International Journal of Social Science, Educational, Economics, Agriculture Research and Technology (IJSET) | ISSN (e) : 2827-766X
Volumes 5 No. 1 (2025)

ANALYSIS OF CYBER THREAT AWARENESS LEVELS, PROTECTIVE BEHAVIOR, AND COMMUNICATION PREFERENCES AMONG THE DIGITAL SOCIETY IN SEMARANG CITY

Tika[1], Rizky Prawita Utami[2], Adi Marsoni[3], Anesthesia Aryan Putri[4], dan Rakesh Sitepu[5]
[1,2,3,4,5] Universitas BPD, Semarang
Email: tikaa1834@gmail.com, rizkyprawitaa@gmail.com, marsoniadi09@gmail.com, putri21aap@gmail.com

Received	: 25 November 2025	Published	:19 January 2026
Revised	: 05 December 2025	DOI	:https://doi.org/10.54443/ijset.v5i1.1598
Accepted	: 30 December 2025	Publish Link	:https://www.ijset.org/index.php/ijset/index

Abstract

Digital transformation in Indonesia has increased access to technology while also expanding the risk of cyber threats. This study aims to analyze the relationship between cyber threat awareness, protective behavior, and digital security communication preferences among the digital society in Semarang City. The research method used an explanatory quantitative approach with Structural Equation Modeling-Partial Least Squares (SEM-PLS) through SmartPLS 4.0, involving 100 active internet users as respondents. The results show that cyber threat awareness has a positive and significant effect on protective behavior ($\beta = 0.847$; $p < 0.001$) and digital security communication preferences ($\beta = 0.822$; $p < 0.001$). However, protective behavior did not significantly affect communication preferences ($\beta = 0.159$; $p = 0.234$) and did not mediate the relationship between awareness and communication preferences ($\beta = 0.135$; $p = 0.294$). These findings indicate an intention-behavior gap where awareness has not been fully applied in safe communication behavior. Theoretically, the results of this study reinforce the Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT), while practically emphasizing the importance of improving communication-based cyber literacy and awareness to build a resilient digital society.

Keywords: Cyber threat awareness, protective behavior, communication preferences, digital literacy, SEM-PLS.

1. Introduction

The rapid digital transformation in Indonesia has brought fundamental changes in the way people work, communicate, conduct transactions, and access public services. Developments in digital technology, including increased use of the internet, digital financial services, mobile services, and the integration of the Internet of Things (IoT), have significantly expanded people's activities in the digital space (Gusman, 2024). However, this acceleration in digitalization has also been accompanied by an increase in the complexity and intensity of cyber threats, such as phishing, malware, ransomware, identity theft, and various forms of social engineering crimes that target users directly (Tatara et al., 2023; Serac, 2023). As digital systems and cloud-based services become increasingly connected, the surface area for cyberattacks is becoming broader and more difficult to control. Recent studies show that modern cybercrime models, such as Ransomware-as-a-Service (RaaS), enable perpetrators with limited technical capabilities to carry out large-scale, systematic attacks (Wibowo et al., 2025). This situation is exacerbated by weak cybersecurity governance and low public awareness of personal data protection, even though data protection regulations have begun to be implemented in Indonesia (Hariana et al., 2025; Faisal & Zuliarti, 2024).

Various studies show that human factors remain the main weakness in the cybersecurity ecosystem. Low digital literacy, limited understanding of cyber threats, and a lack of basic security practices such as secure password management, information verification, and the use of two-factor authentication are the causes of increased public vulnerability to cyber-attacks (Azzani et al., 2024; Santos et al., 2025). In the Indonesian context, the gap between the level of digital technology utilization and user security readiness indicates that improvements in digital infrastructure have not been fully matched by human resource readiness in dealing with cyber risks. The results of research conducted by Kaufhold et al. (2025), in Germany show that although public awareness of cyber threats is relatively high, most respondents still feel that they are not sufficiently capable of protecting themselves technically and lack trust in national security authorities. A longitudinal study of more than 3,000 citizens found that only 39% of respondents felt confident in their ability to protect their devices from cyber threats, while more than half did not

know of any reliable sources of security information. These findings indicate an awareness-behavior gap, i.e., a gap between awareness of threats and actual protective measures. A similar phenomenon can also be seen in Indonesia. A collaborative survey conducted by the Ministry of Communication and Information Technology (Kominfo) and Katadata Insight Center (KIC) in 2023 shows that the national digital literacy level is still in the moderate category with a score of 3.65 on a scale of 1-5, indicating that the digital capabilities of the society are not yet optimal, especially in terms of security and ethics in the use of technology (Kementerian Komunikasi dan Informatika Republik Indonesia & Katadata Insight Center., 2023). This is reinforced by the results of Kementerian Komunikasi Dan Digital (2025), for 2024, which recorded a score of 43.34, indicating that the public's digital skills and readiness still need to be improved. In addition, the BSSN (2025), report, Indonesia's Cybersecurity Landscape 2024, released by the National Cyber and Crypto Agency (BSSN), reveals a significant increase in cyber threats, including phishing activities that have reached tens of millions of incidents and data leaks detected on the darknet. These conditions emphasize that the increased adoption of digital services in various sectors needs to be balanced with awareness of cyber threats, protective behavior, and more mature security communication patterns among Indonesia's digital society.

From a Human Computer Interaction (HCI) perspective, cybersecurity behavior is influenced not only by technological factors, but also by risk perception, self-confidence, and user communication preferences (Kaufhold et al., 2025). Theoretically, this relationship can be explained through Protection Motivation Theory (PMT), which emphasizes that threat appraisal and coping appraisal are the main factors in forming the intention to take protective action. Meanwhile, Technology Threat Avoidance Theory (TTAT) expands on this concept by considering response effectiveness, perceived costs, and user efficacy in avoiding technological threats. In the national context, good digital literacy has been shown to be positively associated with readiness to adapt to digital transformation in various sectors (Isabella et al., 2024; Hendriawan et al., 2025). However, research that simultaneously integrates the relationship between cyber threat awareness, protective behavior, and security communication preferences is still very limited, especially at the general public level in Indonesia. Most previous studies are still descriptive in nature and have not tested the structural relationship between human factors predictively. Most previous studies have focused on technical aspects of security, while studies on the relationship between threat awareness, protective behavior, and security communication preferences at the general public level, especially in major Indonesian cities such as Semarang, are still very limited.

Based on these research gaps, this study developed an analytical approach based on Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT) to analyze the relationship between cyber threat awareness, protective behavior, and digital security communication preferences among the people of Semarang City. The Structural Equation Modelling Partial Least Squares (SEM-PLS) approach is used to test the simultaneous relationship between latent variables and identify significant factors that influence the security behavior of the digital society. Based on the background description above, it can be identified that there is still a gap between the level of public awareness of cyber threats and the protective behaviors they apply in their daily digital activities. Although awareness of cyber threats is increasing, protective measures and individuals' ability to manage digital risks have not yet reached an adequate level. This condition raises questions about the extent to which awareness of cyber threats, protective behaviors, and digital security communication preferences are interrelated and contribute to the public's readiness to face cyber threats in the digital era.

Thus, this study aims to analyze the relationship between cyber threat awareness, protective behavior, and digital security communication preferences among the people of Semarang City. More specifically, this study seeks to identify the level of cyber threat awareness among the society, describe the protective behaviors applied in the use of digital technology, and examine the patterns and preferences of communication used by the society in obtaining cyber security information. In addition, this study also aims to test the latent relationship between these variables using the Structural Equation Modeling-Partial Least Squares (SEM-PLS) approach based on the Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT) theoretical frameworks. Theoretically, this research is expected to contribute to the development of cyber security behavior studies by integrating aspects of awareness, protective actions, and digital communication into a comprehensive analytical model. Meanwhile, in practical terms, the results of this study are expected to serve as a basis for local governments, cybersecurity agencies, and digital service providers in designing more effective strategies to improve cybersecurity literacy and awareness among urban communities, particularly in the city of Semarang.

