International Civic Engagement Studies (ICES)
p-ISSN : 00000 | e-ISSN : 0000
Vol. 1 No. 2 (2026) | p.21 - 26
DOI: .....

Human Shield: Addressing Social Engineering Threats by Strengthening a Security Culture and Ethics in Digital Business Communication

Keisha Najwa Khairana[1], Naqinni Azhara[2], Sasikirana Azalia Rahmadhani[3], Syalu Aulia Hakim[4]
[1,2,3,4]Universitas Bhayangkara Jakarta Raya, Bekasi, Indonesia

[*]Correspondence: E-mail: 2023104150l1@mhs.ubharajaya.ac.id

A B S T R A C T S

Social engineering is one of the most dangerous cyber threats in business communication because it utilizes psychological manipulation to gain illegal access. Attacks such as phishing, pretexting, baiting, and whaling are on the rise, especially in organizations that don't yet have a strong security culture. This study aims to analyze how social engineering threatens business communication and examine the effectiveness of information security and governance policies in reducing these risks. The method used is a qualitative descriptive analysis by combining academic literature and empirical data from national institutions such as BSSN. The results of the study show that security policies are only effective if they are supported by technical controls, user education, audit mechanisms, and consistent security leadership. These findings confirm that the human factor remains the most vulnerable point and requires ongoing mitigation strategies.

A R T I C L E I N F O

Article History:
Received:01 Januari 2026
Accepted: 04 Januari 2026
Published by: 16 Januari 2026

Keywords:
Social Engineering, Tactics
Psychological, Manipulation
Phishing, Spear-Phishing
Pretexting

1. INTRODUCTION

Digital transformation brings significant changes to the way organizations communicate and conduct business processes. However, this convenience also opens up space for cyber threats. One of the threats that continues to increase is social engineering, which is a psychological manipulation technique to deceive individuals into providing information or access that should not be shared. BSSN (2022) notes that incidents involving social engineering are increasing almost every year, mainly through phishing and misuse of business email credentials.

Business communication is the main target because this channel contains critical information such as customer data, transactions, business plans, and internal system access. Social engineering-based attacks often succeed not because of technological weaknesses, but because of human negligence. Therefore, information security policies play an important role as a structural fence in reducing risks. The journal takes an in-depth look at: 1. how social engineering disrupts business communication, 2. the forms of threats that are most relevant to the organization, 3. how security and governance policies can effectively mitigate these threats.

According to the information security study group, social engineering works by exploiting psychological principles such as authority, urgency, trust, and compliance (Cialdini, 2006; Mouton et al., 2016).

In Indonesia, Putra and Rochim (2021) found that low security awareness and permissive organizational culture make it easier for perpetrators to manipulate. Information security policy is defined as a set of formal rules that govern how information is

managed, protected, and used (Whitman & Mattord, 2018).

Information security governance involves the integration of policies, organizational structures, audit processes, and management commitments (Von Solms & Van Niekerk, 2013).

2. METHODS

This study uses a descriptive qualitative approach with a literature study method. All data was obtained through tracing and reading various relevant scientific sources, such as academic journals, information security textbooks, and official reports of national institutions.

The data collection process is carried out by identifying articles and publications that discuss social engineering, threats to business communication, and information security policies and governance. Each source is read thoroughly, then information related to the research topic is recorded and classified.

The data obtained from these various sources are then combined and analyzed thematically. The analysis was carried out by comparing findings between journals to see similarities in concepts, threat patterns, and the effectiveness of reported security policies.

The results of this merger are used to build a more comprehensive understanding of how social engineering poses a threat to business communications and how security policies can respond to those threats. This literature study method was chosen because the research topic is conceptual and relies heavily on the understanding of existing theories and academic findings. By combining a variety of reliable sources, this research produces a scientifically robust study that is relevant to the context of information security in modern organizations.

3. RESULTS AND DISCUSSION

Results

The discussion on this has been studied in depth from the field involved. Studies on engenerating and security and there are various research results that have been worked on. This can be seen in the following table.

Table 1. Studies and Findings

Yes	Name/Title/Year	Findings
1	Putra & Rochim (2021) "Analysis of Kerta nan Social Enginee ring in Public Sector Organizations"	Low Awareness security and Permissive organizational culture Squirt at Employees are easy to manip Review.
2	Bullee et al. (2017) "Spear Phishin g in Organis ations Explain ed"	Spear phishing Successful because it utilizes Work context and Psychology victims.
3	Mouton et al. (2016) Social Enginee ring Attack Exampl es, Templat es and Scenari os	Social engineering utilizes the principle of authority, urgency, and trust.
4	Abawaj y (2014) User Preference nce of Cyber Security Awareness Delivery Methods	Users use interactive security education to prevent phishing.
5	Whitm an & Mattor d (2018) Principl es of Information Securit y	Security policies must be clear, relevant, and supported by audit and management.
6	Von Solms & Van Nieker k (2013) From Informa tion Security to Cyber Security	Security governance is important to prevent human threats
7	Hidayat et al. (2022) The Level of Literacy of Digital Literacy of the Internet in Indonesia	The digital literacy of the Indonesian people is still low, increasing the risk of social engineering.
8	Conti et al. (2016) A Survey of Man-inthe-Mid dle Attacks	Seranga n MITM often starts from the social engine ring to steal the ielal credentials.
9	Nurse et al. (2014) Resource Analysis and Effective Communication of Cyber Security Risks	Breast milk organists often fail to communicate safety risks properly.

