SMATIKA : STIKI Informatika Jurnal
Accredited Sinta 4 Ministry of Higher Education, Science and Technology Republic of Indonesia SK No. 79/E/KPT/2023
E-ISSN: 2580-6939 || P-ISSN: 2087-0256

Cybersecurity Awareness and Community Response to Phishing Threats: An Indonesian Social Behavior Analysis

Fadhil Rozi Hendrawan*, Arif Rahman Hakim[2], Dewi Marini Umi Atmaja[3] ,Zaidan Mufaddhal[4]

[1,2,3] *Telkom University, Industrial Engineering, Information Systems, Minangkabau West Street No. 50, RT. 1/RW. 1, Ps. Manggis, Setiabudi District, South Jakarta City, Special Capital Region of Jakarta 12970*

[4,] *Huazhong University of Science and Technology, School of Artificial Intelligence and Automation, No. 1037 Luoyu Road, Hongshan District, Wuhan, Hubei, China*

Keyword

Indonesia; Online Behavior; Phishing Cybercrime; Risk Management; Socio-Cultural Perspective

Corresponding Author:
fadhilrozihendrawan@telkomuniversity.ac.id

Abstract

This research discusses the increased levels of connectivity and digital engagement experienced by the people of Indonesia due to the development of digital technology as well as the risks associated with the growing prevalence of phishing cyber crimes in the country despite having the third-highest population of internet users globally. Although the level of digital literacy varies across different regions in the country, younger users in Indonesia appear to be the most vulnerable to phishing attacks. In view of the above, this paper seeks to identify and explore the behavioral dimensions that determine vulnerability to phishing amongst young internet users in Indonesia through a qualitative exploration of behavioral exposure towards such cyber crime. The research employs a quantitative cross-sectional survey method using structured questionnaires provided to 53 participants in their teens who were frequently involved in using digital platforms for purposes such as engaging on social media, making purchases from e-commerce sites, and executing payments via digital platforms, all chosen using a purposive sample method. Validity and reliability were measured using the Principal Component Analysis, the Kaiser-Meyer-Olkin validity test, Bartlett's Test of Sphericity and Cronbach's Alpha test respectively. Validity tests produced a KMO measure of 0.587 with a statistically significant Bartlett test result (χ^2=71.940, df=10, p<0.001). Using PCA, two factors contributing 70.997% cumulative variance were identified with Eigenvalue values of 2.299(45.98%) and 1.251(25.02%). The first factor measures active reception of links via digital platforms and the second measures exposure to bypassing attempts via OTP channels. The four-item scale had a Cronbach Alpha of 0.743 implying acceptable internal consistency.

1. Introduction

The rapid growth of internet users and digital platforms in Indonesia has expanded opportunities for connectivity and economic participation; however, it has simultaneously increased exposure to cybersecurity threats, particularly phishing cybercrime a form of deceptive online manipulation that exploits communication channels to obtain sensitive information such as passwords, financial data, and personal

identities[1]. Indonesia ranks among the countries with the largest internet user populations globally, yet cybersecurity awareness and digital literacy remain uneven across demographic groups and regions, leaving many users especially young people vulnerable to phishing attacks, online fraud, and social engineering [2]. The growing number of cyber incidents in Indonesia demonstrates that phishing is not merely a technical problem but a human and behavioral one, shaped by online habits, trust patterns, risk perception, and the socio-cultural environment in which users engage with digital platforms [3]. Consequently, cybersecurity awareness has become a crucial factor in shaping safe online behavior and reducing susceptibility to cybercrime [4]. The increasing number of cyber incidents worldwide demonstrates that digital crime is transboundary and can affect anyone regardless of age, profession, or social background; therefore, strengthening cybersecurity awareness, improving digital literacy, and understanding the socio-cultural dimensions of online behavior are essential steps toward enhancing cyber resilience and promoting safer digital practices in Indonesia.

Table 1. Respondents' Experience and Exposure to Phishing Cybercrime

Type of Implementation	Result
Never implementation any violations	74.00%
Have Implementation (total)	
Less than 5 times	13.00%
Less than 3 times	2.30%
Less than 10 times	0.50%
Email account hacked	4.20%
Social media accounts hacked	23.20%
Hearing cases from friends/family	
Heard it once	33.50%
1-5 Times	46.20%
More than 5 times	17.50%

Implementation of cybersecurity awareness programs and preventative measures among survey participants remains inconsistent. According to the survey results, 74% of participants reported not having engaged in any activities that violated cybersecurity measures. However, 13% reported experiencing fewer than five cyber incidents, 2.3% fewer than three, and 0.5% fewer than ten. Regarding experiences with cyberattacks, 4.2% reported having their email accounts compromised, and 23.2% reported having their social media accounts compromised. Furthermore, awareness of cybersecurity incidents in the surrounding environment was relatively high, with 33.5% of participants reporting hearing about such incidents from friends or family at least once, 46.2% 1-5 times, and 17.5% 5 or more times [5]. These results highlight the importance of continuous cybersecurity awareness and education programs, as opportunities to directly experience cybersecurity incidents are relatively low, but exposure to them through social circles is very high . With the increasing prevalence of advanced authentication technologies, such as biometrics, multifactor authentication, and token-based security systems, usernames and passwords remain the dominant form of digital authentication. However, many users prioritize convenience over security and reuse the same or similar passwords across multiple platforms and accounts. This habit significantly increases the risk of cyberattacks, particularly credential theft, phishing, and account breaches. In Indonesia, a lack of public awareness regarding the safe use of digital technologies and the inconsistent implementation of cybersecurity measures in daily life exacerbate these risks [6].