2. Literature Review

2.1 Cyber Threat Awareness

Cyber threat awareness describes the extent to which individuals understand the potential risks, forms of threats, and impacts that can arise from unsafe digital activities. This level of awareness influences the extent to which a person is able to recognize, avoid, and react to digital threats such as phishing, malware, and personal data theft (Kaufhold et al., 2025). Previous research shows that high cyber awareness encourages protective behaviors, such as the use of strong passwords and two-factor authentication (Azzani et al., 2024; Santos et al., 2025). However, the gap between knowledge and action, known as the awareness-behavior gap, remains a major issue in strengthening individual cyber resilience (Kaufhold et al., 2025).

2.2 Protective Behavior

Protective behavior refers to preventive and responsive actions taken by individuals to protect themselves from digital threats. Based on the Protection Motivation Theory (PMT) introduced by Rogers and later developed conceptually by various researchers, an individual's motivation to engage in protective behavior is determined by two main cognitive processes, namely threat appraisal and coping appraisal. Threat appraisal includes an individual's perception of the severity and likelihood of a threat, while coping appraisal includes beliefs about the effectiveness of responses, self-efficacy, and the costs that may arise from protective actions (González-Ponce et al., 2024). In the context of information security, this theory has been proven relevant in explaining how threat perception and self-efficacy influence digital protective behaviors, such as the use of two-factor authentication, security system updates, and information source verification (Khan et al., 2023). In the context of cybersecurity, Liang & Xue (2009), Technology Threat Avoidance Theory (TTAT) expands PMT by incorporating variables such as perceived effectiveness of prevention efforts, perceived effort cost, and individual efficacy in avoiding threats. This theory asserts that the higher the perception of threat and self-efficacy, the stronger the intention to implement digital security behaviors such as updating systems, using multi-factor authentication, and verifying information sources.

2.3 Security Communication Preferences

Security communication preferences refer to the methods, sources, and media that individuals trust most to receive information related to digital security. In Human-Computer Interaction (HCI) studies, communication preferences are key to understanding how people interpret and respond to security messages (Kaufhold et al., 2025). Research shows that trust in information sources, message relevance, and communication style significantly influence the extent to which security messages can change user behavior. A study by Gier et al. (2023), confirms that message framing affects users' trust and interpretation of messages, while research by Searle & Renaud (2023), shows that the level of trust in information sources plays an important role in shaping responses and vulnerability to digital security behavior. Effective security communication must be able to build a sense of urgency without causing excessive fear, and be delivered through channels that are appropriate to the characteristics of the audience. Therefore, understanding communication preferences is important in designing education strategies and cyber literacy campaigns in the society (Isabella et al., 2024; Hendriawan et al., 2025).

2.4 Interrelationships Between Variables and Conceptual Model Development

High cyber threat awareness encourages individuals to pay more attention to security messages and choose credible and reliable sources of communication. A study by Kaufhold et al. (2025), highlights that the level of threat awareness correlates positively with trust in security institutions and a preference for official sources of communication, such as the government and digital service providers that are considered to have authority. Similar results were shown by Klein et al. (2021), who found that cyber awareness not only plays a role in increasing protective behavior, but also strengthens individuals' sensitivity to digital security messages. Meanwhile, research by Naqvi et al. (2024), shows that threat perception and security awareness influence how individuals assess the effectiveness of security communication strategies in an organizational context, including trust in the media and communication channels used. Thus, the higher an individual's level of cyber threat awareness, the stronger their preference for credible communication sources and relevant security messages.

H1: Cyber threat awareness has a positive effect on digital security communication preferences.

Cyber threat awareness plays an important role in encouraging protective behavior among individuals in the digital space. Individuals with a high level of awareness of threats such as phishing, malware, and data breaches tend to be more cautious and implement preventive measures, such as using two-factor authentication and regularly updating security systems. A study by Li et al. (2022), confirms that increased cyber awareness significantly strengthens protective intentions and actions through the threat appraisal and coping appraisal mechanisms described

in Protection Motivation Theory (PMT). Similar results were found by Zwilling et al. (2022), confirms that increased cyber awareness significantly strengthens protective intentions and actions through the threat appraisal and coping appraisal mechanisms described in Protection Motivation Theory (PMT). Similar results were found by Dinev & Hu (2007), shows that threat awareness is a strong predictor of users' behavioral intentions in adopting protective technologies. Thus, it can be assumed that the higher a person's level of cyber threat awareness, the more likely that individual is to develop protective behaviors in their digital activities.

H2: Cyber threat awareness has a positive effect on the protective behavior of the digital society.

Protective behavior is closely related to security communication preferences because individuals who actively implement digital security practices tend to be more selective and critical of the sources of information they trust. According to Searle & Renaud (2023), the level of trust in security message sources influences users' psychological responses and protective behaviors. This study emphasizes that perceptions of the reliability and credibility of message sources play a role in determining whether individuals will adopt digital security behaviors on an ongoing basis. Additionally, Gier et al. (2023), show that message framing and communication style have a significant influence on the effectiveness of security messages in shaping protective attitudes, where messages that focus on negative consequences tend to be more effective in encouraging user compliance. In line with this, research by Rodríguez-Priego et al. (2020), confirms that the combination of message framing (gain vs. loss) and trust in the source of information influences users' risk perceptions and behavioral intentions in the context of online security. Based on these findings, it can be concluded that the effectiveness of security communication depends on the extent to which individuals' protective behaviors shape their preferences for digital security message sources and styles.

H3: Protective behavior has a positive effect on digital security communication preferences.

Protective behavior acts as a mediating mechanism between cyber threat awareness and digital security communication preferences. Individuals who are highly aware of threats tend to develop protective measures before determining credible sources of security information. Based on Technology Threat Avoidance Theory (TTAT), perceptions of prevention effectiveness and self-efficacy serve as a link between threat perception and security information-seeking behavior (Liang & Xue, 2009). Similar findings by Li et al. (2022), and Duzenci et al. (2023), show that protective motivation strengthens the relationship between threat awareness and effective digital security communication behavior. Thus, protective behavior can be an intermediary variable that explains how cyber threat awareness influences digital security communication preferences.

H4: Protective behavior mediates the relationship between cyber threat awareness and digital security communication preferences.

Based on theoretical studies and previous research results, the relationship between these variables is summarized in the following conceptual research model (Figure 1).

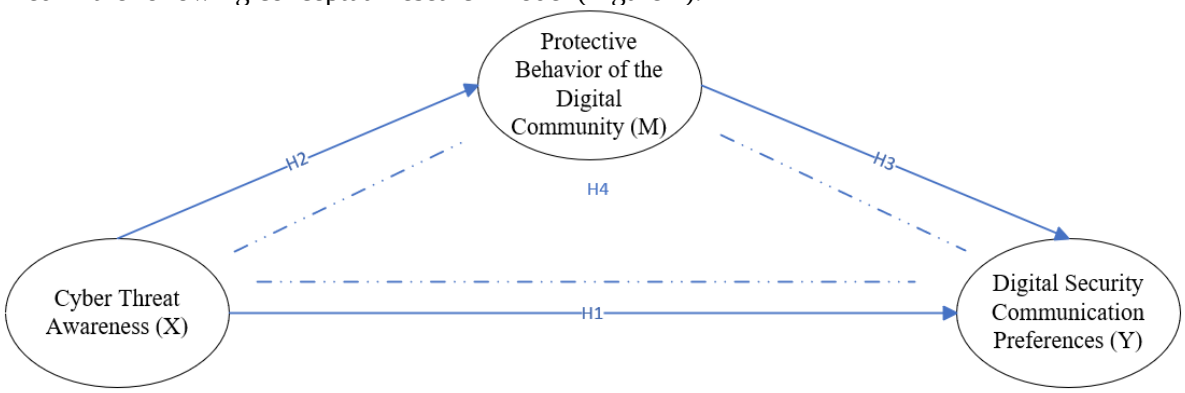

Figure 1. *Framework model*

3. Research Method

3.1 Research Approach

This study uses an explanatory quantitative approach with Structural Equation Modeling-Partial Least Squares (SEM-PLS) analysis to test the causal relationship between latent variables, namely cyber threat awareness, digital community protective behavior, and digital security communication preferences. The selection of the SEM-PLS method is based on its ability to analyze complex models with relatively small sample sizes and data distributions that do not have to be normal (Russo & Stol, 2022; Hair et al., 2024). This method also allows for testing direct and indirect (mediation) relationships, making it suitable for the research objective, which focuses on testing conceptual models based on Technology Threat Avoidance Theory (TTAT) and Protection Motivation Theory (PMT).