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

Discussion

1. Social Engineering as a Major Threat to Business Communication

a. Phishing and Spear Phishing

Phishing is the most common attack that targets business communications because it uses email as the primary medium. The perpetrator designs the message as if it comes from an official party, such as the finance division, HR, or vendor. Spear phishing is more dangerous because the messages are designed based on the victim's profile so that the success rate is high (Bullee et al., 2017). In Indonesian companies, spear phishing is often used to divert vendor payments through invoice manipulation (BSSN, 2022).

b. Whaling and Executive Fraud

Whaling targets executives with messages that mimic the company's internal communication style. Perpetrators take advantage of a hierarchical culture, where requests from superiors are often executed without verification. These attacks mostly occur on urgent fund transfer requests or sensitive data access.

c. Pretexting: Identity Engineering

Pretexting is done by creating fake scenarios, for example impersonating IT staff asking for an OTP code or password "for system updates". The case in Indonesia shows that pretexting is often successful because the perpetrator understands the context of the targeted organization (Wibowo & Santoso, 2022).

d. Impact on Business Communication

Social engineering attacks can: 1. change the content of communication (fraud), 2. stealing business email credentials, 3. spreading malware, 4. resulting in data leakage, and 5. Undermine trust between business units and with external partners.

2. The Effectiveness of Information Security Policies in Overcoming Social Engineering

a. Policy Quality and Relevance

Operational An ideal security policy contains not only technical prohibitions and procedures, but also behavioral guidelines. Effective policies are characterized by: 1. clear, 2. easy to understand, 3. relevant to business processes, 4. supporting daily decision-making, and 5. updated regularly (Whitman & Mattord, 2018). Policies that are only administrative in nature have proven to be unable to withstand social engineering attacks.

b. Mindfulness Training

Security as the Main Key User awareness is the most important factor in preventing social engineering. Effective training includes: 1. phishing simulations, 2. two-step verification practices, 3. real-life case-based learning, 4. incident reporting without sanctions. In Indonesia, BSSN and Kominfo emphasize the importance of improving digital literacy because most incidents start from user negligence, not system failure.

c. Security Governance and Management Roles

The Summit of security governance ensures policies run through a clear structure, regular audits, and evaluation mechanisms. If management does not show commitment, the policy simply becomes a non-functional document. Organizations that successfully suppress social engineering typically have: 1. dedicated security units, 2. secure communication SOPs, 3. clear incident escalation flows, 4. "check before click" culture.

d. Supporting Technical Control

Although the main focus of social engineering is on humans, technical controls are still important, such as: 1. email filtering, 2. domain verification, 3. multi-factor authentication, 4. endpoint protection, 5. communication encryption. Technical controls act as a second layer if the user fails to detect manipulation.

From the description above, it is necessary to have a breadth in acting to understand whether social engineering is a threat and to understand the effectiveness of information policies regarding social security engineering.

For this reason, it is necessary to introduce as in the following table.

Table 2. Social Mitigation Engeneering

Threat Type	Psychological Mechanisms	Effective Policy Solutions
BEC / CEO Fraud	Authority & Urgency	Two-Step Verification Protocol (Dual-Signature)

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

Phishing	Curiosity / Fear	Phishing Simulation Training & Email Filtering
Pretexting	Trust	Data Classification Policy & Minimum Access Rights

The evolution of digital business communication has shifted the paradigm of cyber threats from the exploitation of technical code to the exploitation of human psychology. Social engineering in modern organizations is not just an ordinary deception, but a systematic manipulation that utilizes cognitive principles such as authority and urgency. According to Cialdini (2007), humans tend to obey automatically to authority figures, which in the business context is often manifested through Business Email Compromise (BEC) attacks. When an employee receives urgent instructions from an account that resembles an executive leader, situational pressure often paralyzes their logical skepticism mechanism, resulting in a fatal security breach.

The effectiveness of information security policies (ISPs) in modern organizations depends heavily on their ability to adapt to increasingly sophisticated pretexting tactics. Policies that are only static and administrative tend to fail because they do not consider the dynamic behavior aspects of employees. As stated by Bulgurcu et al. (2010), compliance with information security policies is influenced by employees' perception of security benefits compared to the efforts that must be expended. Therefore, policies should be designed to be user-centric, where security procedures such as two-step verification (2FA) are seamlessly integrated into the workflow without being considered an excessive productivity barrier.