Table 2. Cybersecurity Behavior Research

Factor Category	Specific Variables	Key Research Findings	Geographic Context
Demographics – Age	Age groups, generational differences	Older adults tend to be more cautious about cyber risks but may experience lower digital literacy, while younger users demonstrate higher technological familiarity but often engage in riskier online behavior.	Serbia, Malaysia, Western countries
Demographics – Gender	Risk tolerance, cybersecurity behavior	Existing findings show mixed results regarding gender differences in cybersecurity behavior. Some studies indicate women are more likely to adopt safer online practices, while males often report slightly higher risk-taking tendencies.	Serbia, Malaysia, International studies
Demographics – Education	Educational level, digital literacy	Higher educational attainment is generally associated with better cybersecurity awareness and stronger information security practices. Individuals with greater digital literacy are more capable of identifying cyber threats and protecting personal data.	Malaysia, healthcare sector, international studies
Risk Perception	Perceived vulnerability, threat awareness, security confidence	Stronger perceptions of cybersecurity risks encourage individuals to adopt safer online behavior. Risk awareness also influences protective actions such as password management and verification of suspicious digital content.	US, Malaysia, Saudi Arabia, International
Cyber Incident Experience	Previous phishing incidents, victimization experience	Individuals who have previously experienced phishing attacks or cyber incidents tend to demonstrate greater awareness and more cautious online behavior in future digital interactions.	Various international studies, online environments
Technology Use	Digital dependency, platform usage, internet engagement	Frequent use of social media, e-commerce, and digital payment platforms increases exposure to cyber threats. Intensive digital engagement may also contribute to risky online habits and oversharing of personal information.	Philippines, Hong Kong, global/international context

Previous studies indicate that there is a relation between cybersecurity awareness and behaviors, and some determinants such as demographics, digital literacy, perceived risk, and socio-cultural aspects. The above factors determine the level at which internet users understand cyber risks and behave in order to protect themselves from phishing attacks. In developing countries such as Indonesia, cybersecurity awareness and digital skills may differ from each other, posing a threat to users. Young people aged 17–25 represent the most digitally active segment of Indonesia's internet user population and constitute the primary focus of this study. This demographic engages intensively with social media, e-commerce, digital payment services, and online communication platforms, making them both frequent targets of phishing attacks and key agents in shaping responsible digital culture [6] . Despite their technological familiarity, risky online behaviors persist within this group with including impulsive responses to unverified messages, inadequate account security practices, and over-sharing of personal information, behaviors that phishing and social engineering techniques are specifically designed to exploit [7]. The complexity of cybersecurity awareness in Indonesia is closely linked to the country's socio-cultural diversity and differences in digital literacy. Indonesia's diverse population, ranging from urban to rural areas, results in significant regional disparities in access to technology, education, and information infrastructure. While urban areas generally have broader internet access and more opportunities to participate in digital literacy campaigns, rural areas often face limitations regarding infrastructure, educational resources, and cybersecurity awareness programs. Consequently, these differences in digital competence influence how individuals perceive and respond to cyber threats. Individual responses to cybersecurity issues are also influenced by social trust, peer influence, group norms, and local cultural practices, which can proactively promote or discourage digital behavior [8].

Despite the growing body of cybersecurity literature, previous studies have mainly focused on technical protection mechanisms, regulatory compliance, and organizational security practices. Limited empirical research has investigated how socio-cultural factors influence cybersecurity awareness and online behavior

related to phishing attacks in Indonesia. Furthermore, most existing studies focus on urban populations and rely on international frameworks that may not fully reflect Indonesian digital culture and communication patterns. Therefore, this study aims to examine cybersecurity awareness and online behavior against phishing cybercrime from a socio-cultural perspective among young Indonesian internet users.