3.2 Sample Population

The research population includes the digital community residing in Semarang City who actively use the internet and digital services in their daily activities. The sampling technique used purposive sampling, with respondents aged 18-50 years and having at least one year of experience in using digital applications. A total of 100 respondents participated in this study. This number is considered adequate for SEM-PLS analysis because it meets the minimum sample size recommended by Hair et al. (2024), which is 10 times the number of indicators in the most complex variable in the model. Previous studies with similar designs also showed that a sample size of 64–150 respondents can produce reliable and valid models (Fattah et al., 2023; Judijanto et al., 2023).

3.3 Data Collection Techniques

Data were collected through an online questionnaire using a 5-point Likert scale, ranging from 1 (strongly disagree) to 5 (strongly agree). The research instrument was developed based on the adaptation of indicators from relevant previous studies: cyber threat awareness indicators were adapted from (Kaufhold et al., 2025), protective behaviors from (Li et al., 2022), and digital security communication preferences from (Searle & Renaud, 2023), as well as (Rodríguez-Priego et al., 2020). Content validation was conducted through expert judgment by three academics in the field of information systems and digital security.

3.4 Data Analysis Techniques

Data analysis was performed using SmartPLS 4.0. The analysis stages included testing the measurement model (outer model) and structural model (inner model). In the outer model stage, convergent validity was evaluated using factor loading values (>0.70) and Average Variance Extracted (AVE) (>0.50), as well as construct reliability using Composite Reliability (CR) values (>0.70). Furthermore, discriminant validity was tested using the Fornell-Larcker criteria and Heterotrait-Monotrait ratio (HTMT) (Latif et al., 2025). In the inner model stage, the relationship between variables was tested through bootstrapping with 5,000 resampling to assess the significance of the path coefficient and t-statistics value ($p < 0.05$). The R^2 value was used to assess the predictive power of the model, while Q^2 and SRMR (Standardized Root Mean Square Residual) were used to assess goodness of fit (Hair et al., 2024). The SEM-PLS method was chosen because it has high flexibility in analyzing complex models and mediating variables in small sample sizes, and has been proven effective in various cybersecurity and user behavior studies. A similar approach was used by Sulaiman et al. (2022), in analyzing the security behavior of government employees based on Protection Motivation Theory, and by Vrhovec & Fujs (2023), who showed that trust in information sources and perceptions of digital authority play an important role in shaping protective motivation among users.

3.5 Methodological Justification

According to Hair et al. (2024), is superior for predictive research involving latent variables with non-normal data and small to medium sample sizes. Meanwhile, research by Judijanto et al. (2023), shows that the PLS-SEM method is effective in testing complex relationships in the context of information security in Indonesia. This approach was also used by Fattah et al. (2023), in analyzing students' cyber security awareness, and by Latif et al. (2025), to test the PMT-based protective behavior model in the era of industry 4.0. Thus, the use of SEM-PLS in this study is considered most appropriate for testing the causal relationship between cyber threat awareness, protective behavior, and digital security communication preferences in the community of Semarang City.

4. Results

4.1 Demographic Characteristics of Respondents

This study involved 100 digital community respondents in Semarang City, with characteristics dominated by the young productive age group. The majority of respondents were in the 17–25 age range (34%) and 26–30 age range (30%), so that cumulatively 64% of respondents were active users of digital technology with high internet usage intensity. This age group has a greater chance of exposure to cyber threats due to their intense digital activities, but often still has gaps in their understanding of data security practices, such as awareness of phishing and password management (Mahipal et al., 2025; Chasanah & Candiwan, 2020). These findings are in line with international studies showing that young users with high internet usage duration tend to have uneven cyber awareness and still need to strengthen their digital literacy to minimize the risk of online attacks (Naik, 2025). In terms of gender, the composition of respondents was relatively balanced between males (48%) and females (52%), indicating that cybersecurity issues are a cross-gender need and are increasingly relevant in daily digital activities, including in the context of local communities (Anggraheni et al., 2024).

In terms of education, the majority of respondents were D3/S1 graduates (64%), followed by SMA/SMK (34%), and master's degree (2%), indicating that most respondents have sufficient educational capacity to understand digital security risks, even though digital literacy in Indonesia is still moderate and needs to be strengthened, especially in terms of security and media ethics (Afrina et al., 2024); Ministry of Communication and Information Technology of the Republic of Indonesia & Katadata Insight Center, 2023). The respondents' occupational backgrounds were also diverse, including civil servants (27%), students (26%), private employees (20%), entrepreneurs (19%), housewives (7%), and freelancers (1%), indicating that exposure to cyber threats occurs across all social strata. The intensity of internet use was dominated by 4–6 hours/day (47%) and more than 6 hours per day (30%), with the main activities being social media (75%), online shopping (29%), work (28%), and digital financial services (23%). This usage pattern carries a high risk of cybercrime such as online fraud, data theft, and phishing, as shown by research in Indonesia and Southeast Asia which confirms that digital security knowledge and awareness play an important role in increasing users' awareness and safe behavior in online activities and digital transactions (Imran & Asmoro, 2024; Muliawan & Hasnawati, 2024; Lim & Tan, 2025).

4.2 Descriptive Statistics of Variables

Based on the results of descriptive statistical analysis, it was found that the average value of all research indicators ranged from 3.80 to 4.20. This finding shows that, in general, respondents have a high level of awareness of cyber threats, digital protective behavior, and security communication preferences. The indicator with the highest average value is Y5 (Mean = 4.20), which shows that the majority of respondents strongly agree with the statements in this indicator, so this aspect can be considered the strongest dimension in shaping digital security communication preferences. Conversely, the lowest average scores were obtained for indicators X1 (Mean = 3.80) and M3 (Mean = 3.82), indicating that although respondents have relatively good awareness and protective attitudes, there is still room for improvement in understanding and consistency in applying digital security behaviors.

These findings are in line with research by Imran & Asmoro (2024), which states that Indonesian public awareness of personal data security is quite high, but not evenly distributed across all demographic groups. This shows that some digital users already understand the importance of data protection, while others are still inconsistent in applying everyday cyber security behaviors. Furthermore, research by Kristiyenda & Ramli (2025) confirms that the public's weak understanding of intellectual property rights and digital security can increase the potential for data breaches and the spread of false information, reinforcing the argument that variations in understanding and practice of digital security are still quite high in society. Standard deviation values ranging from 0.829 to 1.145 indicate that the variation in respondents' answers is moderate. The highest standard deviations were found in indicators Y1 (Std. Dev. = 1.145) and M3 (Std. Dev. = 1.104), which means that respondents' perceptions of these two indicators were more diverse than those of other indicators. This shows that there is a group of respondents who already have a good understanding and practice of cybersecurity, but there is also another group that is still inconsistent. These results are in line with the findings of Ginting et al. (2025), which state that low digital literacy and lack of cyber infrastructure are major challenges in raising national awareness of digital threats in Indonesia.

