Cyber Security and Network Management E-ISSN: 3124-0054

Research Article

A Social Engineering Mitigation Model Based on Digital Security Literacy for Social Media Users in Indonesia

Diana Novita [1]*, Hanifah [2], and Agus Herwanto [3]

[1] Universitas Esa Unggul, Indonesia; e-mail : diana.novita@esaunggul.ac.id
[2] Sekolah Tinggi Ilmu Bisnis, Indonesia; e-mail : hanifah@stiebi.ac.id
[3] Universitas Esa Unggul, Indonesia; e-mail : agus.herwanto@esaunggul.ac.id
* Corresponding Author : diana.novita@esaunggul.ac.id

Abstract: The development of digital technology and the increasing use of social media in Indonesia have expanded people's communication activities, but have also increased the risk of security attacks based on human manipulation or social engineering. These attacks exploit user behavioral weaknesses rather than technical system vulnerabilities, thus posing a significant threat in the modern information security ecosystem. This study aims to develop a social engineering mitigation model based on digital security literacy to increase social media user awareness. The research method uses a quantitative approach with a survey technique of 210 respondents who are active social media users in Indonesia. Data were analyzed using Structural Equation Modeling–Partial Least Square (SEM-PLS) to examine the relationship between digital security literacy, cybersecurity awareness, and user vulnerability to social engineering attacks. The results show that digital security literacy significantly increases user awareness ($\beta = 0.71$; $p < 0.001$) and can reduce attack vulnerability by 64%. This finding emphasizes the importance of a human-centric cybersecurity approach that places humans as the primary layer of defense in digital security. The proposed mitigation model includes continuous digital security education, increased security awareness, and the implementation of adaptive authentication as a preventive strategy against social engineering attacks. This research provides practical contributions to the development of user behavior-based information security strategies and provides recommendations for educational institutions, organizations, and policymakers in strengthening the digital security resilience of Indonesian society.

Keywords: Social Engineering, Digital Security Literacy, Cybersecurity, Social Media, Human-Centered Security.

Received: March 01, 2026
Revised: March 29, 2026
Accepted: April 21, 2026
Published: May 31, 2026
Curr. Ver.: May 31, 2026

Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY SA) license (https://creativecommons.org/licenses/by-sa/4.0/)

1. Introduction

Digital transformation has brought significant changes to the communication and interaction patterns of modern society. The development of internet technology and the increasing use of social media in Indonesia have encouraged people to engage in various digital activities, from social communication and economic transactions to real-time information exchange. Recent data shows that internet penetration rates in Indonesia continue to increase annually, making social media a primary interaction space for digital communities.

However, this increased connectivity is also accompanied by a growing risk of increasingly complex and adaptive cybersecurity threats (Verizon, 2023). One cybersecurity threat that has seen a significant increase is social engineering attacks. Unlike attacks based on technical exploits, social engineering targets human psychology as the primary weakness of information security systems. Attackers exploit social manipulation such as trust, emotional pressure, panic, or situational urgency to obtain sensitive information without having to technically hack the system (Mitnick & Simon, 2011). These attack techniques include phishing,

identity impersonation, baiting, and digital communication manipulation to mimic official institutions (Hadnagy, 2018).

The increasing phenomenon of social engineering attacks demonstrates that modern security technologies such as firewalls, encryption, and intrusion detection systems are not fully capable of protecting users if the human factor is not addressed. Global security reports indicate that the majority of information security breaches involve human error or low user digital security awareness (ENISA, 2022). This situation demonstrates that cybersecurity is no longer solely a technological issue, but also a matter of public behavior and digital literacy. Several previous studies have focused on the development of technology-based security systems, such as malware detection, network analysis, and system-based authentication. However, these approaches still have limitations because they have not optimally integrated user behavior as a key component of information security defense (Sasse & Flechais, 2005). Research on digital security literacy as a social engineering mitigation strategy is still relatively limited, particularly in the socio-cultural context of social media users in Indonesia, which have unique digital interaction characteristics.

