Social Engineering as a Major Cybersecurity Threat: Analysis of Challenges and Solutions for Organizations

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Abstract: Social engineering is a psychological manipulation technique used by attackers to exploit human weaknesses in information security. This research aims to identify the challenges organizations face in protecting themselves from social engineering attacks and offer effective solutions. Through analysis of case studies and relevant literature, it was found that a lack of employee awareness and training is one of the main causes of the success of these attacks. In addition, many organizations still rely on inadequate technology to detect threats. To address these issues, this paper recommends implementing regular training programs, strengthening security policies, and using advanced technology. With this comprehensive approach, organizations can strengthen their defences and reduce the risks associated with social engineering. Organizations should prioritize continuous education programs, foster a culture cantered on security, and establish protocols that encourage alertness. Moreover, robust access controls, defined incident reporting processes, and the use of technology like behavioural analytics can further reduce the risks posed by social engineering.

Keywords: Social engineering, information security, challenges and solutions, awareness

Introduction

Information security has become an increasingly important issue in today's digital age. With the increasing use of technology and the internet, valuable data and information of individuals and organizations have become highly vulnerable to various cyber threats. Among these threats, social engineering has emerged as one of the most effective methods used by attackers to exploit human weaknesses.(Baltuttis & Teubner, 2024) Social engineering refers to psychological manipulation techniques that aim to influence individuals to perform certain

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia
E-mail: budiwibowo1993@gmail.com

Received August 30, 2024; Revised September 30, 2024; Accepted October 31, 2024; Published November 1, 2024

actions, such as providing sensitive information or accessing systems without authorization. (Momoh et al., 2023) According to a report from the Cybersecurity and Infrastructure Security Agency (CISA) (2020), more than 90% of data breaches are caused by social engineering techniques, showing how significant this threat is to information security. The FBI's Internet Crime Complaint Centre reported a 2023 complaint volume from the US public of 880,418, which is a 10% increase from 2022. The total loss from these complaints amounted to $12.5 billion.

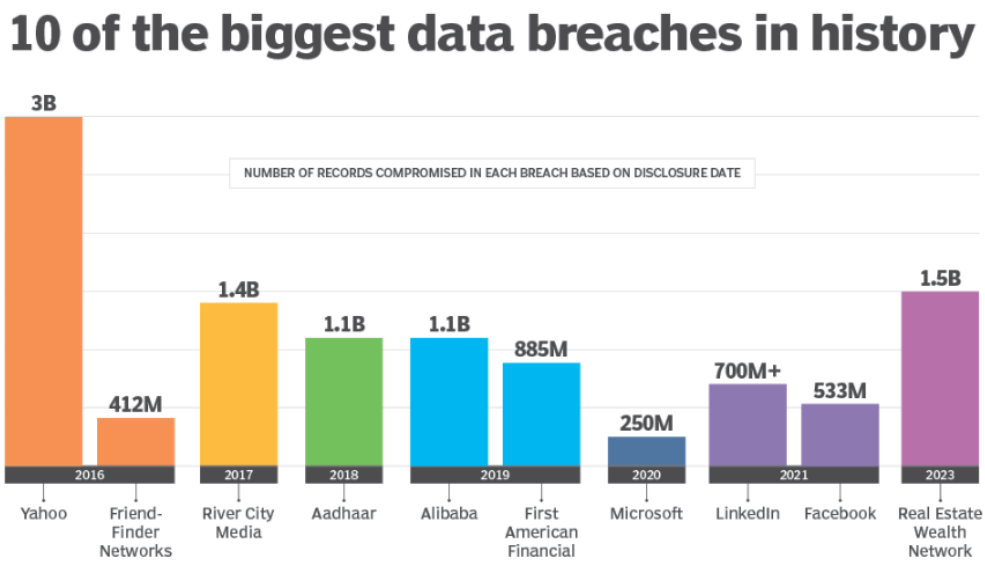

Figure 1 Number of records compromised in each breach based on disclosure date

The background of this problem is increasingly complex with the development of information and communication technology. Many organizations, especially those with limited resources, are unable to implement adequate security policies to protect themselves from social engineering attacks. (Perwej et al., 2021) In information security, small companies tend to be more vulnerable to social engineering attacks than large companies because large companies generally have larger budgets and resources to invest in information security, in terms of technology, training, and security policies. 50 percent of large companies (with more than 10,000 employees) spent $1 million or more annually on security last year, with 43 percent spending $250,000 to $999,999, and only 7 percent spending under $250,000, according to Cisco. On the other hand, smaller companies often have limited budgets, making it difficult to implement optimal cybersecurity. Data from Cybersecurity Ventures shows that small companies typically spend less on security, making them more vulnerable to various threats, including social engineering at https://cybersecurityventures.com/cybersecurity-almanac-2022.