4.3 Evaluation of Measurement Models (Outer Model)

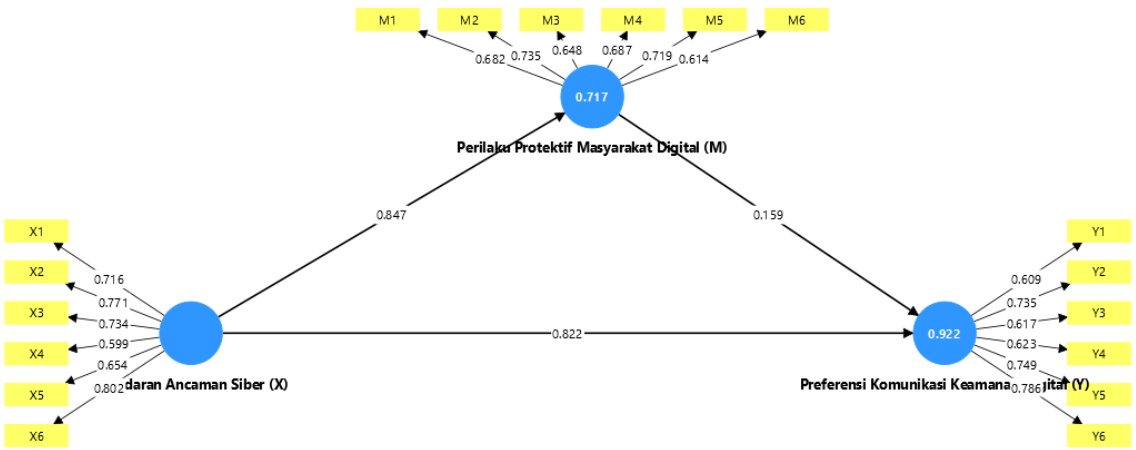

Figure 2. Structural model

The measurement model (outer model) was evaluated to assess whether the indicators used were able to reflect the construct validly and reliably. Convergent validity was tested through factor loading values and Average Variance Extracted (AVE). The analysis results showed that most indicators had loading values above 0.60, thus meeting the minimum threshold for convergent validity. Several indicators, such as X1 (0.716), X2 (0.771), X3 (0.734), X6 (0.802), M2 (0.735), M5 (0.719), Y2 (0.735), Y5 (0.749), and Y6 (0.786) show a strong contribution in explaining the construct. However, there are still indicators with loading values below 0.70, such as X4 (0.599), X5 (0.654), M1 (0.682), M3 (0.648), and M6 (0.614). However, according to the guidelines of Hair et al. (2024), and empirical research by Latif et al. (2025), indicators with loading values ≥ 0.60 can still be retained if the model as a whole show's good measurement performance, especially in exploratory and predictive studies such as the PLS-SEM approach. The AVE values indicate that the Cyber Threat Awareness construct has a value of 0.513, while the Digital Community Protective Behavior and Digital Security Communication Preference constructs have values of 0.465 and 0.476, respectively. The AVE values for the last two constructs are indeed slightly below the minimum threshold of 0.50, but because the values are close to the tolerance threshold, the constructs are still practically acceptable in a predictive PLS-SEM approach (Keefe et al., 2025). Construct reliability was tested using Cronbach's Alpha and Composite Reliability (CR). The test results showed that all constructs had reliability values above 0.70, as shown in Table 1 below.

Table 1. Construct Reliability

Variable	Cronbach's Alpha	Composite Reliability (CR)
Cyber Threat Awareness (X)	0,807	0,862
Protective Behavior of the Digital Society (M)	0,769	0,839
Digital Security Communication Preferences (Y)	0,776	0,844

All latent variables have Cronbach's Alpha and Composite Reliability values greater than 0.70. This indicates that each construct has good internal consistency, so the instrument can be considered reliable. These findings are in line with the results of Vortia (2025) study, which shows that a reliability level above 0.70 is sufficient for measuring online safety behavior constructs based on Protection Motivation Theory (PMT). Furthermore, the results of the discriminant validity test using the Heterotrait-Monotrait Ratio (HTMT) show that the values between constructs range from 1.072 to 1.207. These values slightly exceed the limit of 0.90, which indicates conceptual proximity between variables. A similar phenomenon was also found in a study (Kim, 2025), where constructs related to self-efficacy and cyber awareness had a high correlation because they were in the same security behavior domain. Therefore, the model is still practically acceptable considering that this study is predictive and exploratory in nature. The multicollinearity test shows that all indicators have a Variance Inflation Factor (VIF) value between 1.33 and 2.43. This value is well below the critical limit of 5, indicating that there is no problem of high correlation between indicators. These results are in line with the findings of Hendriawan et al. (2025), which emphasize the importance of multicollinearity stability in PLS models to maintain the accuracy of estimates between constructs in cybersecurity analysis In addition, the Standardized Root Mean Square Residual (SRMR) value of 0.100 and the Normed Fit Index (NFI) value of 0.575 indicate that the model is still at an acceptable level of suitability for the PLS-SEM approach. These values are in line with the model testing standards proposed by Latif et al. (2025), where models with SRMR ≤ 0.10 and NFI > 0.50 can be categorized as suitable for further interpretation.

4.4 Structural Model Evaluation (Inner Model)

The evaluation of the structural model (inner model) aims to assess the relationships between latent constructs and measure the overall predictive ability of the model. This test is conducted by considering the R^2 (Coefficient of Determination), Q^2 (Predictive Relevance), and Effect Size (f^2) values generated through bootstrapping analysis in SmartPLS 4.0. In addition, the relationships between variables are tested to determine the direct and indirect effects between the constructs developed in this research model.

Table 2. Structural Model Evaluation Results (Inner Model)

Construction / Relationship	R^2	Q^2	f^2	Effect Category	Description
Cyber Threat Awareness (X) →Protective Behavior (M)	0,511	0,352	0,473	Large	Significant ($p < 0.05$)
Protective Behavior (M) →Communication Preference (Y)	0,586	0,414	0,317	Moderate	Significant ($p < 0.05$)
Cyber Threat Awareness (X) →Communication Preference (Y)	-	-	0,148	Small	Significant ($p < 0.05$)

The R^2 value shows how much of the endogenous variable can be explained by the exogenous variable. Based on the data processing results, the Digital Community Protective Behavior (M) construct has an R^2 value of 0.511, which means that 51.1% of the variability in protective behavior can be explained by the Cyber Threat Awareness (X) construct. Meanwhile, the Digital Security Communication Preference (Y) construct has an R^2 value of 0.586, which indicates that 58.6% of the variability in digital security communication preferences can be explained by the Cyber Threat Awareness (X) and Protective Behavior (M) variables. Based on Chin's (1998) classification adopted by Hair et al. (2024), an R^2 value between 0.33 and 0.67 is classified as moderate, so this model is considered to have fairly good predictive power for the context of digital behavior.

The Q^2 value (Predictive Relevance) was calculated using the blindfolding approach with an omission distance value (D = 7). The calculation results show that Q^2 for construct M is 0.352 and for construct Y is 0.414. Since all Q^2 values are > 0, it can be concluded that the model has good predictive relevance and is capable of predicting observational data with adequate accuracy (Vortia, 2025). In addition, the f^2 value (Effect Size) is used to assess the strength of the influence between constructs in the structural model. Based on the analysis results, the influence of Cyber Threat Awareness (X) on Protective Behavior (M) has an f^2 value of 0.473, which is categorized as a large effect. Meanwhile, the influence of Protective Behavior (M) on Digital Security Communication Preference (Y) has an f^2 value of 0.317 (moderate effect), and the direct influence of Cyber Threat Awareness (X) on Digital Security Communication Preference (Y) has a value of 0.148 (small effect). This category refers to Cohen (1988), guidelines, where f^2 values ≥ 0.35 are categorized as large, 0.15 as moderate, and 0.02 as small. The bootstrapping test results show that all paths between constructs have t-statistic values > 1.96 and p-values < 0.05, which means that all relationships are statistically significant. Specifically, Cyber Threat Awareness (X) has a significant effect on Protective Behavior (M) and Digital Security Communication Preferences (Y), both directly and through a mediating effect. This shows that the higher an individual's awareness of cyber threats, the more likely they are to engage in protective digital behavior and choose secure communication.