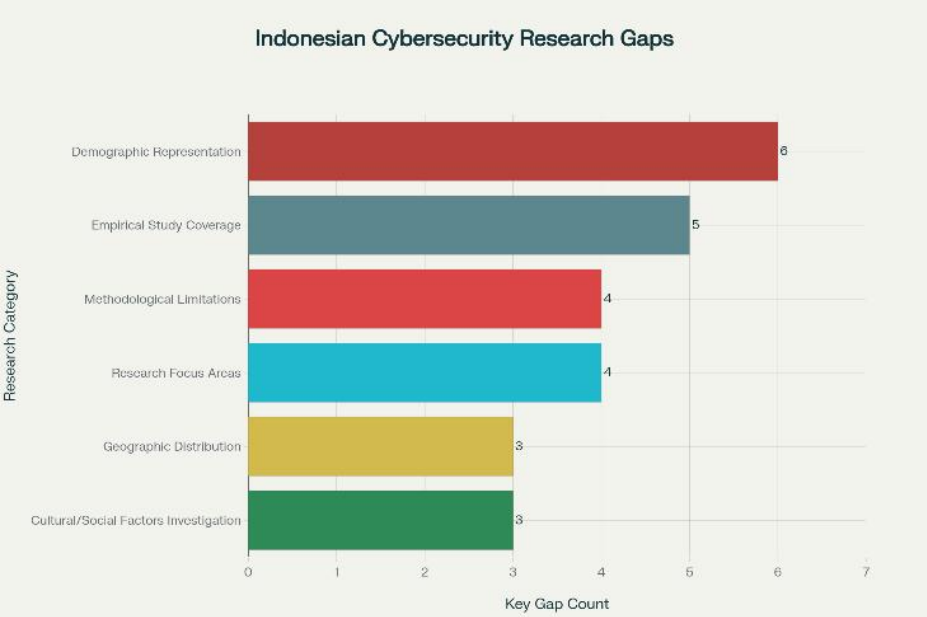

Figure 1. Indonesian Cybersecurity Research Gaps

This study investigates the relationship between cybersecurity awareness and online behavior against phishing cybercrime among Indonesian internet users aged 17–25, with socio-cultural context treated as an interpretive lens rather than a directly measured construct. Using a quantitative approachA sample size of 53 participants was deemed adequate for EFA based on the criterion set forth by suggesting a minimum ratio of subjects to items of 5:1. With an original questionnaires consisting of six items, the minimum sample size required should be 30 subjectsf. Therefore, the collected sample exceeded this threshold and was considered adequate for factor extraction and reliability assessment.. The study contributes to the literature by providing empirical evidence of the awareness–behavior relationship within Indonesia's specific digital environment, and by identifying behavioral patterns that context-sensitive cybersecurity education programs should address. While socio-cultural variables such as trust-based communication norms and collective online behavior are not operationalized as independent constructs in the analysis, they are drawn upon to interpret the behavioral findings within their local context [9]. Their cybersecurity awareness, critical thinking skills, and sense of digital responsibility will have a significant impact on the future resilience of Indonesian digital society [10]. The Indonesian government and various stakeholders recognize these challenges and have therefore launched numerous initiatives to increase cybersecurity awareness, strengthen digital systems, and promote safer internet use [11]. Therefore, it is becoming increasingly important to understand the relationship between cybersecurity awareness and digital behavior when developing strategies tailored to the unique characteristics of Indonesian society. This research aims to investigate how knowledge and awareness of cyber threats influence people's attitudes, decision-making processes, and digital habits, particularly among general internet users. The research also emphasizes the importance of socio-cultural factors in shaping cybersecurity behavior and acknowledges the need to support technical solutions with cultural adaptation and community involvement. The results of this research are expected to contribute to the development of more effective and comprehensive public strategies and policies in the field of cybersecurity education, taking into account the local context [12].

2. Research Method

This study employed a quantitative cross-sectional survey design to examine phishing-related behavioral exposure among young Indonesian internet users. A structured questionnaire was used as the primary data collection instrument, enabling systematic measurement of participants' behavioral patterns in relation to phishing cybercrime. This design was selected because it allows efficient collection of standardized data across a defined population at a single point in time, making it suitable for exploratory factor analysis and psychometric instrument development in a behavioral cybersecurity context [13].

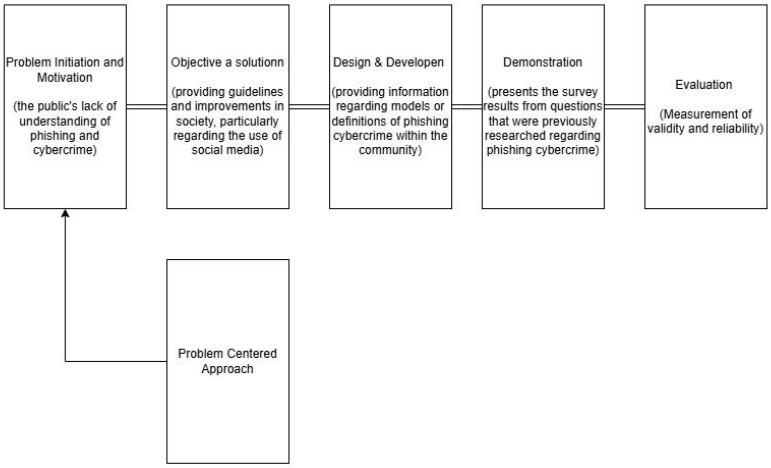

Figure 2. Design Science Research of Phishing Cybersecurity

This study adopted the Design Science Research (DSR) methodology to investigate cybersecurity awareness and online behaviors related to phishing cybercrime in Indonesia, following the established framework for information system artifact development and evaluation [15]. The first stage of research is the Problem Identification and Motivation, which emphasizes the growing number of phishing attacks in spite of the rapidly increasing use of digital technologies and lack of public knowledge on cybersecurity measures. The second stage – Define Objectives for a Solution – sets the objective of improving cybersecurity awareness and promoting healthier online behaviors from the socio-cultural standpoint. For achieving this goal, the study combines elements of already existent cybersecurity and data governance theories, namely ISO 27001, NIST Cybersecurity Framework, and DAMA-DMBOK, to construct a conceptual view of factors that can influence phishing susceptibility of Indonesian internet users.

Design and Development stage includes creating a questionnaire instrument and conceptual measurement model in relation to phishing awareness and behavior. This tool will be employed in the Demonstration stage in the form of a survey administered to active internet users aged 17–25 years. Information received from the questionnaire helps to explore individuals' experiences of phishing attacks and their knowledge about cybersecurity measures. Furthermore, the Evaluation stage consists of assessing the quality of the developed instrument based on validity and reliability testing with the help of such criteria as Kaiser-Meyer-Olkin (KMO) measure, Bartlett's Test of Sphericity, and Cronbach's Alpha. Thus, findings provided by the evaluation test give empirical evidence on the effectiveness of the measurement model in question.

2.1 Data Collection

The data collection process took place in January–February 2026, using an online self-administrated questionnaire that was conducted using Google forms. The questionnaire was sent out on WhatsApp groups, Instagram, and LINE chat groups where there is high interaction among young people who are either students or working professionals in Indonesia. It was voluntary for participants to take part in the study, and they were made aware of the scholarly objective behind the research before answering the questions.

Personal details were not recorded from the participants. The online method of data collection was chosen because the research population is quite active on the

2.2 Validity and Reliability

Construct validity was assessed using the Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and Bartlett's Test of Sphericity, followed by Principal Component Analysis (PCA) to examine the underlying factor structure of the instrument. The KMO test was used to determine whether the data were suitable for factor analysis by evaluating the proportion of variance among variables that may be attributed to common factors; values above 0.50 are considered acceptable [14]. Bartlett's Test confirmed whether the correlation matrix was significantly different from an identity matrix, a necessary condition for meaningful factor extraction [13].

Following PCA, items with factor loadings below the accepted threshold of 0.40 were removed from the scale Internal consistency reliability of the retained items was subsequently assessed using Cronbach's Alpha, with a minimum threshold of 0.70 considered acceptable for social science research All statistical analyses were performed using IBM SPSS tools [16].

2.3 Cybersecurity Implementation

The concept of cybersecurity awareness has evolved significantly with the rapid development of digital technologies and online communication, and the increase in phishing crimes in modern society [17]. With the expansion of Internet usage, cybersecurity awareness is no longer viewed solely as a technical issue, but also as an issue concerning individual behavior and sociocultural aspects in the digital environment. Various international frameworks have offered different perspectives on the application of cybersecurity awareness, especially to mitigate user exposure to cyber threats such as phishing attacks, identity theft, online fraud, and social engineering. Among these frameworks, ISO 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the DAMA DMBOK Guide are particularly prominent. These offer complementary approaches to improving cybersecurity awareness, improving data governance, and promoting safe online behavior [18]. Although these frameworks share the common goal of strengthening cybersecurity resilience, each reflects its own unique philosophical foundation, governance mechanisms, and operational strategies. Organizations and communities should consider these points when developing comprehensive cybersecurity awareness programs [19].