Attackers often use convincing methods, such as official-looking phishing emails or phone calls from authoritative-looking "representatives" to trick victims. This makes individuals, especially less experienced employees, easy targets for attackers. The unfamiliarity and lack of awareness about these techniques leads many people to fall into well-planned traps.

The importance of research on social engineering cannot be overlooked, given its far-reaching impact on organizations and individuals. (Al-Hashem & Saidi, 2023) In addition to significant financial losses, social engineering attacks can also damage reputation and customer trust. (Salahdine & Kaabouch, 2019) In this context, employee education and training are crucial. Previous research shows that effective training programs can reduce the risk of social engineering attacks. However, despite increased awareness, many organizations still lack a comprehensive prevention strategy.

The literature review shows that a few studies have identified social engineering techniques and their impact on information security.(Momoh et al., 2023) describes various methods used by attackers, while (Aldawood & Skinner, 2018) underline the importance of employee awareness in reducing vulnerabilities. While these studies provide valuable insights, there is a gap when it comes to implementing practical solutions that organizations can implement. Many studies remain theoretical and lack concrete guidance on steps that can be taken to protect against social engineering attacks. This gap analysis shows the need for a more applied approach to social engineering research. Organizations need to not only understand the techniques used by attackers, but also how to implement effective policies and training to raise awareness among employees. In addition, the use of advanced technologies, such as phishing detection software and two-factor authentication, should be integrated in security strategies to minimize risks.(Yuswanto et al., 2024)

Considering the background, the problem, the importance of the research, as well as the existing gaps, the purpose of this research is to identify the challenges organizations face in protecting themselves from social engineering attacks. This research also aims to offer practical solutions that can improve organizational awareness and defences. With a comprehensive approach, it is hoped that this paper can make a significant contribution in the effort to strengthen information security and protect organizational data and assets from social engineering threats.

Literature Review

Social engineering is known as an attack method that relies on psychological manipulation to influence an individual's decision to perform a certain action or divulge sensitive information. (Stewart & Dawson, 2018) According to some literature, social engineering is divided into

several types, including phishing, baiting, pretexting, and tailgating.(Siddiqi et al., 2022) Phishing is one of the most used methods and often takes the form of legitimate-looking messages or emails designed to obtain important information such as passwords or account numbers. Pretexting, on the other hand, involves creating fictitious scenarios to build trust with victims.(Syafitri et al., 2022) This study shows that social engineering attacks take advantage of human nature's lack of vigilance, especially under urgent or stressful conditions. The theory supporting the effectiveness of social engineering in information security also highlights that humans are the "weakest link" in the security chain.(Wibowo, n.d.) According to previous studies, social engineering techniques are effective because humans have a natural tendency to believe in authority or information that appears credible. (Wibowo & Hidayat, 2024) Some high-profile cases, such as fake email attacks that successfully breached large corporate networks, serve as evidence that social engineering requires a specialized mitigation approach that differs from technically based threats. By understanding this literature, this research is expected to provide new insights into the need for a comprehensive approach in dealing with human-based attacks.

Research Method

This research was conducted using qualitative and quantitative approaches to analyse the impact of social engineering in information security. Materials used included questionnaires and survey forms for data collection, as well as related literature on social engineering and information security. Respondents consisted of 100 employees from various organizations, randomly selected from sectors such as information technology, finance, and education. Data was collected through a survey containing questions about the respondents' experience with social engineering, their awareness of common techniques used, and the training they had received. In addition, in-depth interviews were conducted with 10 respondents to delve deeper into their experiences. The questionnaire was designed to cover aspects of social engineering, and was distributed via email, with an explanation of the research objectives.