4.5 Hypothesis Testing (Bootstrapping)

Hypothesis testing was conducted to confirm the relationship between latent variables in the structural model through the bootstrapping procedure in SmartPLS 4.0 with 5,000 resampling. This test was used to determine the significance of direct effects, indirect effects, and total effects between constructs. The test results are presented in Table 3 below.

Table 3. Bootstrapping Hypothesis Test Results

Hypothesis Code	Relationship Between Constructs	Path Coefficient (β)	t-Statistic	p-Value	Description
H1	Cyber Threat Awareness (X) → Digital Community Protective Behavior (M)	0,847	11,416	0,000	Significant
H2	Cyber Threat Awareness (X) → Digital Security Communication Preference (Y)	0,822	6,191	0,000	Significant
H3	Digital Community Protective Behavior (M) → Digital Security Communication Preference (Y)	0,159	1,189	0,234	Not Significant
H4	Cyber Threat Awareness (X) → Digital Security Communication Preference (Y) through Protective Behavior (M)	0,135	1,050	0,294	Not Significant

Based on the results of bootstrapping analysis using SmartPLS 4.0, it was found that Cyber Threat Awareness (X) has a positive and significant effect on Digital Community Protective Behavior (M) ($\beta = 0.847$; $t = 11.416$; $p < 0.001$). This means that the higher the level of awareness of cyber risks, the greater the tendency for individuals to take digital protection measures such as changing passwords regularly, avoiding suspicious links, and protecting personal data privacy. This finding is consistent with the research by Latif et al. (2025), which confirms that cybersecurity awareness and self-efficacy are key factors in shaping protective behavior based on Protection Motivation Theory (PMT) in the digital environment of industry 4.0. In addition, Cyber Threat Awareness (X) also has a positive and significant effect on Digital Security Communication Preferences (Y) ($\beta = 0.822$; $t = 6.191$; $p < 0.001$). These results indicate that individuals with high cyber awareness tend to choose more secure communication platforms, for example, through the use of two-factor authentication, message encryption, and strict privacy management. These findings are in line with research (Kim, 2025), which shows that cybersecurity self-efficacy has a significant influence on safe digital behavior and user trust in digital economic activities.

However, the influence of Digital Society Protective Behavior (M) on Digital Security Communication Preferences (Y) was not significant ($\beta = 0.159$; $t = 1.189$; $p = 0.234$). This condition indicates the existence of an intention-behavior gap, where the intention to behave safely is not always realized in practice. A similar phenomenon was also found in Vortia (2025) study, which highlighted that despite high levels of awareness, most young users still prioritize convenience over digital security in their online activities. Furthermore, the results of the mediation effect test show that Protective Behavior (M) does not significantly mediate the relationship between Cyber Threat Awareness (X) and Digital Security Communication Preference (Y) ($\beta = 0.135$; $t = 1.050$; $p = 0.294$). This means that the direct influence of awareness on secure communication preferences is stronger than the indirect effect through protective behavior. These results are consistent with the study by Sajikumar et al. (2024), which found that mobile cybersecurity awareness has a significant direct effect on protective behavior, while the mediating effect of protective motivation is partial. Empirically, the results of this study confirm that Cyber Threat Awareness (X) is a key factor influencing Digital Protective Behavior (M) and Secure Communication Preferences (Y). However, protective behavior does not yet function as a significant mediator, indicating that changes in digital communication preferences tend to occur directly as a result of increased cyber awareness, rather than through changes in behavior first.

4.6 Discussion of Findings

The results of the hypothesis testing using the bootstrapping procedure demonstrate that cyber threat awareness plays a central and dominant role in shaping digital security behavior and communication preferences among the digital society in Semarang City. Specifically, cyber threat awareness has a strong and significant effect on protective behavior ($\beta = 0.847$; $p < 0.001$) as well as a significant direct effect on digital security communication preferences ($\beta = 0.822$; $p < 0.001$). In contrast, protective behavior does not significantly influence communication preferences ($\beta = 0.159$; $p = 0.234$) and does not mediate the relationship between cyber threat awareness and communication preferences ($\beta = 0.135$; $p = 0.294$). These findings indicate that awareness exerts a direct influence on both behavioral and communication-related security outcomes, while protective behavior does not function as a significant intermediary, reflecting the presence of an intention behavior gap in digital security practices.

The strong relationship between cyber threat awareness and protective behavior supports the core assumptions of Protection Motivation Theory (PMT), which posits that threat appraisal and coping appraisal are key drivers of individual security actions. Individuals who are more aware of cyber risks such as phishing, malware, and data breaches tend to be more proactive in implementing protective measures. This finding is consistent with prior studies showing that cybersecurity awareness and self-efficacy are critical predictors of protective intention and response behavior in digitally intensive environments (Latif et al., 2025; Kim, 2025). In the context of Semarang, this relationship is particularly relevant given that the respondent profile is dominated by young, productive-age users with high internet usage intensity, a group that has been widely identified as highly exposed to cyber threats yet uneven in security readiness (Mahipal et al., 2025; Naik, 2025). This pattern is also consistent with the respondent profile, which reflects a digitally intensive urban cohort with balanced gender composition, predominantly tertiary education, and diverse occupational backgrounds, while daily internet use is largely oriented toward social media, e-commerce, work-related activities, and digital financial services contexts frequently associated with elevated exposure to phishing, fraud, and data theft risks (Anggraheni et al., 2024; Afrina et al., 2024; Imran & Asmoro, 2024; Muliawan & Hasnawati, 2024; Lim & Tan, 2025).

Cyber threat awareness also demonstrates a strong and significant direct effect on digital security communication preferences, indicating that individuals with higher awareness levels are more selective in choosing trusted, secure, and credible communication channels. This result aligns with previous research emphasizing that cyber self-efficacy and perceived risk directly shape users' preferences for secure platforms, including the use of encryption and multi-factor authentication (Kim, 2025). From a practical perspective, this finding suggests a shift from convenience-oriented digital behavior toward trust-based communication decisions, where security considerations increasingly influence how individuals engage with digital platforms. However, the non-significant effect of protective behavior on communication preferences highlights an important behavioral inconsistency. Despite having protective habits, individuals do not necessarily apply these practices consistently when selecting communication channels. This intention behavior gap has been widely reported in cybersecurity research, particularly among younger users who often prioritize convenience and speed over security (Vortia (2025). Similar patterns were observed by Hendriawan et al. (2025), who found that digital literacy significantly enhances cybersecurity awareness but does not always translate into sustained cyber resilience or consistent protective practices. These findings suggest that awareness alone is insufficient to ensure behavioral consistency without reinforcing psychological and contextual factors such as motivation, perceived effort, and self-control.

The absence of a significant mediating effect of protective behavior further indicates that cyber threat awareness influences communication preferences primarily through a direct pathway rather than indirectly through habitual security actions. This result is consistent with studies showing that awareness often produces an immediate cognitive and decision-making impact, while routine protective behaviors require longer-term reinforcement to become embedded (Sajikumar et al., 2024; Keefe et al., 2025). In this regard, awareness functions as a trigger factor that shapes security-related judgments and preferences more strongly than established habits. Insights from the descriptive statistics reinforce these structural findings. Although respondents generally reported high levels of cyber threat awareness, protective behavior, and security communication preferences, the moderate variation in responses suggests that not all individuals apply security knowledge consistently. This pattern supports prior evidence that improvements in digital literacy increase awareness but do not automatically result in uniform protective behavior across individuals (Hendriawan et al., 2025). Studies at the community level further emphasize that participatory and practice-oriented training approaches are more effective in translating awareness into consistent protective actions (Syafiih et al., 2024). Simulation-based cybersecurity training has also been shown to enhance preparedness and response capability by bridging the gap between knowledge and practice (Azzani et al., 2024).