Based on these issues, a human-centric cybersecurity approach is needed that positions users as the first line of defense (human firewall) against the threat of social manipulation. Digital security literacy is a crucial factor in enhancing users' ability to recognize attack patterns, verify information, and make secure decisions in the digital environment (Ng, 2012). Research by Parsons et al. (2017) shows that increased security awareness can significantly reduce the success of phishing and social manipulation attacks. This study aims to analyze the influence of digital security literacy on the level of vigilance of social media users and develop a social engineering mitigation model based on user behavior. The research approach uses a quantitative method with Structural Equation Modeling–Partial Least Square (SEM-PLS) analysis to comprehensively examine the relationship between variables. The main contribution of this study lies in the development of a digital security mitigation model based on user literacy that is relevant to the characteristics of Indonesia's digital society. The results are expected to serve as a strategic reference for educational institutions, organizations, and policymakers in enhancing national cybersecurity resilience through educational and preventive approaches. Social engineering is a psychological manipulation technique to obtain sensitive information. Digital security literacy plays a crucial role in increasing user awareness of digital threats. The human-centric cybersecurity approach places humans as the primary layer of defense.

State of the Art and Research Gap Cybersecurity research continues to evolve in line with the rise of global digital threats. Previous studies have examined social engineering from the perspective of security technology, user behavior, and organizational mitigation strategies. However, approaches that integrate digital security literacy with the behavioral characteristics of social media users in Indonesia are still limited. Mitnick and Simon (2011) explain that social engineering is a psychological manipulation technique that exploits human trust as a key vulnerability in information security. This research confirms that humans are often the most effective entry point compared to technical system exploits. Furthermore, Hadnagy (2018) developed the concept of human hacking, emphasizing that attack success is heavily influenced by factors such as emotion, authority, and social urgency.

Workman (2008) examined user psychological factors in social engineering attacks and found that trust levels and social pressure increase the likelihood of victims disclosing sensitive information. Meanwhile, Parsons et al. (2017) demonstrated that increasing security awareness through information security training can significantly reduce the success of phishing attacks.

Another study by Heartfield and Loukas (2016) focused on an intelligent system-based attack detection approach. The study successfully identified social engineering attack patterns using digital behavior analysis, but still placed technology at the center of security solutions. A similar approach is also found in the research of Krombholz et al. (2015), which emphasized the classification of attack techniques without considering user literacy as a key preventative factor. On the other hand, the concept of human-centric cybersecurity introduced by Sasse and Flechais (2005) began to shift the security paradigm from technology-centered security to a human-centered approach. This approach emphasizes that users should be positioned as human firewalls through increased digital security literacy and changes in security behavior.

Although various studies have addressed social engineering, several research gaps remain:

a. Most studies focus on technical solutions rather than user literacy factors.
b. Empirical studies based on social media user behavior in Indonesia are still limited.

c. Not many studies integrate digital security literacy into social engineering mitigation models based on quantitative structural analysis.

Based on this gap, this research offers novelty in the form of developing a social engineering mitigation model based on digital security literacy using the Structural Equation Modeling–Partial Least Squares (SEM-PLS) approach. This model integrates aspects of user security knowledge, awareness, and behavior as key variables in reducing vulnerability to social engineering attacks.

Table 1. State of the Art Table of Previous Research.

Researcher	Research Focus	Method	Limitations	Contribution of the Present Study
Mitnick & Simon (2011)	Konsep social engineering	Studi konseptual	Tidak empiris	Model empiris berbasis data
Workman (2008)	Faktor psikologis korban	Behavioral study	Tidak integrasi literasi digital	Integrasi literasi keamanan
Parsons et al. (2017)	Security awareness	Survey	Fokus organisasi	Fokus pengguna media sosial
Heartfield & Loukas (2016)	Deteksi teknis	Machine learning	Technology-centered	Human-centered model
Krombholz et al. (2015)	Klasifikasi serangan	Analisis serangan	Tidak mitigasi perilaku	Model mitigasi preventif

2. Research Methodology

Research Design

This study uses a quantitative explanatory approach to test the causal relationship between digital security literacy, cyber awareness, and vulnerability to social engineering attacks. This approach was chosen because it allows for empirical testing of the conceptual model through latent variable-based statistical analysis (Hair et al., 2019). The research design is cross-sectional, with data collected once during the study period through an online survey of social media users in Indonesia.

Research Conceptual Model

This study adopts the Human-Centric Cybersecurity paradigm, which positions humans as the primary component of information security defense.

Conceptual Relationship :

Digital Security Literacy → Cyber Awareness → Social Engineering Vulnerability
Digital Security Literacy also has a direct influence on Social Engineering Vulnerabity.

Research Model

Digital Security Literacy (X)

↓

Cyber Awareness (Z)

↓

Social Engineering Vulnerability (Y)

Research Variables

In this section, you need to describe the proposed method step by step. Explanations accompanied by equations and flow diagrams as illustrations will make it easier for readers to understand your research.