Result and Discussion

Implementation of IT Security Awareness in the organization

The findings in this article may highlight that effective security training can improve employees' ability to recognize social engineering threats. Based on a study by Parsons et al. (2014), training that focuses on increasing security awareness is directly correlated with increased employee protective behaviour against cyber threats. The Protection Motivation Theory framework emphasizes the importance of factors such as perceived effectiveness of

protective measures and self-efficacy in improving employee security behaviour through training. Identify Challenges in Overcoming Social Engineering

Based on the research results, some key challenges in dealing with social engineering threats have been identified, especially in the aspect of employee awareness and response to increasingly sophisticated manipulative techniques. The findings show that many employees lack an understanding of the dangers of social engineering attacks. For example, while most organizations have provided security training, few have included simulations of social engineering attacks, such as phishing, in their training programs. This suggests a gap in employees' understanding and awareness of these threats, which in turn provides an opening for human-based attacks. In addition, evolving social engineering techniques, such as the use of deepfakes to fake voices or images in vishing (phishing through voice calls), have added to the complexity of the threat. Some organizations are having difficulty identifying and mitigating such attacks, as the technologies supporting these attacks are increasingly difficult to detect with traditional security tools. The research also found that internal trust among employees is often a loophole that attackers exploit. In some cases, employees easily provide sensitive information to individuals posing as team members or organizational leaders, especially if the attacker demonstrates a level of urgency or authority. On the solution side, implementing multi-factor authentication (MFA) has proven to be an effective measure that can reduce the risk of unauthorized access to sensitive information. In addition, organizations that regularly conduct social engineering attack simulations tend to have a higher level of vigilance among their employees. These simulations allow employees to experience an attack situation in a safe scenario, improving their preparedness when facing a real attack. Organizations are also starting to implement stricter access control policies, where only certain employees have direct access to critical information. This reduces the chances of sensitive information falling into the wrong hands, while making it easier to monitor internal activities.

The results of this study include analysis of data obtained from questionnaires and interviews, as well as observations of patterns that emerged from respondents' experiences with social engineering. Table 1 presents a demographic summary of the respondents, showing the distribution by age, gender and industry sector.

Table 1 Respondent Demographics

Category	Number of Respondents	Percentage (%)
Age		
18-25	30	30
26-35	40	40
36-45	20	20
>45	10	10

Gender		
Male	50	50
Female	50	50
Sector Industry		
IT	45	45
Financial	25	25
Education	30	30

Of the 100 respondents, 65% reported having experienced at least one form of social engineering attack, such as phishing or phone scams. Table 2 presents data on the types of attacks experienced by respondents.

Table 2 Types of Social Engineering Attacks Experienced

Type of Attack	Number of Respondents	Percentage (%)
Phishing	40	40
Vishing (Voice Phishing)	25	25
Pretexting	15	15
Baiting	10	10
No Idea	10	10

The results show that social engineering attacks have a significant impact on organizations. The percentage of respondents who reported experience with these attacks (65%) indicates that this threat is highly relevant and needs to be addressed. This is in line with previous findings that many individuals do not have sufficient understanding of social engineering techniques.

One notable finding from the data analysis is that phishing attacks dominate the types of attacks experienced, with 40% of respondents reporting exposure. This suggests that attackers prefer methods that are easily accessible and can reach many people at once. Additionally, the interview results indicated that many respondents did not receive sufficient security training, which contributed to the high success rate of the attacks. This highlights the need for organizations to improve security training and awareness programs for their employees. Table 2 shows the variety of attack types experienced by respondents. While phishing is the most common, other forms such as vishing and pretexting also show significant prevalence. This indicates that attackers use a variety of methods to exploit human weaknesses, making it important for organizations not to focus on just one type of attack.

Discussion of these results leads us to the question of why and how these social engineering attacks occur. Many factors influence individual vulnerability, including lack of knowledge,

time pressure, and the social nature of humans to trust information that appears legitimate. Unawareness of the techniques used by attackers creates loopholes that can be exploited.

From these findings, it can be concluded that awareness and training are key in mitigating social engineering risks. Organizations that implement structured and continuous training programs and use advanced technologies such as two-factor authentication, can strengthen their defences. In addition, a multi-layered approach to information security, including clear policies and regular audits, can also help mitigate risks.

Overall, the results of this study not only provide an overview of the prevalence of social engineering in various sectors, but also emphasize the importance of proactive measures in improving information security. The findings can be applied to other organizations facing similar challenges, providing guidance to develop more effective strategies to protect themselves from social engineering threats.