The concept of cybersecurity awareness has evolved significantly alongside the rapid development of digital technologies and online communication, and the documented increase in phishing crimes in modern society[20]. With the expansion of internet usage, cybersecurity awareness is no longer viewed solely as a technical issue, but also as a matter of individual behavior and sociocultural context in the digital environment[20]. Various international frameworks have offered complementary perspectives on applying cybersecurity awareness to mitigate user exposure to cyber threats such as phishing attacks, identity theft, online fraud, and social engineering. Among these, ISO 27001, the National Institute of Standards and Technology (NIST) Cybersecurity Framework, and the DAMA DMBOK Guide are particularly prominent, each reflecting a distinct philosophical foundation, governance mechanism, and operational strategy [21]. This framework uses a risk-based approach, requiring organizations to identify potential cybersecurity risks, including phishing attacks, and implement appropriate measures through awareness initiatives, security policies, and systematic training programs. In addition, ISO 27001 emphasizes the importance of adapting awareness strategies to user roles, responsibilities, and digital exposure levels to ensure effective mitigation of cyber risks in diverse organizational environments. The implementation process follows a Plan-Do-Check-Act (PDCA) cycle, enabling organizations to continually improve their cybersecurity awareness practices in response to emerging threats and evolving online behavior patterns [22].

The implementation of this standard follows a Plan-Do-Check-Act (PDCA) cycle, enabling organizations to continually improve their cybersecurity awareness practices in response to emerging threats and evolving online behavior patterns. In parallel, the National Institute of Standards and Technology (NIST) Cybersecurity

Framework focuses on cybersecurity awareness through five core functions identify, protect, detect, respond, and recover that work together to support proactive cybersecurity management and user preparedness against phishing attacks [19]. This framework emphasizes user behavior, incident response capabilities, and the continuous improvement of security practices. Meanwhile, the Data Management Body of Knowledge (DAMA DMBOK) provides a perspective on data governance emphasizing the importance of data quality, protection, access management, and responsible information processing to mitigate cybersecurity vulnerabilities [23]. Integrating these two frameworks provides a comprehensive foundation for understanding the relationship between cybersecurity awareness and online behavior, especially in countries undergoing rapid digital transformation, such as Indonesia. In the sociocultural context of Indonesia, factors such as collective social norms, trust-based communication patterns, active social interaction on social networks, and digital literacy disparities significantly influence users' vulnerability to phishing attacks. Despite increasing awareness of cyber threats, many internet users still engage in risky online behaviors, such as using weak passwords, over-sharing personal information, and failing to properly screen suspicious digital content. Therefore, raising awareness of cybersecurity through education, policymaking, and digital literacy initiatives that consider sociocultural contexts is essential to promote safe online behavior and strengthen Indonesia's national capacity to combat cyber phishing [24].

Table 3. Comparation of framework in security awareness

Framework	Definition	Focus Analysis	Approach	Component
ISO 27001	Security Awareness in ISMS	Into security control & risk register	Systematic ISMS Implementation	Training, Awareness, Competence
NIST	Understand Cyber threats & protection	Risk based cyber framework function	Identify, Protect, Detect, Recover	Training, Campaign, Behavior Change
DAMA DMBOK V2	Data Security Awareness in Management	Data Governance & Security Management	Knowledge and Integration	Data Stewardship, Control, Governance

A comparative analysis of cybersecurity awareness across the ISO 27001, NIST, and DAMA DMBOK frameworks shows that effective defense against phishing cybercrime requires a multidimensional approach integrating technical, behavioral, and sociocultural aspects [25]. Across these frameworks, cybersecurity awareness is consistently positioned as a strategic element to mitigate human vulnerability to digital threats, particularly phishing attacks that exploit the trust, emotional responses, and limited digital literacy of online users. These frameworks emphasize the importance of fostering responsible online behavior, improving individual decision-making skills, and cultivating a security-conscious digital culture, rather than focusing solely on technical defense mechanisms. In Indonesia, where internet penetration and social media usage continue to grow rapidly, the importance of cybersecurity awareness is growing as users are more exposed to fraudulent online activities, deceptive messages, fake digital platforms, and identity-based cyber fraud [26].

ISO 27001 addresses cybersecurity awareness through a structured information security management system (ISMS) that prioritizes governance, accountability, and continuous risk reduction [27]. This framework emphasizes the need to embed awareness programs into organizational processes and support them with measurable controls, internal assessments, and policy enforcement mechanisms [28]. Meanwhile, the NIST Cybersecurity Framework places greater emphasis on adaptability and functionality, focusing on proactive risk identification, threat detection, incident response preparedness, and user readiness against emerging phishing techniques. In addition, the DAMA DMBOK introduces a data governance perspective, emphasizing the importance of data protection, information integrity, access management, and responsible handling of digital information to mitigate exposure to cyber threats. Integrating these frameworks leads to a broader understanding that cybersecurity awareness is not only about recognizing cyber risks, but also about developing sustainable behavioral patterns that support safe digital interactions and responsible information sharing practices.

Furthermore, the development of phishing cybercrime indicates that cyberattacks are increasingly exploiting sociocultural characteristics and human psychology, rather than relying solely on technical system vulnerabilities. In Indonesia, cultural trends such as collective trust, frequent online interaction, and heavy reliance on digital communication platforms may inadvertently increase vulnerability to phishing and social engineering attacks. Many users remain vulnerable due to habits such as clicking on unverified links, reusing passwords, disclosing personal information, and failing to monitor suspicious digital communications. These behavioral patterns indicate that cybersecurity programs need to be designed not only from a technical perspective, but also by considering the sociocultural dynamics of local communities and the disparities in digital literacy between different communities [29]. Therefore, integrating international cybersecurity frameworks with sociocultural understanding can help develop more contextually aware strategies, strengthen cyber resilience, and promote safer online behavior among Indonesian internet users facing increasingly sophisticated phishing cybercrimes [30].

