Leaders on Employees' Information Security Compliance. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-025-10592-4

Vedadi, A., Warkentin, M., Straub, D. W., & Shropshire, J. (2024). Fostering information security compliance as organizational citizenship behavior. *Inf. Manage.*, *61*(5). https://doi.org/10.1016/j.im.2024.103968

Xu, F., Hsu, C., Wang, T., & Lowry, P. B. (2024). The antecedents of employees' proactive information security behaviour: The perspective of proactive motivation. *Information Systems Journal*, *34*(4), 1144–1174. https://doi.org/10.1111/isj.12488

Yazdanmehr, A., Li, Y., & Wang, J. (2023). Employee responses to information security related stress: Coping and violation intention. *Information Systems Journal*, *33*(3), 598–639. https://doi.org/10.1111/isj.12417

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269