In addition to technical policies, strengthening organizational culture through Security Awareness Training (SAT) is the main pillar in mitigating communication risks. The biggest challenge today is the emergence of Deepfake technology and AI that are able to mimic visual and auditory identities with high precision. Organizations can no longer rely on implicit trust in a single medium of communication. Modern policies should adopt the principle of Zero Trust, where any request for sensitive data or financial transactions must be validated through a secondary communication channel (out-of-band verification). It aims to create a layer of cognitive defense that allows employees to detect anomalies in day-to-day business communications.

Conclusively, the synergy between strict security policies and a deep understanding of communication psychology is the key to organizational resilience. The effectiveness of information security cannot be measured only by the sophistication of the software used, but by how resilient individuals within the organization are in the face of information manipulation. By building an environment that encourages transparency and no-blame reporting, companies can transform employees from easy targets to proactive first lines of defense. The integration of security values into these business ethics will ultimately maintain the integrity of the organization's information assets and long-term reputation in the global marketplace.

.

4. CONCLUSION

Social engineering is the most critical threat in modern business communication because it takes advantage of human weakness, not technology. Attacks such as phishing, spear phishing, whaling, and pretexting have been proven to be able to damage the integrity of communications and cause financial losses and organizational reputation. Information security policies can be an effective mitigation tool if they are clearly designed, relevant, and supported by strong governance. Security awareness training is the most important element in preventing attacks because humans are the main vulnerable points. The combination of education, management commitment, auditing, and technical control has been proven to increase organizational resilience to social engineering.

5. References

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. Behaviour & Information Technology, 33(3), 237–248.

Alshehri, M., Alabdulmohsin, I., & Algalil, S. (2023). Detecting phishing emails using deep learning techniques. Journal of Cybersecurity and Digital Forensics, 5(2), 77–92.

National Cyber and Cryptography Agency. (2022). Annual Report on Indonesian Cybersecurity. BSSN RI.

Bullee, J. H., Montoya, L., Pieters, W., Junger, M., & Hartel, P. (2017). Spear phishing in organisations explained. Information & Computer Security, 25(5), 593–613.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.2307/25750690

Cialdini, R. B. (2007). *Influence: The psychology of persuasion* (Revised ed.). Harper Business. (Original work published 1984). https://doi.org/10.4324/9781315664361

Cherdantseva, Y., & Hilton, J. (2013). Information security and information assurance: The discussion about the meaning, scope, and goals. International Journal of Computer Science and Engineering, 7(1), 36–43.

Cialdini, R. B. (2006). Influence: The psychology of persuasion (Rev. ed.). Harper Collins.

Conti, M., Dragoni, N., & Lesyk, V. (2016). A survey of man-in-the-middle attacks. IEEE Communications Surveys & Tutorials, 18(3), 2027–2051.

Firmansyah, A., & Suryanto, W. (2022). Analysis of the security risks of public WiFi networks in urban areas. Journal of Information Technology and Security, 10(1), 45–54.

Fruhlinger, J. (2020). Whaling attack definition and examples. CSO Online.

Harris, A. J., Patten, K., & Regan, E. (2012). The need for BYOD mobile device security awareness. Information Security Journal, 21(3), 123–131.

Hidayat, R., Fadhilah, N., & Yuliana, D. (2022). The level of digital security literacy of internet users in Indonesia. Indonesian Journal of Digital Communication Sciences, 4(2), 101–114.

IBM Security. (2023). Cost of a Data Breach Report 2023. IBM Corporation.

Mitnick, K. D., & Simon, W. L. (2002). The art of deception: Controlling the human element of security.

Wiley. Mouton, F., Leenen, L., & Venter, H. (2016). Social engineering attack examples, templates and scenarios. Computers & Security, 59, 186–209.

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2014). Trustworthy and effective communication of cyber security risks. ACM Computing Surveys, 47(4), 1–44.

Parsons, K., McCormac, A., Pattinson, M., Butavicius, M., & Jerram, C. (2014). The human aspects of information security questionnaire (HAIS-Q): Measuring security awareness. Computers & Security, 42, 165–176.

Putra, B. S., & Rochim, A. F. (2021). Analysis of social engineering vulnerabilities in public sector organizations. Nusantara Cyber Security Journal, 3(2), 89–102.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

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

Wibowo, E., & Santoso, I. (2022). Evaluate the risk of insider threats in the company's information system. Indonesian Journal of Information Systems, 8(1), 55–63.

Hadnagy, C. (2018). *Social engineering: The science of human hacking* (2nd ed.). John Wiley & Sons. https://doi.org/10.1002/9781119433729

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the human*

DOI: http://dx.doi.org/10.xxxxx/ijost.vXiX
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx

element of security. John Wiley & Sons. ISBN: 978-0471237129

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning. ISBN: 978-0357506431

DOI: xxxxxxxxxxxxxxxxxx
p- ISSN xxxx-xxxx e- ISSN xxxx-xxxx