3. Result and Discussions

3.1 Respondent Characteristic

The respondent profile in this study was identified based on the intensity of digital platform utilization, especially in activities involving social media, online communication, and digital services. Analyzing respondent characteristics is essential to understand patterns of online behavior, levels of cybersecurity awareness, and the potential exposure of internet users to phishing cybercrime and other digital threats. The findings show that the majority of participants consist of individuals with frequent interaction in digital environments, indicating a high dependency on internet-based platforms in everyday activities. This condition reflects the growing importance of cybersecurity awareness in shaping safer online behavior among Indonesian digital users. The dominant respondent group consists primarily of young individuals aged 17–25 who actively engage with social media platforms for communication, entertainment, education, and social interaction. Although this group demonstrates strong familiarity with digital technology and high levels of online connectivity, many users still exhibit risky online behavior, including oversharing personal information, interacting with unverified content, and responding impulsively to suspicious digital messages. Such behavioral tendencies increase vulnerability to phishing cybercrime and social engineering attacks that frequently exploit emotional responses and trust-based communication patterns.

In addition, a significant proportion of respondents are students and early-career professionals who depend heavily on digital applications to support academic, organizational, and professional activities. This group generally possesses a higher understanding of digital technology and recognizes the importance of protecting personal information; however, cybersecurity risks remain prevalent due to insecure password practices, repeated password usage, insufficient account verification, and the use of shared or unsecured devices. Furthermore, active users of e-commerce platforms and digital financial services represent another major respondent category within this study. The intensive use of online shopping applications, mobile banking, and digital payment systems increases awareness of cyber risks, but simultaneously expands exposure to phishing attempts, fraudulent transactions, and online scams targeting financial information. These findings demonstrate that frequent digital engagement does not necessarily guarantee strong cybersecurity behavior, emphasizing the need for continuous cybersecurity awareness and socio-culturally adaptive digital literacy initiatives in Indonesia.

3.2 Question for Respondents

The profiles of respondents in this survey were identified based on their frequency of use of digital platforms, especially in activities such as social networking, online communication, and digital services. Analyzing the characteristics of the respondents is essential to understand patterns of online behavior, levels of cybersecurity awareness, and the likelihood that internet users will be exposed to phishing and other digital threats. The survey results indicate that the majority of participants are people who frequently interact in the digital environment and are highly dependent on online platforms in their daily lives. This situation reflects

the increasing importance of cybersecurity awareness in shaping safer online behavior among digital users in Indonesia.

Table 4. Dimension of Variable of Phishing Crime

Dimension	Variable	Reference
Phising Cybercrime (PC)	PC1. Do you often receive links through website services? PC2. Do you often receive links through social media services? PC3. How much do you know about phishing-related knowledge? PC4. How often do you receive links via the WhatsApp application? PC5. Have you ever received a digital code in the form of a link, such as an OTP? PC6. How often do you receive OTPs in your WhatsApp application?	[31], [32],[33]

The majority of survey participants are young people aged 17 to 25 who actively use social media for communication, entertainment, education and social interaction. Despite their technological savvy and high internet connectivity, many still engage in risky behaviors, such as over-sharing personal information, interacting with unverified content and responding impulsively to suspicious digital messages. These behaviors increase their vulnerability to phishing, cybercrime and social engineering that exploit emotions and trusting communication patterns.

Furthermore, students and young professionals make up a significant portion of the participants, who heavily use digital applications to support their studies, organizational activities and career aspirations. Although this group generally has a good understanding of digital technology and recognizes the importance of protecting personal information, cybersecurity risks persist due to practices such as using weak passwords, reusing passwords, inadequate account authentication and using shared or unsecured devices. Active users of e-commerce platforms and digital financial services also represent a large segment of the survey participants. With the increasing use of e-commerce applications, mobile banking and digital payment systems, awareness of cyber risks is growing. However, this is also accompanied by an increase in exposure to online fraud, phishing and financial scams. These results show that frequent use of digital technologies does not necessarily guarantee the implementation of effective cybersecurity measures, highlighting the need for ongoing cybersecurity awareness and the provision of socio-culturally informed digital education programs in Indonesia.

3.3 Validity

To evaluate the validity of the indices used in this study, the Kaiser-Meyer-Olkin (KMO) sample validity test and the Bartlett sphericity test were performed to determine the suitability of the data for factor analysis. These tests are important for assessing whether the variables related to cybersecurity awareness and online behavior when faced with phishing crimes have a sufficiently correlated structure for further statistical analysis. The KMO test measures the fit of the sample distribution, and the Bartlett test examines the significance of the correlation matrix between variables. The results of these validity tests indicate that the database is suitable for factor analysis and can be used to identify underlying dimensions related to phishing behavior in the socio-cultural context of Indonesian internet users.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.587
Bartlett's Test of Sphericity	Approx. Chi-Square	71.940
	df	10
	Sig.	<,001

Figure 3. Validity KMO and Bartlett's Test of Phishing Crime

A validation assessment revealed that the database met the requirements for factor analysis. The Kaiser-Meier-Olkin (KMO) goodness-of-fit score was 0.587, exceeding the acceptable threshold of 0.50, indicating a sufficient sample size to study the relationships between variables related to cybersecurity awareness and online behavior against phishing attacks. In addition, Bartlett's test for sphericity yielded a chi-square value of 71.940 with 10 degrees of freedom and a significance level less than 0.001, confirming that the correlation matrix was statistically significant and suitable for factor extraction using principal component analysis (PCA).

