Guidelines to Prevent Social Engineering Attacks for Law Enforcement Agency

Shankar Muniandy, Ganthan Narayana Samy, Nurazean Maarop, Mahiswaran Selvanathan & David Lau Keat Jin
Faculty of Artificial Intelligence
Universiti Teknologi Malaysia
ganthan.kl@utm.my

Sundresan Perumal
Faculty of Science and Technology
Universiti Sains Islam Malaysia
sundresan.p@usim.edu.my

Abstract

Social engineering attacks remain a significant cybersecurity threat to organizations worldwide. As attackers increasingly exploit human vulnerabilities, organizations need effective strategies to mitigate the risks posed by social engineering. Therefore, the objective of this paper is to present a comprehensive study by developing a propose guidelines to address social engineering attacks within organizations. The research employs a mixed-methods approach, combining qualitative and quantitative data collection methods. Data was gathered through surveys and literature reviews to understand the various dimensions of social engineering and existing countermeasures. The findings lead to the identification of proposed guidelines for organizations to strengthen their defense against social engineering attacks. The proposed guidelines cover essential aspects, such as employee training, password policies, encryption, incident response planning, and ongoing system monitoring. By implementing these guidelines, organizations can enhance their security posture and reduce the risk of unauthorized access through social engineering attacks. Future research could explore the effectiveness of these guidelines in various organizational settings and examine the role of emerging technologies in detecting and mitigating social engineering attacks. Overall, this research contributes to the understanding of social engineering attacks and provides a valuable guidelines for organizations to combat this evolving threat effectively.

Keywords: *Social Engineering Attacks, Law Enforcement Agency, Guidelines*

1. Introduction

The rapid growth of the digital landscape and increased connectivity in Malaysia have led to an alarming rise in cyber threats and incidents up until December 2022, as evidenced by the 7,292 reported incidents received by Cyber Security Malaysia through (MyCERT, 2023). Among these incidents, the most significant concern arises from the staggering number of fraud-related cases, totaling 4,741 in 2022 alone. Online fraud, encompassing various subcategories such as spoofing, impersonation, illegal investments, unauthorized transactions, cyber-blackmail scams, business email compromise, parcel scams, and fraudulent purchases, poses a substantial risk to both individuals and entities within and beyond Malaysia. The multifaceted nature of these cyber-attacks, often involving social engineering techniques and the introduction of malware, highlights the potential for devastating consequences once attackers gain access to computer systems. This escalating threat environment necessitates urgent attention and comprehensive strategies to enhance cybersecurity measures and safeguard the digital ecosystem of Malaysia. As such, addressing the root causes and implementing proactive solutions to mitigate cyber threats is critical to protect the interests and security of home users, businesses, industries, and international partners who are affected by the malicious activities originating from both inside and outside the country.

Therefore, before developing preventive measures for information systems, it is critical to identify and characterize potential threats (Klein et al., 2022). As businesses become more cautious about defending their networks by investing in stronger security solutions, fraudsters' focus has turned to targeting and abusing end users, who are the weakest link in the security chain. When it comes to information security, people are nearly always regarded the program's weakest link (Ani et al., 2019), as human error is frequently a primary contributor to vulnerabilities that develop as a result of technology implementations. Social interactions, especially pleasant gestures, can be utilized to obtain critical and sensitive information from a victim. The article is organized into five sections. The next section describes previous studies related to this research. This is followed by an explanation of the research method and then the results and discussion and conclusion complete the article.

2. Literature Review

This section will discuss about definition of key concept and explanation about different type’s social engineering attacks. Social engineering is known as a process of identifying and exploiting psychological and behavioral vulnerabilities in people in order to get unauthorized access to protected information is known as social engineering (Wang et al., 2021). The principal application of the phrase "social engineering" relates to the activity of manipulating other people in order to get personal and sensitive information while posing as a trustworthy source (Kaushalya et al., 2018). The victim, who could be an individual or an organization, is tricked into disclosing personal information by social interaction, persuasion, or requests involving a third party affiliated with information technology. Attacks based on social engineering may be conducted everywhere there is human contact, and they can take a wide variety of different forms. Table 1 depicted top seven attack types that often include in social engineering attacks.

Table 1: Top seven attack types that often include in social engineering attacks

No.	Attack	Description
1.	Phishing (Alkhalil et al., 2021)	Hackers use fake phishing emails, websites, and text messages to get sensitive personal or business information from people who don't know they are being socially engineered. Most of the time, this is how social engineering is done. Even though phishing emails are very common, many people still falls for them and clicks on the harmful links.
2.	Spear Phishing (Allodi et al., 2020)	Using phishing emails to attack specific people or businesses is a common thing to do. A spear phishing email is much more complicated than a typical mass phishing email because it requires a lot of research on the potential victims and the companies they work for.
3.	Baiting (Chetioui et al., 2022)	This kind of attack can happen either online or in real life. Most of the time, an online criminal will offer a reward to the victim in exchange for private information or information about where the stolen item is.
4.	Malware (Selvaganapathy et al., 2021)	Attacks that use fake warning messages to deceive users into downloading malware on their devices. Some scammers try to trick their victims into paying in order to remove malware from their computers by claiming the infection is already installed. Attackers choose this strategy since it is simple.
5.	Pretexting (Chetioui et al., 2022)	In this kind of attack, the attacker would pretend to be someone else so that the victim would tell them something private. Pretexting is often used as a weapon against banks, credit card companies, and utility companies that store a lot of information about their customers.