From a measurement perspective, the evaluation of the outer model confirms that the research instrument demonstrates adequate reliability and convergent validity. Most indicators achieved acceptable factor loadings, consistent with the exploratory and predictive orientation of PLS-SEM (Hair et al. 2024; Latif et al., 2025). Although AVE values for some constructs were slightly below the ideal threshold, they remained within acceptable tolerance limits for predictive modeling (Keefe et al., 2025). Strong internal consistency, as reflected by Cronbach's Alpha and Composite Reliability values above 0.70, indicates that the constructs were measured reliably. Although HTMT values indicated conceptual proximity among constructs, multicollinearity diagnostics (VIF) remained within acceptable limits, and overall fit indices (e.g., SRMR and NFI) suggested that the measurement model was adequate for predictive interpretation in PLS-SEM (Hair et al. 2024; Latif et al., 2025). These results are consistent with previous studies in the Indonesian digital literacy context, which suggest that minor discriminant validity limitations do not necessarily compromise predictive validity when internal consistency is strong (Syafiih et al., 2024).

Overall, the structural model demonstrates satisfactory predictive accuracy and relevance, as indicated by moderate to high R^2 and Q^2 values. Consistent with this, the model's explanatory and predictive performance (R^2 and Q^2) fall within the moderate-to-strong range, while effect size estimates (f^2) indicate that cyber threat awareness exerts the most substantial contribution to the structural relationships, reinforcing its role as the primary driver of the proposed model (Cohen,1988; Hair et al. 2024). The effect size analysis confirms that cyber threat awareness is the primary driver of both protective behavior and communication preferences. This finding aligns with global cybersecurity behavior models emphasizing that awareness has a stronger direct influence on security-related decisions than indirect effects mediated by habitual practices (Keefe et al., 2025). Collectively, these results support the applicability of Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT) in explaining cybersecurity behavior within an urban digital society context.

Conclusion

This study concludes that cyber threat awareness is a dominant factor that directly influences the protective behavior of the digital society and communication preferences for digital security in the city of Semarang. Bootstrapping test results show that the influence of cyber threat awareness on protective behavior and communication preferences is significant, with path coefficient values of $\beta = 0.847$ and $\beta = 0.822$ ($p < 0.001$), respectively. Meanwhile, the effect of protective behavior on digital security communication preferences is not significant, indicating the existence of an intention-behavior gap among the digital society. Theoretically, these findings reinforce Protection Motivation Theory (PMT) and Technology Threat Avoidance Theory (TTAT) in the context of Indonesian society's cyber security behavior, where awareness and risk perception have been proven to be the main determinants in shaping intentions and preferences for safe digital behavior. In practical terms, this research confirms that strategies to improve cyber literacy and awareness are the most effective measures in shaping protective behavior and preferences for secure communication in the era of urban digitalization.

Recommendations

Based on the results of the study, it is recommended that the government and cybersecurity agencies such as BSSN and Kominfo expand community-based cyber literacy programs with a behavioral communication approach that combines technical education and risk-based persuasive messages to increase public awareness and safe digital behavior. Educational institutions and organizations also need to integrate digital security literacy into their curricula and training through interactive methods such as cyber drill simulations so that protective habits are formed early on. For future researchers, expanding the study area, adding variables such as digital trust and self-efficacy, and using a longitudinal approach are recommended to deepen understanding of the dynamics of digital security behavior among Indonesians. Overall, increasing cyber awareness through cross-sector synergy is key to building a digital society that is secure, adaptive, and resilient in the face of threats in the era of digital transformation 5.0.

REFERENCES

Afrina, C., Zulaikha, S. R., & Jumila. (2024). The Low Level of Digital Literacy in Indonesia: An Analysis of Online Media Content. *Record and Library Journal*, *10*(2), 374–387. https://doi.org/10.20473/RLJ.V10-I2.2024.374-387

Anggraheni, P., Fatharini, A. T., Nurhaqiqi, H., Mustikasari, R. P., Diaz, Y. G., & Gultom, M. N. (2024). The Role of Women in Community Development: Reenacting Digital Activism in Improving Education for All Children, Lesson Learned from Tulungagung and Semarang. *Jurnal Sosial Humaniora*, *17*(2), 219. https://doi.org/10.12962/J24433527.V17I2.20906

Azzani, I. K., Purwantoro, S. A., & Almubarok, H. Z. (2024). Enhancing awareness of cyber crime: a crucial element in confronting the challenges of hybrid warfare In Indonesia. *Defense and Security Studies*, *5*, 1–9. https://doi.org/10.37868/DSS.V5.ID255

Chasanah, B. R., & Candiwan, C. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. *SISFORMA*, *7*(2), 49–57. https://journal.unika.ac.id/index.php/sisforma/article/view/2706

Cohen, J. (1988). Statistical Power Analysis for the Behavioral Sciences. *Statistical Power Analysis for the Behavioral Sciences*, 1–567. https://doi.org/10.4324/9780203771587/STATISTICAL-POWER-ANALYSIS-BEHAVIORAL-SCIENCES-JACOB-COHEN/RIGHTS-AND-PERMISSIONS

Data Pemerintah Dominasi 58 Persen Kebocoran di Dark Web, Platform Baru Ini Tawarkan Deteksi Dini - AWANPINTAR. (n.d.). Retrieved December 14, 2025, from https://www.awanpintar.id/data-pemerintah-dominasi-58-persen-kebocoran-di-dark-web-platform-baru-ini-tawarkan-deteksi-dini/

Dinev, T., & Hu, Q. (n.d.). The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, *8*(7), 386–408. https://doi.org/10.17705/1jais.00133

Duzenci, A., Kitapci, H., & Gok, M. S. (2023). The Role of Decision-Making Styles in Shaping Cybersecurity Compliance Behavior. *Applied Sciences*, *13*(15). https://doi.org/10.3390/APP13158731

Faisal, F., & Zuliarti, W. O. (n.d.). *International Journal of Social Science and Human Research The Awareness Gap in Personal Data Privacy in Indonesia's Cyberspace*. https://doi.org/10.47191/ijsshr/v7-i07-84

Fattah, A., Wagimin, & Nurlia. (2023). Enhancing Cybersecurity Awareness among University Students: A Study on the Relationship between Knowledge, Attitude, Behavior, and Training. *JSI: Jurnal Sistem Informasi (E-Journal)*, *15*(1), 3139–3149. https://doi.org/10.18495/JSI.V15I1.115

Gier, N. R., Krampe, C., & Kenning, P. (2023a). Why it is good to communicate the bad: understanding the influence of message framing in persuasive communication on consumer decision-making processes. *Frontiers in Human Neuroscience*, *17*. https://doi.org/10.3389/FNHUM.2023.1085810/PDF

Gier, N. R., Krampe, C., & Kenning, P. (2023b). Why it is good to communicate the bad: understanding the influence of message framing in persuasive communication on consumer decision-making processes. *Frontiers in Human Neuroscience*, *17*. https://doi.org/10.3389/FNHUM.2023.1085810/PDF

Ginting, R. G., Arifyanto, G. T., & Ghafur, F. (2025). Defending The State in The Digital Domain: Between Cyber Threats and National Awareness. *Cakrawala: Journal of Citizenship Teaching and Learning*, *3*(1), 11–20. https://doi.org/10.70489/8YBGRR82

González-Ponce, B. M., Carmona-Márquez, J., Pilatti, A., Díaz-Batanero, C., & Fernández-Calderón, F. (2024). The protection motivation theory as an explanatory model for intention to use alcohol protective behavioral strategies related to the manner of drinking among young adults. *Alcohol and Alcoholism (Oxford, Oxfordshire)*, *59*(5), agae059. https://doi.org/10.1093/ALCALC/AGAE059

Gusman, S. W. (2024). Development of the Indonesian Government's Digital Transformation. *Dinasti International Journal of Education Management And Social Science*, *5*(5), 1128–1141. https://doi.org/10.38035/DIJEMSS.V5I5.2868

Hair, J. F., Sarstedt, M., Ringle, C. M., Sharma, P. N., & Liengaard, B. D. (2024). Going beyond the untold facts in PLS–SEM and moving forward. *European Journal of Marketing*, *58*(13), 81–106. https://doi.org/10.1108/EJM-08-2023-0645