Further analysis of the extracted components revealed two principal components with eigenvalues greater than 1, both showing effective contributions to explaining the observed variance of the data. Factor 1, with an eigenvalue of 2.299, explained 45.98% of the total variance, while Factor 2, with an eigenvalue of 1.251, explained 25.02% of the variance. These two factors together accounted for 70.997% of the cumulative variance, demonstrating strong ability to explain patterns related to participants' perceptions of fishing and their online behavioral tendencies. Furthermore, the rounded factor solutions showed a more even distribution of variance, with the first factor explaining 44.74% of the total variance and the second factor explaining 26.25%, indicating a relatively balanced factor structure within the study model.

3.4 Reliability

The initial six-item scale (PC1–PC6) was subjected to PCA as described in Section C. Following extraction, two items were removed based on standard psychometric criteria: PC3 ("How much do you know about phishing-related knowledge?") and PC6 ("How often do you receive OTPs in your WhatsApp application?") were excluded because their factor loadings fell below the accepted threshold of 0.40 [14], indicating insufficient contribution to either extracted component. PC3 was additionally noted as conceptually distinct from the behavioral exposure items — it measures self-reported knowledge rather than behavioral frequency, which may explain its weak loading pattern relative to the remaining items. PC6 showed overlap with PC5 in content coverage, contributing to its low discriminant loading. The four retained items (PC1, PC2, PC4, PC5) demonstrated sufficient loading on the two extracted factors and formed the basis for reliability analysis.

Reliability

Scale: Phising Cybercrime

Case Processing Summary

		N	%
Cases	Valid	53	100.0
	Excluded[a]	0	.0
	Total	53	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.743	4

Figure 4. Reliability of Phishing Crime

A reliability test was conducted to determine the internal consistency of the instrument on the Phishing Cybercrime construct. Based on the analysis results Figure 4All statistical analyses were performed using it was found that the number of respondents used was 53 people with a total of 4 items analyzed after undergoing a validity test using PCA. The Cronbach's Alpha value obtained was 0.743, which is above the minimum threshold of 0.70. This value not only exceeds the conventional 0.70 threshold but also comfortably clears the more lenient 0.60 benchmark considered acceptable for exploratory research of this kind [14], reinforcing that the four-item Phishing Cybercrime scale demonstrates adequate internal consistency despite the relatively small sample size. so it can be concluded that this instrument has good reliability. Thus, the four items in the Phishing Cybercrime construct can be declared consistent and suitable for use as measurements in this study.

The validation process revealed that the collected data were fit for exploratory factor analysis, as evidenced by a KMO measure of 0.587 and a statistically significant result on the Bartlett's Test of Sphericity ($p < 0.001$). While the KMO measure falls under the moderate category, it meets the requirement of a KMO measure higher than the recommended level of 0.50 and similar results in studies of exploratory cybersecurity awareness [34]. This pattern of moderate sampling adequacy combined with a well-defined multidimensional factor structure is consistent with previous exploratory factor analysis studies. A five-factor structure explaining 60.922% of the total variance, with an overall Cronbach's Alpha of 0.780, has also been reported for cybersecurity awareness behavior among university students [38]. Although the explained variance in that study was lower than the 70.997% obtained in the present study, the findings similarly demonstrate that multidimensional latent constructs can be identified with satisfactory reliability, even when based on relatively compact measurement instruments. Comparable exploratory research involving a relatively small sample size ($n = 30$) reported a Kaiser–Meyer–Olkin (KMO) value of 0.346 together with an acceptable Cronbach's Alpha of 0.803, indicating that satisfactory internal consistency may still be achieved even when sampling adequacy is relatively low in exploratory behavioral studies [39]. In comparison, the KMO value of 0.587 obtained in the present study indicates moderate sampling adequacy while maintaining a substantially higher level of explained variance through a two-factor structure. Taken together, these findings suggest that the psychometric characteristics of the proposed instrument are consistent with those commonly reported in exploratory studies on cybersecurity awareness and online behavior, supporting the suitability of the instrument for exploratory factor analysis despite the relatively modest sample size [38], [39].

The high frequency of obtaining moderate KMO measures for research on cybersecurity behavior and phishing vulnerability studies is associated with the behavioral and perceptual measures included in such

research. These components explain 70.997% of the cumulative variance. From the perspective of behavioral construct validity, such multifactoriality means that the phishing vulnerability of the sample cannot be described by one behavioral construct but requires a multicomponent structure. Specifically, the first component seems to represent exposure to phishing links spread through various websites and online channels. In contrast, the second component appears to represent exposure to authentication-related phishing attacks, including phishing with OTPs. This conceptual separation between link-based exposure and credential-bypass exposure is broadly consistent with the multidimensional structure proposed in established information security awareness instruments such as the HAIS-Q, which similarly treats different categories of risky online behavior as psychometrically distinct rather than collapsing them into a single undifferentiated awareness construct [34], [35]. In other words, the emergence of two principal components can be interpreted as evidence of the role of different modes of digital interaction in phishing vulnerability.

Table 5. comparison of Current Findings with Previous Studies on Phishing Vulnerability and Cybersecurity Awareness

Research Context	Main Findings	Simmilarity With Curent Study	Reference
Information security awareness	Awareness consists of multiple dimensions.	Similar to the two-factor structure found in this study.	[35]
Phishing susceptibility	Susceptibility is influenced by cognitive and behavioral factors.	Supports the multidimensional nature of phishing vulnerability.	[36]
Phishing attack channels	Websites and social media are major phishing vectors.	Similar to Factor 1 (website/social media exposure).	[37]
Cybersecurity awareness scale validation	Five-factor structure explaining 60.922% cumulative variance; Cronbach's Alpha 0.780.	Comparable multidimensional structure and high explained variance (vs. 70.997% here).	[38]
Online behavioral indicator development	KMO of 0.346 (poor) with a comparably small sample (n = 30); Cronbach's Alpha 0.803.	Shows a moderate KMO (0.587 here) is not disqualifying in small-sample exploratory research.	[39]

The removal of items PC3 and PC6 further demonstrates interesting behavioral traits of the study sample. As noted earlier, PC3 represents the variable of phishing knowledge. However, the weak loading of this variable indicates the absence of correspondence between cybersecurity knowledge and secure online behavior. This relationship has been observed repeatedly in cybersecurity awareness literature. Similarly, item PC6 was removed due to its conceptual closeness to another item (PC5), measuring exposure to OTP-based attacks. Thus, the removal of this item made sense because of the relatively low discriminative power of PC6. From the socio-cultural perspective specific to the Indonesian population, the findings suggest that interpersonal trust communication, heavy social media use, and intensive online interactions play a central role in making the sample population vulnerable to phishing.