Variable	Type	Operational Definition
Literasi Keamanan Digital	Independen (X)	Kemampuan memahami, mengenali, dan menerapkan praktik keamanan digital
Kewaspadaan Siber	Mediasi (Z)	Tingkat kesadaran dan kehati-hatian terhadap ancaman digital
Kerentanan Social Engineering	Dependen (Y)	Tingkat kemungkinan pengguna menjadi korban manipulasi sosial

Population and Sample

The study population was all active social media users in Indonesia.

Respondent Criteria

a. Actively using social media for at least 6 months
b. Have a personal digital account
c. Aged ≥18 years

The sampling technique used was purposive sampling.
Sample size: 210 respondents.
This number meets the SEM-PLS rules:
Minimum sample = 10 × the largest number of indicators (Hair et al., 2019).

Data Collection Techniques

Data were collected using:

a. Online questionnaire (Google Form)
b. 5-point Likert scale4. Results and Discussion

Skor	Kategori
1	Sangat Tidak Setuju
2	Tidak Setuju
3	Netral
4	Setuju
5	Sangat Setuju

The instrument was adapted from previous information security research (Parsons et al., 2017).

Variable Measurement Indicators

Digital Security Literacy (X)

Kode	Indikator
X1	Memahami ancaman phishing
X2	Mengetahui praktik password aman
X3	Memverifikasi sumber informasi
X4	Memahami privasi digital
X5	Kesadaran perlindungan data

Cyber Awareness (Z)

Kode	Indikator
Z1	Skeptis terhadap pesan mencurigakan
Z2	Melakukan verifikasi identitas
Z3	Tidak mudah klik tautan
Z4	Respons terhadap ancaman digital

Social Engineering Vulnerabilities (Y)

Kode	Indikator
Y1	Mudah percaya pesan online
Y2	Pernah membagikan data pribadi
Y3	Klik link tanpa verifikasi
Y4	Mengabaikan peringatan keamanan

Data Analysis Techniques

The analysis used Structural Equation Modeling–Partial Least Squares (SEM-PLS) using SmartPLS software.

Measurement Model Evaluation (Outer Model)

Used to test construct validity and reliability.

Convergent Validity

Criteria:

a. Loading Factor > 0.70
b. AVE > 0.50

Table :

Variabel	AVE	Status
Literasi Digital	0.67	Valid
Kewaspadaan Siber	0.71	Valid
Kerentanan SE	0.65	Valid

Reliability Test

Variabel	Cronbach Alpha	Composite Reliability
Literasi Digital	0.89	0.92
Kewaspadaan Siber	0.91	0.93
Kerentanan SE	0.87	0.90

Kriteria:

a. Alpha > 0.70
b. CR > 0.70

All constructs were declared reliable.

Discriminant Validity

Tested using:

a. Fornell-Larcker Criterion
b. Cross Loading

Results show that each construct has the highest correlation value with its own variable, thus meeting discriminant validity.

Structural Model Evaluation (Inner Model)

Used to test the strength of the relationship between variables

R-Square

Variabel Endogen	R^2
Kewaspadaan Siber	0.58
Kerentanan SE	0.64

Interpretation:

The model has strong predictive ability.

Effect Size (f^2)

Relationship f^2

X → Z 0.45 (large)

Z → Y 0.39 (large)

Predictive Relevance (Q^2)

Q^2=0.41 (>0)

The model has good predictive relevance.

Hypothesis Testing (Bootstrapping)

Bootstrapping was performed with 5,000 subsamples.

Hypothesis Path β T-stat P-value Decision

H1 X → Z 0.71 11.32 <0.001 Accepted

H2 X → Y -0.42 6.87 <0.001 Accepted

H3 Z → Y -0.53 9.15 <0.001 Accepted

H4 X → Z → Y -0.31 5.92 <0.001 Significant mediation

Model Interpretation

The results show:

a. Digital security literacy increases user awareness.
b. Cyber awareness reduces the risk of social engineering.
c. The human factor is a critical component of modern digital security.

This model supports the Human-Centric Cybersecurity approach.

3. Results and Discussion

Respondent Profile

The study involved 210 respondents who are active social media users in Indonesia. Respondent characteristics are presented in the following table.

Characteristics Category Percentage
Gender Male 46%
Female 54%
Age 18–25 years 41%
26–35 years 37%
>35 years 22%
Dominant platform: Instagram 38%
WhatsApp 34%
TikTok 28%

The majority of respondents are from the productive generation with high levels of digital interaction, making them relevant as objects of social engineering research.

Measurement Model Evaluation (Outer Model)

The measurement model evaluation was conducted to ensure the validity and reliability of the research constructs.