Hariana, R. R., Hadi, E. N., & Jamal, A. P. (2025). Strengthening Cybersecurity: A Comparative Analysis of Agile Governance in Preventing Data Leakage in Indonesia and Malaysia. *Agile Governance and Innovation Measurement Journal*, *2*(1), 40–58. https://doi.org/10.18196/AGIMJOURNAL.V2I1.23

Hendriawan, A., Gautama, I., Siahaan, D., & Kurniawan, K. (2025). Analysis of The Influence of Factors on Maritime Cyber Resilience on Board With Intervening Maritime Cyber Security Awareness. *Syntax Literate ; Jurnal Ilmiah Indonesia*, *10*(3), 2783–2794. https://doi.org/10.36418/SYNTAX-LITERATE.V10I3.56311

Imran, M. F., & Asmoro, D. (2024). Public Awareness on Data: Case in Indonesian Elections and Advocating For Cybersecurity Reinforcement. *Journal of Governance*, *9*(1). https://doi.org/10.31506/JOG.V9I1.23854

Isabella, I., Alfitri, A., Saptawan, A., Nengyanti, N., & Baharuddin, T. (2024). Empowering Digital Citizenship in Indonesia: Navigating Urgent Digital Literacy Challenges for Effective Digital Governance. *Journal of Governance and Public Policy*, *11*(2), 142–155. https://doi.org/10.18196/JGPP.V11I2.19258

Judijanto, L., Rahardian, R. L., Muthmainah, H. N., & Erkamim, Moh. (2023). Analysis of Threat Detection, Prevention Strategies, and Cyber Risk Management for Computer Network Security in Government

Information Systems in Indonesia. *West Science Information System and Technology*, *1*(02), 90–98. https://doi.org/10.58812/WSIST.V1I02.479

Kaufhold, M. A., Bäumler, J., Bajorski, M., & Reuter, C. (2025). Cyber Threat Awareness, Protective Measures and Communication Preferences in Germany: Implications from Three Representative Surveys (2021-2024). *Conference on Human Factors in Computing Systems - Proceedings*. https://doi.org/10.1145/3706598.3713795

Keefe, D. H. S., Jang, H., & Ercan, E. N. (2025). Digitalization in sustainable agriculture supply chain: how digital literacy and support affect attitudes and adoption intentions. *International Trade, Politics and Development*, *9*(2), 129–144. https://doi.org/10.1108/ITPD-02-2025-0007

Kementerian Komunikasi dan Digital. (n.d.). Retrieved December 14, 2025, from https://www.komdigi.go.id/berita/siaran-pers/detail/imdi-2025-naik-ke-4453-indonesia-makin-cakap-digital

Kementerian Komunikasi dan Informatika Republik Indonesia & Katadata Insight Center. (2023). *Status literasi digital di Indonesia 2023*. https://cdn1.katadata.co.id/media/Report_LITDIG_2023.pdf?utm_source=chatgpt.com

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/10.1016/J.COSE.2022.103049

Kim, S. (2025). Impact of Cybersecurity Self-Efficacy on Digital Economic Behaviors Among Older Adults. *Inquiry: A Journal of Medical Care Organization, Provision and Financing*, *62*. https://doi.org/10.1177/00469580251370933

Klein, G., Zwilling, M., Lesjak, D., Klein, G., Zwilling, M., & Lesjak, D. (1 C.E.). A Comparative Study in Israel and Slovenia Regarding the Awareness, Knowledge, and Behavior Regarding Cyber Security. *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Aspx?Doi=10.4018/978-1-7998-4285-9.Ch007*, 128–147. https://doi.org/10.4018/978-1-7998-4285-9.CH007

Kristiyenda, Y. S., & Ramli, T. S. (2025). IMPLEMENTATION OF INTELLECTUAL PROPERTY LAW AWARENESS AND CYBERSECURITY TECHNOLOGY AGAINST DIGITAL COPYRIGHT VIOLATIONS IN INDONESIA DURING THE 2024 ELECTIONS. *Awang Long Law Review*, *7*(2), 349–358. https://doi.org/10.56301/AWL.V7I2.1548

Latif, S. F. A., Sulaiman, S. N., Aziz, S. N. A., Yacob, A., & Nasir, A. (2025). Development of Cybersecurity Awareness Model Based on Protection Motivation Theory (PMT) for Digital IR 4.0 in Malaysia. *IJACSA) International Journal of Advanced Computer Science and Applications*, *16*(3), 2025. www.ijacsa.thesai.org

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165. https://doi.org/10.1016/J.CHBR.2021.100165

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly: Management Information Systems*, *33*(1), 71–90. https://doi.org/10.2307/20650279

Lim, Y. Z., & Tan, A. J. (2025). Cybersecurity Awareness Among Youth: What's Vital? *PaperASIA*, *41*(2), 166–172. https://doi.org/10.59953/PAPERASIA.V41I2B.334

Mahipal, M., Shivananjappa, N., & Creutzburg, R. (2025). Cybersecurity Awareness Among Young Adults: An Analytical Study. *Electronic Imaging*, *37*(3). https://doi.org/10.2352/EI.2025.37.3.MOBMU-312

Muliawan, D., & Hasnawati, H. (2024). The Influence of Cyber Security Knowledge, Cyber Security Awareness, and Behaviour Protection on Intention to Use Among Mobile Banking Users in Jakarta. *Jurnal Indonesia Sosial Teknologi*, *5*(11), 4904–4916. https://doi.org/10.59141/JIST.V5I11.8763

Naik, G. A. (2025). *Cybersecurity Awareness in Goa: A Descriptive and Inferential Study*. *13*. https://doi.org/10.22214/ijraset.2025.74467

Naqvi, S. G., Alishba, Mughal, M. A., Shehzad, K., & Noor, R. T. (2024). Organizational Environment, Protection Motives, Adoption of Machine Learning, and Cybersecurity Behavior. *Journal of Excellence in Social Sciences*, *3*(4), 11–25. https://doi.org/10.69565/JESS.V3I4.352

Rodríguez-Priego, N., van Bavel, R., Vila, J., & Briggs, P. (2020). Framing Effects on Online Security Behavior. *Frontiers in Psychology*, *11*. https://doi.org/10.3389/FPSYG.2020.527886/PDF

Russo, D., & Stol, K. J. (2022). PLS-SEM for software engineering research: An introduction and survey. *ACM Computing Surveys*, *54*(4). https://doi.org/10.1145/3447580;SUBPAGE:STRING:ABSTRACT;WEBSITE:WEBSITE:DL-

SITE;REQUESTEDJOURNAL:JOURNAL:CSUR;TAXONOMY:TAXONOMY:ACM-PUBTYPE;PAGEGROUP:STRING:PUBLICATION

Sajikumar, S., Ajithkumar, N., & Vijayan, G. (2024). Exploring the Interplay of Privacy Concerns, Mobile Cybersecurity Awareness, and Protective Motivation Behavior. *International Journal of Religion*, *5*(5), 612–619. https://doi.org/10.61707/KQYQ0505

Santos, C. P., Rodríguez González, V., Zenaida, N., Pineda, D., Diz-Casal, J., Carlos Fernández-Rodríguez, J., José, J., & Morán, D. (2025). The Role of the Human Factor in the Cybersecurity Ecosystem. *Journal of Information Systems Engineering and Management*, *10*(4), 217–229. https://doi.org/10.52783/JISEM.V10I4.8983

Searle, R., & Renaud, K. (n.d.). *Trust and Vulnerability in the Cybersecurity Context*. Retrieved December 14, 2025, from https://hdl.handle.net/10125/103273

Searle, R., & Renaud, K. (2023). Trust and Vulnerability in the Cybersecurity Context. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2023-January*, 5228–5240. https://doi.org/10.24251/HICSS.2023.639

Serac, C. A. (2023). DIGITAL TRANSFORMATION VULNERABILITIES: ASSESSING THE RISKS AND STRENGTHENING CYBER SECURITY. *THE ANNALS OF THE UNIVERSITY OF ORADEA. ECONOMIC SCIENCES*, *3*(1), 771–781. https://doi.org/10.47535/1991AUOES32(1)059