4. Conclusions and Future Works

As mentioned above, the current exploratory factor analysis aimed at identifying specific behaviors related to susceptibility to phishing attacks among young Indonesian netizens aged 17-25 years old. According to the findings obtained, phishing-related behavior among young people in this country is multidimensional and can be described as comprising two separate dimensions. First of all, the obtained results reveal that Factor 1 (with eigenvalue equal to 2.299 and accounting for 45.98% of the total variance) represents the frequency of

receiving links in the form of active phishing behavior on social media and websites. This behavior can also be referred to as a manifestation of how often users experience phishing-related activities online. As for the second factor, its eigenvalue equals 1.251, which explains that it accounts for 25.02% of the variance. This factor describes phishing activities that target users' accounts using authentication bypass and include obtaining access to the user's profile with OTPs via WhatsApp messages. The two dimensions identified explained 70.997% of the cumulative variance, thus proving the reliability of the instrument used to determine them. It is important to note that the obtained data confirm the validity of the instrument applied since the value of the KMO test equals 0.587 and Bartlett's Test of Sphericity yields $\chi^2 = 71.940$ ($df = 10$; $p < 0.001$). Internal consistency was confirmed using the Cronbach's Alpha test, which yielded 0.743, which is higher than the minimum acceptable value. Thus, according to the obtained results, many young people continue to have risky behavior online, despite their high level of digital knowledge: they react impulsively to suspicious links received, use improper means to secure accounts, and share too much personal information online. Additionally, it is necessary to mention that socio-cultural factors like reliance on trustworthy relationships and high social media activity increase the risk of being a target of phishing and social engineering among young people, who tend to interact with each other collectively and in large groups online. There are several potential limitations associated with the current study. First of all, it should be noted that due to its cross-sectional nature, it cannot make any assumptions regarding the causation between cybersecurity awareness and behavior online. Although the sample size was sufficient enough to conduct the exploratory analysis (n=53), it is characterized by high diversity and homogeneity, as it comprised mostly active netizens.

5. References

[1] A. A. Vărzaru and C. G. Bocean, "Digital Transformation and Innovation: The Influence of Digital Technologies on Turnover from Innovation Activities and Types of Innovation," *Systems*, vol. 12, no. 9, p. 359, 2024, doi: 10.3390/systems12090359.

[2] E. Wijaya, D. P. Wulan, and T. D. Nursanti, "Exploring Millennial Security Awareness of Data Protection, Cybercrime, and Privacy Management in Indonesia," in *2025 International Conference on Computer Science, Engineering and Technology Innovation (ICoCSETI)*, 2025, pp. 858–863. doi: 10.1109/ICOCSETI63724.2025.11019204.

[3] T. Bui, E. Clemons, and K. Streff, "Information Security and Privacy," in *Proceedings of the Annual Hawaii International Conference on System Sciences*, 2018, p. 4702. doi: 10.1201/b18827-22.

[4] H. Omotunde and M. Ahmed, "A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond," *Mesopotamian J. Cyber Secur.*, pp. 115–133, 2023, doi: 10.58496/MJCSC/2023/016.

[5] H. Sama and S. E. Prasetyo, "The Cyber Threat Landscape in Indonesia: Attacks and Security System Analysis," *SMATIKA*, vol. 16, no. 1, pp. 148–156, 2026, doi: 10.32664/smatika.v16i01.2200.

[6] M. W. M. Al-Quran, "Traditional Media versus Social Media: Challenges and Opportunities," *Tech. Rom. J. Appl. Sci. Technol.*, vol. 4, no. 10, pp. 145–160, 2022, doi: 10.47577/technium.v4i10.8012.

[7] S. Creese, W. H. Dutton, and P. Esteve-González, "The Social and Cultural Shaping of Cybersecurity Capacity Building: A Comparative Study of Nations and Regions," *Pers. Ubiquitous Comput.*, vol. 25, no. 5, pp. 941–955, 2021, doi: 10.1007/s00779-021-01569-6.

[8] W. Febriyani, T. F. Kusumasari, and M. Lubis, "An Narrative Review on Achieving Data Governance in Indonesia Amidst Data Security Challenges," vol. 6, no. 158, pp. 785–792, 2023.

[9] S. B. MacKenzie, P. M. Podsakoff, and C. B. Jarvis, "The Problem of Measurement Model Misspecification in Behavioral and Organizational Research and Some Recommended Solutions," *J. Appl. Psychol.*, vol. 90, no. 4, pp. 710–730, 2005, doi: 10.1037/0021-9010.90.4.710.

[10] F. R. Hendrawan, T. F. Kusumasari, and D. Praditya, "A Comprehensive Framework of Role Data Governance in Ensuring Data Quality: Literature Review," in *2023 Eighth International Conference on Informatics and Computing (ICIC)*, 2023. doi: 10.1109/ICIC60109.2023.10381991.

[11] T. Oketunji and O. Omodara, "Design of Data Warehouse and Business Intelligence System," Master Thesis, 2011.

[12] M. Yunus and M. Yunus, "Klasifikasi Sentimen Terhadap Badan Penyelenggara Jaminan Sosial (BPJS) Pada Media Sosial Twitter Menggunakan Naive Bayes," *SMATIKA*, vol. 11, pp. 81–91, 2021, doi: 10.32664/smatika.v11i02.577.

[13] M. S. Ummah, "DRM, A Design Research Methodology," 2019.

[14] J. F. Hair, W. C. Black, B. J. Babin, and R. E. Anderson, *Multivariate Data Analysis: A Global Perspective*. Upper Saddle River, NJ: Pearson, 2010.