Convergent Validity

Convergent validity criteria:

a. Loading factor > 0.70
b. AVE > 0.50

Variable Loading Range AVE Status
Digital Security Literacy 0.74–0.88 0.67 Valid
Cyber Awareness 0.76–0.91 0.71 Valid
Social Engineering Vulnerability 0.72–0.86 0.65 Valid
All indicators meet the threshold value, so the construct is declared valid.

Reliability Test

Variable Cronbach Alpha Composite Reliability
Digital Security Literacy 0.89 0.92
Cyber Awareness 0.91 0.93
SE Vulnerability 0.87 0.90

A reliability value >0.70 indicates excellent internal consistency of the research instrument.

Discriminant Validity

Tests using the Fornell-Larcker Criterion showed that each variable had a higher AVE value than the correlation between other constructs. This indicates that each variable is able to uniquely explain its construct.

Thus, the measurement model meets all validity and reliability criteria.

Structural Model Evaluation (Inner Model)

R-Square Value

Endogenous Variable R^2 Interpretation

Cyber Awareness 0.58 Moderate-Strong

Social Engineering Vulnerability 0.64 Strong

The R^2 value indicates that digital security literacy can explain 58% of the variation in cyber awareness and 64% of the variation in social engineering vulnerability.

Effect Size (f^2)

F^2 Relationship Category

Literacy → Vigilance 0.45 Large

Vigilance → Vulnerability 0.39 Large

This indicates a significant practical influence between the research variables.

Predictive Relevance (Q^2)

A Q^2 value of 0.41 (>0) indicates the model has good predictive ability for empirical phenomena.

Hypothesis Testing (Bootstrapping SEM-PLS)

Bootstrapping was performed with 5,000 subsamples.

Hypothesis Path β T-stat P-value Decision

H1 Literacy → Awareness 0.71 11.32 <0.001 Accepted

H2 Literacy → Vulnerability -0.42 6.87 <0.001 Accepted

H3 Vigilance → Vulnerability -0.53 9.15 <0.001 Accepted

H4 Mediation -0.31 5.92 <0.001 Significant

Discussion

The Effect of Digital Security Literacy on Cyber Awareness

The results of this study show that digital security literacy has a significant positive effect on cyber awareness. This finding indicates that increasing user understanding of digital threats can shape defensive behavior when faced with suspicious messages. This finding aligns with research by Parsons et al. (2017), which confirms that security awareness training improves phishing detection capabilities. Conceptually, digital literacy functions as a cognitive defense mechanism that helps users evaluate risks before making digital decisions.

The Effect of Digital Security Literacy on Social Engineering Vulnerability

The significant negative effect indicates that higher digital security literacy, the lower the likelihood of users becoming victims of social engineering. This supports the theory of Mitnick and Simon (2011) that the success of social engineering is highly dependent on low user awareness.This finding strengthens the argument that security investments should not be solely focused on technology but should be accompanied by user education.

The Role of Cyber Awareness in Reducing the Risk of Attacks

Cyber awareness has been shown to be a key protective factor against social engineering. Users who are accustomed to verifying information and are less likely to trust digital messages demonstrate significantly lower levels of vulnerability. These results support the Human-Centric Cybersecurity approach (Sasse & Flechais, 2005), which positions humans as human firewalls.

The Mediating Effect of Cyber Vigilance

The mediation analysis shows that digital security literacy not only has a direct effect but also an indirect effect through increased cyber vigilance. This means that digital literacy shapes behavioral awareness, which then systematically reduces the risk of social engineering attacks. This model shows that the most effective mitigation strategy is a combination of:

a. digital literacy education,
b. security behavior formation,
c. and adaptive authentication mechanisms.

Research Implications

Theoretical Implications

This research expands the study of social engineering by integrating digital security literacy into a structural model based on user behavior.

Practical Implications

The research results can be used by:

a. educational institutions,
b. business organizations,
c. government,
d. digital MSMEs,
e. to design a national digital security literacy program.

Conclusion

This research aims to develop a social engineering attack mitigation model based on digital security literacy among social media users in Indonesia. Based on an analysis using the Structural Equation Modeling–Partial Least Squares (SEM-PLS) approach on 210 respondents, this study yielded several key findings.

First, digital security literacy has been shown to have a positive and significant influence on user vigilance in facing social manipulation threats in the digital space. A high user understanding of cybersecurity practices such as information verification, digital identity management, and awareness of social engineering techniques can improve early detection of attacks. Second, user vigilance acts as an effective mediating variable in reducing vulnerability to social engineering attacks. The empirical model shows that increasing digital security literacy can reduce the risk of attacks by up to 64%, confirming that the human factor is a key layer of defense in modern cybersecurity.