Conclusions

Social engineering presents a significant challenge for information security within organizations, as it focuses on exploiting human psychology rather than technical vulnerabilities. By taking advantage of employees' trust and access rights, social engineering can circumvent even the most advanced security measures, underscoring the importance of comprehensive security training. To combat these risks effectively, a layered approach is essential. Organizations should prioritize continuous education programs, foster a culture cantered on security, and establish protocols that encourage alertness. Moreover, robust access controls, defined incident reporting processes, and the use of technology like behavioural analytics can further reduce the risks posed by social engineering. A balanced strategy combining human awareness and technological safeguards can help organizations build greater resilience against social engineering, ensuring a safer information environment in the long run.

References

Al-Hashem, N., & Saidi, A. (2023). The Psychological Aspect of Cybersecurity: Understanding Cyber Threat Perception and Decision-Making. *International Journal of Applied Machine Learning and Computational Intelligence*, *13*(8), 11–22. https://neuralslate.com/index.php/Machine-Learning-Computational-I/article/view/41

Aldawood, H., & Skinner, G. (2018). Educating and Raising Awareness on Cyber Security

Social Engineering: A Literature Review. *Proceedings of 2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering, TALE 2018*, *December 2018*, 62–68. https://doi.org/10.1109/TALE.2018.8615162

Baltuttis, D., & Teubner, T. (2024). Effects of visual risk indicators on phishing detection behavior: An eye-tracking experiment. *Computers and Security*, *144*(April), 103940. https://doi.org/10.1016/j.cose.2024.103940

Ladayya, U., Prayitno, D., Syani, M., Hikmawan, R., & Abdulmajid, N. W. (2024). Kesadaran Keamanan Informasi atas Phising , Smishing , dan Vishing pada Warga Kota Cimahi. 18, 109–119.

Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). *Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution*. *December*. https://doi.org/10.13140/RG.2.2.35640.52489

Perwej, D. Y., Qamar Abbas, S., Pratap Dixit, J., Akhtar, D. N., & Kumar Jaiswal, A. (2021). A Systematic Literature Review on the Cyber Security. *International Journal of Scientific Research and Management*, *9*(12), 669–710. https://doi.org/10.18535/ijsrm/v9i12.ec04

Salahdine, F., & Kaabouch, N. (2019). Social engineering attacks: A survey. *Future Internet*, *11*(4). https://doi.org/10.3390/FI11040089

Siddiqi, M. A., Pak, W., & Siddiqi, M. A. (2022). A Study on the Psychology of Social Engineering-Based Cyberattacks and Existing Countermeasures. *Applied Sciences (Switzerland)*, *12*(12). https://doi.org/10.3390/app12126042

Stewart, J., & Dawson, M. (2018). How the modification of personality traits leave one vulnerable to manipulation in social engineering. *International Journal of Information Privacy, Security and Integrity*, *3*(3), 187. https://doi.org/10.1504/ijipsi.2018.10013213

Syafitri, W., Shukur, Z., Mokhtar, U. A., Sulaiman, R., & Ibrahim, M. A. (2022). Social Engineering Attacks Prevention: A Systematic Literature Review. *IEEE Access*, *10*, 39325–39343. https://doi.org/10.1109/ACCESS.2022.3162594

Thompson, N., McGill, T., & Narula, N. (2024). “No point worrying” – The role of threat devaluation in information security behavior. Computers and Security, 143(May), 103897. https://doi.org/10.1016/j.cose.2024.103897

Van Geest, R. J., Cascavilla, G., Hulstijn, J., & Zannone, N. (2024). The applicability of a hybrid framework for automated phishing detection. Computers and Security, 139(February 2023), 103736. https://doi.org/10.1016/j.cose.2024.103736

B. Wibowo and M. Alaydrus, "Smart Home Security Analysis Using Arduino Based Virtual Private Network," 2019 Fourth International Conference on Informatics and

Computing (ICIC), Semarang, Indonesia, 2019, pp. 1-4, doi: 10.1109/ICIC47613.2019.8985669.

Wibowo, B., & Hidayat, T. (2024). Strategi Efektif dalam Meningkatkan Kesadaran Keamanan Siber terhadap Ancaman Phishing di Lingkungan Perusahaan PT. XYZ. *Jurnal Pengabdian Masyarakat Sultan Indonesia*, *2*(1), 1–9. https://doi.org/10.58291/abdisultan.v2i1.294

Yuswanto, A., Wibowo, B., & Hafiz, L. (2024). A Review Method for Analysis of the Causes of Data Breach in the Pasca Pandemic. *Jurnal Komputer Dan Elektro Sains*, *3*(1), 1–5. https://doi.org/10.58291/komets.v3i1.205