[15] A. R. Hevner, S. T. March, J. Park, and S. Ram, "Design Science in Information Systems Research," *MIS Q.*, vol. 28, no. 1, pp. 75–105, 2004, doi: 10.2307/25148625.

[16] N. H. A. Hardani *et al.*, *Buku Metode Penelitian Kualitatif*. 2020.

[17] A. P. Nugraha, A. Kurnia, P. I. P. Putra, A. Rahman, and D. Dikrurahman, "The Impact of Social Media on Social Interaction and Self-Identity in Indonesian Society," *J. Soc. Res.*, vol. 3, no. 9, pp. 1–8, 2024, doi: 10.55324/josr.v3i9.2254.

[18] R. Tanti, "Phishing Attack: A Case Study and Their Prevention Techniques," 2024, doi: 10.55041/IJSREM38042.

[19] T. Moore, "The NIST Cybersecurity," 2024.

[20] ISO/IEC 27001 International Standard, "Information Security, Cybersecurity and Privacy Protection -- Information Security Management Systems -- Requirements," 2013.

[21] M. Yasin, A. A. Arman, I. J. M. Edward, and W. Shalannanda, "Designing Information Security Governance Recommendations and Roadmap Using COBIT 2019 Framework and ISO 27001:2013 (Case Study Ditreskrimsus Polda XYZ)," in *Proceedings of the 14th International Conference on Telecommunication Systems, Services, and Applications (TSSA)*, 2020, pp. 3–7. doi: 10.1109/TSSA51342.2020.9310875.

[22] R. Fauzi, "Implementasi Awal Sistem Manajemen Keamanan Informasi pada UKM Menggunakan Kontrol ISO/IEC 27002," *JTERA (Jurnal Teknol. Rekayasa)*, vol. 3, no. 2, pp. 145–156, 2018, doi: 10.31544/jtera.v3.i2.2018.145-156.

[23] DAMA International Technics, *DAMA-DMBOK: Data Management Body of Knowledge: 2nd Edition*. 2017.

[24] S. Wadho, A. Meghji, A. Yichiet, R. Kumar, and F. Shaikh, "Encryption Techniques and Algorithms to Combat Cybersecurity Attacks: A Review," *VAWKUM Trans. Comput. Sci.*, vol. 11, pp. 295–305, 2023, doi: 10.21015/vtcs.v11i1.1521.

[25] F. R. Hendrawan, S. A. Aafiyah, and Z. Mufaddhal, "Adapting DAMA DMBOK Principles for Strengthening Data Security Governance: Digital Transformation in MSMEs," 2025, doi: 10.52661/jict.v7i2.476.

[26] V. K. Septiyana, S. Sutikno, and K. Surendro, "Design of e-Government Security Governance System Using COBIT 2019," in *International Conference on Information Systems Security (ICISS)*, 2020, pp. 1–6. doi: 10.1109/ICISS48059.2019.8969808.

[27] M. A. Lanure, F. Maulana, and M. Lubis, "Assessment of IT Maturity Level and Roadmap Preparation for Improving Governance Based on COBIT 5 (Case Study: XYZ Company)," in *1st International Conference on Information Systems and Information Technology (ICISIT)*, 2022, pp. 31–36. doi:

10.1109/ICISIT54091.2022.9872860.

[28] S. De Haes and W. Van Grembergen, "COBIT as a Framework for Enterprise Governance of IT," in *Enterprise Governance of Information Technology*, 2015. doi: 10.1007/978-3-319-14547-1_5.

[29] M. Lubis and F. A. Maulana, "Information and Electronic Transaction Law Effectiveness (UU-ITE) in Indonesia," in *Proceedings of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M)*, 2010, pp. C–13--C–19. doi: 10.1109/ICT4M.2010.5971892.

[30] M. Lubis, R. Fauzi, A. R. Lubis, and R. Fauzi, "Analysis of Project Integration on Smart Parking System in Telkom University," in *2018 6th International Conference on Cyber and IT Service Management (CITSM)*, 2019. doi: 10.1109/CITSM.2018.8674270.

[31] J. H. Pengabdian and P. Masyarakat, "https://journal.unm.ac.id/index.php/JHP2M," vol. 2, pp. 1–8, 2023.

[32] F. Primarius, N. Koten, A. Jufriansah, and H. Hikmatiar, "Analisis Penggunaan Aplikasi WhatsApp sebagai Media Informasi dalam Pembelajaran: Literature Review," pp. 72–84, 2022, doi: 10.37640/jip.v14i1.1409.

[33] M. B. Yel and M. K. M. Nasution, "Keamanan Informasi Data Pribadi pada Media Sosial," *J. Ilmu Komput.*, vol. 6, no. 1, pp. 92–101, 2022, doi: 10.59697/jik.v6i1.144.

[34] K. Parsons, A. Mccormac, M. Butavicius, M. Pattinson, and C. Jerram, "ScienceDirect Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[35] K. Parsons, D. Calic, M. Pattinson, M. Butavicius, A. McCormac, and T. Zwaans, "The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies," *Comput. & Secur.*, vol. 66, pp. 40–51, 2017, doi: 10.1016/j.cose.2017.01.004.

[36] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, and F. Cetin, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *J. Comput. Inf. Syst.*, pp. 1–16, 2020, doi: 10.1080/08874417.2020.1712269.

[37] T. Wangchuk and T. A. D. Gonsalves, "Multimodal Phishing Detection on Social Networking Sites: A Systematic Review,"*IEEE Access*, vol. 13, pp. 103405–103416, 2025, doi: 10.1109/ACCESS.2025.3579584.

[38] L. Bognár and L. Bottyán, "Evaluating Online Security Behavior: Development and Validation of a Personal Cybersecurity Awareness Scale for University Students," *Educ. Sci.*, vol. 14, no. 6, p. 588, 2024, doi: 10.3390/educsci14060588.

[39] S. K. Al-Romaihi and R. A. Ikuesan, "Cyberbullying Indicator as a Precursor to a Cyber Construct Development," *in Proceedings of the International Conference on Cyber Warfare and Security*, 2022.