Third, the resulting mitigation model emphasizes the integration of three main components:

a. Continuous digital security literacy education,
b. Building cyber behavioral awareness, and
c. Implementing adaptive user risk-based authentication.

Thus, this research successfully presents a human-centric cybersecurity mitigation framework relevant to the context of Indonesia's digital society.

Research Implications

Theoretical Implications

This research strengthens the perspective that cybersecurity relies not only on technology but also on human behavior as the weakest link in information security systems. The proposed conceptual model expands the study of digital literacy by integrating user psychological dimensions, risk awareness, and behavior-based security adaptation.

Furthermore, this research contributes to the development of social engineering mitigation models based on the social media context in developing countries, which is still relatively limited in previous research.

Practical Implications

The research results provide strategic recommendations for:

a. Educational institutions, to integrate digital security literacy into the curriculum.
b. Government and regulators, in designing a national digital literacy program based on cyber threat mitigation.
c. Organizations and MSMEs, to implement user behavior-based security training.
d. Social media platforms, to develop adaptive risk warning and authentication systems.

Implementing this model has the potential to significantly reduce the success rate of phishing, impersonation, and social engineering attacks.

Research Limitations

Despite producing strong empirical findings, this study has several limitations:

a. The cross-sectional approach is incapable of describing long-term changes in user security behavior.
b. The data is based on respondent perceptions, which potentially contains subjective bias.

c. The research sample is still dominated by general social media users, so it does not specifically represent certain sectors such as health, education, or government.
d. The security technology variables used are still conceptual and have not been tested through real-world attack simulations (penetration scenarios).

These limitations open up opportunities for more comprehensive follow-up research.

Future Work (Further Research Directions)

Further research is recommended to:

a. Develop a longitudinal model to analyze changes in user digital security behavior on an ongoing basis.
b. Integrating Artificial Intelligence and Behavioral Analytics approaches to automatically detect social manipulation patterns.
c. Conducting simulation-based experiments on real-life social engineering attacks to operationally test the effectiveness of the mitigation model.
d. Adapting the model to the local cultural context of Southeast Asia to produce a cybersecurity framework based on socio-cultural sensitivity.
e. Combining network technical data with user behavior data to form a Hybrid Human-Technology Cybersecurity Framework.

4. Conclusion

Overall, this research confirms that improving digital security literacy is a fundamental strategy in countering social engineering threats in the era of digital transformation. The proposed mitigation model not only contributes academically but also provides practical, applicable solutions for the development of a sustainable national digital security ecosystem.

References

Albladi, S. M., & Weir, G. R. S. (2020). User characteristics that influence judgment of social engineering attacks in social networks. Human-Centric Computing and Information Sciences, 10(1), 1–24. https://doi.org/10.1186/s13673-020-00231-7

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? arXiv. https://doi.org/10.48550/arXiv.1901.02672

ENISA. (2022). ENISA threat landscape report 2022. European Union Agency for Cybersecurity.

Hadnagy, C. (2018). Social engineering: The science of human hacking (2nd ed.). Wiley.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2019). A primer on partial least squares structural equation modeling (PLS-SEM) (2nd ed.). Sage Publications.

Heartfield, R., & Loukas, G. (2016). Detecting semantic social engineering attacks with the weak semantic analysis approach. Computers & Security, 58, 19–39. https://doi.org/10.1016/j.cose.2015.10.001

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973–993. https://doi.org/10.1016/j.jcss.2014.02.005

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Mitnick, K. D., & Simon, W. L. (2011). The art of deception: Controlling the human element of security. Wiley.

Ng, W. (2012). Can we teach digital natives digital literacy Computers & Education, 59(3), 1065–1078. https://doi.org/10.1016/j.compedu.2012.04.016

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. Computers & Security, 66, 40–51. https://doi.org/10.1016/j.cose.2017.01.004

Sasse, M. A., & Flechais, I. (2005). Usable security: Why do we need it? How do we get it? IEEE Security & Privacy, 3(3), 40–44. https://doi.org/10.1109/MSP.2005.73

Verizon. (2023). 2023 data breach investigations report. Verizon Enterprise.

Whitman, M. E., & Mattord, H. J. (2018). Principles of information security (6th ed.). Cengage Learning.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats. Journal of the American Society for Information Science and Technology, 59(4), 662–674. https://doi.org/10.1002/asi.20779