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. *Information 2022, Vol. 13, Page 413*, *13*(9), 413. https://doi.org/10.3390/INFO13090413

Syafiih, M., Nadiyah, Khairi, M., Furqan, Moh., & Yusman, B. (2024). Pendampingan Literasi Digital untuk Mengurangi Risiko Kejahatan Siber Membentuk Masyarakat yang Lebih Aman. *JILPI : Jurnal Ilmiah Pengabdian Dan Inovasi*, *2*(4), 1027–1036. https://doi.org/10.57248/JILPI.V2I4.456

Tatara, B. A., Abdurachman, B., Mustofa, D. L., & Yacobus, D. (2023). The Potential of Cyber Attacks in Indonesia's Digital Economy Transformation. *NUANSA: Jurnal Penelitian Ilmu Sosial Dan Keagamaan Islam*, *20*(1), 19–37. https://doi.org/10.19105/NUANSA.V20I1.7362

Vortia, W. (2025). Modelling cybersecurity awareness, perceived threats and secure online behavioral intentions among Ghanaian university students: A PLS-SEM Approach. *Magna Scientia Advanced Research and Reviews*, *14*(2), 096–111. https://doi.org/10.30574/MSARR.2025.14.2.0094

Vrhovec, S., & Fujs, D. (n.d.). Are Perceptions About Government and Social Media Providers Related to Protection Motivation Online? *International Journal of Cyber Behavior*, *13*(1). https://doi.org/10.4018/IJCBPL.324085

Wibowo, B., Hafiz, L., & Hidayat, T. (2025). Unveiling the Cybercrime Ecosystem: Impact of Ransomware-as-a-Service (RaaS) in Indonesia. *International Journal of Science Education and Cultural Studies*, *4*(1), 11–21. https://doi.org/10.58291/IJSECS.V4I1.320

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;WGROUP:STRING:PUBLICATION

KUISIONER PENELITIAN

Halo Warga Digital Semarang!
Kami adalah tim peneliti dari Universitas BPD Semarang yang saat ini sedang melakukan penelitian berjudul:
"**Analisis Tingkat Kesadaran Ancaman Siber, Perilaku Protektif, dan Preferensi Komunikasi pada Masyarakat Digital di Kota Semarang**."
Penelitian ini bertujuan untuk memahami bagaimana masyarakat Semarang **menyadari risiko keamanan siber, menerapkan perilaku perlindungan digital**, serta memilih cara dan sumber komunikasi keamanan yang mereka percayai.
Hasil penelitian ini diharapkan dapat memberikan kontribusi nyata dalam meningkatkan literasi dan keamanan digital masyarakat, khususnya di era transformasi digital saat ini.
Kami sangat berterima kasih apabila Anda bersedia meluangkan beberapa menit untuk mengisi kuesioner ini.
Seluruh jawaban Anda akan dijaga kerahasiaannya, tidak akan dipublikasikan secara individu, dan hanya digunakan untuk kepentingan akademik.

Partisipasi Anda sangat berarti dalam mendukung terciptanya masyarakat digital yang lebih aman, sadar, dan tangguh terhadap ancaman siber.
Terima kasih atas waktu dan kerja samanya! 🌐💻

Hormat kami,
Tim Peneliti
Universitas BPD Semarang

Data Demografi Responden
Berikan tanda centang (√) pada jawaban yang sesuai

1. Usia: _____ tahun
2. Jenis kelamin: ☐ Laki-laki ☐ Perempuan
3. Pendidikan terakhir: ☐ SMA ☐ Diploma ☐ S1 ☐ S2/S3
4. Pekerjaan: _____
5. Frekuensi penggunaan internet per hari: ☐ <1 jam ☐ 1–3 jam ☐ 4–6 jam ☐ >6 jam
6. Penggunaan utama internet: ☐ Media sosial ☐ Belanja daring ☐ Layanan keuangan ☐ Pekerjaan ☐ Lainnya

1 = Sangat Tidak Setuju | 2 = Tidak Setuju | 3 = Netral | 4 = Setuju | 5 = Sangat Setuju

A. Kesadaran Ancaman Siber (X)
(Adaptasi dari Kaufhold et al., 2025; Zwilling et al., 2022; Dinev & Hu, 2007)

NO	Pertanyaan	1	2	3	4	5
1	Saya mengetahui berbagai jenis ancaman siber seperti *phishing*, *malware*, dan pencurian data pribadi.					
2	Saya memahami konsekuensi yang dapat timbul jika data pribadi saya dicuri secara *online*.					
3	Saya mampu mengenali tanda-tanda serangan siber, seperti tautan mencurigakan atau pesan palsu.					
4	Saya merasa ancaman siber dapat menimpa siapa saja, termasuk saya sendiri.					
5	Saya secara aktif mencari informasi terbaru tentang keamanan digital dari sumber terpercaya.					
6	Saya yakin bahwa kesadaran terhadap ancaman siber penting untuk menjaga keamanan pribadi saya di dunia digital.					

B. Preferensi Komunikasi Keamanan Digital (Y)
(Diadaptasi dari Li et al., 2022; Liang & Xue, 2009; Sulaiman et al., 2022)

NO	Pertanyaan	1	2	3	4	5
1	Saya selalu menggunakan kata sandi yang kuat dan berbeda untuk setiap akun digital.					
2	Saya rutin memperbarui sistem operasi dan aplikasi di perangkat saya.					

3	Saya menggunakan autentikasi dua faktor *(two-factor authentication*) untuk melindungi akun digital saya.					
4	Saya berhati-hati dalam membagikan informasi pribadi melalui internet.					
5	Saya segera mengambil tindakan jika mendeteksi aktivitas mencurigakan di akun digital saya.					
6	Saya memiliki keyakinan bahwa tindakan pencegahan pribadi saya cukup efektif melindungi dari ancaman siber.					

C. Perilaku Protektif Masyarakat Digital (M)

(Diadaptasi dari Searle & Renaud, 2023; Rodríguez-Priego et al., 2020; Vrhovec & Fujs, 2023)

NO	Pertanyaan	1	2	3	4	5
1	Saya lebih percaya pada informasi keamanan digital yang disampaikan oleh lembaga resmi seperti Kominfo atau BSSN.					
2	Saya lebih menyukai pesan keamanan yang disampaikan secara singkat dan mudah dipahami.					
3	Saya lebih tertarik pada pesan keamanan siber yang menampilkan contoh kasus nyata, seperti kehilangan akun, kebocoran data pribadi, atau kerugian finansial akibat serangan siber.					
4	Saya cenderung mengikuti saran keamanan siber yang disampaikan melalui akun media sosial tepercaya, seperti akun resmi pemerintah, media berita kredibel, atau institusi keamanan digital.					
5	Saya merasa pesan keamanan lebih meyakinkan jika disertai bukti atau data faktual.					
6	Saya lebih mudah memahami pesan keamanan yang disampaikan dalam bentuk visual seperti video atau infografis.					

Terima kasih banyak atas waktu dan partisipasi Anda dalam mengisi kuesioner ini
Setiap jawaban yang Anda berikan sangat berharga bagi kami untuk memahami bagaimana masyarakat digital di Kota Semarang menyikapi ancaman siber, menerapkan perilaku protektif, dan memilih cara komunikasi keamanan yang dianggap paling terpercaya.
Seluruh data yang Anda berikan akan dijaga **kerahasiaannya** sepenuhnya dan hanya digunakan untuk kepentingan akademik dan pengembangan literasi keamanan digital di Indonesia.

Semoga hasil penelitian ini dapat memberikan kontribusi nyata dalam membangun masyarakat digital yang **lebih sadar, aman, dan tangguh terhadap risiko siber.**
Sekali lagi, terima kasih atas kerja sama dan dukungan Anda 💻🌐

Hormat kami,
Tim Peneliti
Universitas BPD Semarang