6.	Tailgating (Chetioui et al., 2022)	Tailgating is a type of assault in which the target is someone who could give a criminal physical access to a safe building or place. Most of the time, these cons work because the victim is too nice. For example, they hold the door open for a stranger who is pretending to be an employee.
7.	Vishing (Obuhuma & Zivuku, 2020)	In this made-up scenario, cyber thieves would leave urgent voicemails for their victims, trying to convince them that they need to do something right away to avoid being arrested or hurt in some other way. Criminals often pretend to be banks, government organizations, or law enforcement agencies when they set up phishing schemes.

3. Research Methodology

In this study, first phase is adopting quantitative and second phase is utilizing qualitative methods. The quantitative technique is first utilized to examine the information security awareness of users, and then the qualitative method is employed to provide acceptable suggestions for raising the degree of information security awareness. Therefore, using a mixed method in this research enables the strength of quantitative findings to be correlated with the interpretation offered by qualitative data. Consequently, new major findings will be gained from the investigation as mentioned in (Timans et al., 2019).

3.1 Respondent

Basically, all the respondents are from selected department from Royal Malaysia Police (RMP) from Bukit Aman for both the quantitative and qualitative approaches for this study. Respondents in the age range of 25 to 60 are selected as a target group. In addition, 83.3% of selected respondents has more than 10 years of vast experience and knowledge in information security field.

3.2 First Phase: Quantitative Method

The guidelines to prevent social engineering attacks will be proposed for this research. Respondents will be sent questionnaires, both online and offline, to fill out in order to evaluate their present degree of social engineering awareness and the factors that influence it. The data sources will consist of survey data and quantitative analysis data, and their purpose will be to gain an understanding of how well the respondents are informed about information assurance.

Basically, the estimated of sample size for the qualitative study based on the population size. This was done to ensure that the results were accurate as stated in (Krejcie R.V. & Morgan D.W. 1970, Rajendran & Mohd Shah, 2020). Therefore, the total number of respondents that participated in this study are 96 it is considered as optimal sample size for an adequate analysis, providing higher accuracy and validity for this research.

3.2 First Phase: Quantitative Method

One more collection of data was gathered by conducted structured interviews with three selected expert panels from Royal Malaysia Police (RMP) as a expert review for the proposed guidelines which was obtained from quantitative analysis. Structured interviews is conducted throughout this study to generate information assurance awareness guidelines that are appropriate and comprehensive in order to achieve our research objective.

Basically, three experts in the field of information security have reviewed the guidelines and provided feedback on their effectiveness and practicality. The feedback has been incorporated into the guidelines, resulting in a refined set of recommendations.

4. Proposed Guidelines to Prevent Social Engineering Attacks

Basically, the proposed guidelines are categorized into three main groups namely, for Information Technology (IT) administrators, users, and vendors in order to enhance the prevention of social engineering attacks within law enforcement organization. These guidelines are supported by internationally recognized standards, policies, and rules in the field of information security.

For IT administrators, the guidelines as exhibited in Table 2 namely, establishing comprehensive security awareness training programs is crucial. By conducting regular phishing simulation exercises, IT administrators can educate employees on recognizing social engineering tactics. This helps create a vigilant workforce capable of identifying and reporting suspicious activities. Furthermore, implementing Multi-Factor Authentication (MFA) across all systems and services adds an extra layer of protection by requiring multiple authentication factors. IT administrators should also ensure that software and systems are regularly updated and patched to address known vulnerabilities. This can be achieved by establishing a patch management process. Enforcing strict password policies, including complexity and expiration requirements, helps mitigate the risk of unauthorized access. Additionally, encrypting sensitive data in transit and at rest provides an additional safeguard against unauthorized disclosure.

To ensure the effectiveness of these measures, regular security audits and assessments are essential. By conducting periodic penetration testing and vulnerability assessments, IT administrators can identify vulnerabilities and areas for improvement. Establishing an incident response plan, including an incident response team and defined procedures, ensures a timely and effective response to social engineering incidents. Monitoring and logging system activities through a security information and event management (SIEM) system helps detect and respond to social engineering attempts. Lastly, providing ongoing security training for IT administrators is crucial to keep them updated on the latest social engineering techniques.

Table 2: Guidelines for IT Administrator

Category	**Guideline Description**	**Example Event/ Activity**	**Step-by-Step Policies**	**International Standard/Policy/Rules**
IT Administrator	1. Establish comprehensive security awareness training programs for employees to recognize social engineering tactics.	Conduct regular phishing simulation exercises	Develop and implement a training curriculum	ISO/IEC 27001:2013
	2. Implement multi-factor authentication (MFA) for all systems and services.	Enforce MFA for accessing company email accounts	Configure MFA settings for all relevant systems	NIST SP 800-63B
	3. Regularly update and patch all software and systems to address known vulnerabilities.	Apply security updates promptly and regularly	Establish a patch management process	ISO/IEC 27001:2013
	4. Implement strict password policies requiring strong,	Enforce password complexity	Define password policy guidelines	NIST SP 800-63B

	unique passwords.	and expiration requirements		
	5. Enforce the use of encryption for sensitive data in transit and at rest.	Encrypt data stored on company servers and databases	Implement encryption protocols and technologies	ISO/IEC 27001:2013
	6. Regularly conduct security audits and assessments to identify vulnerabilities and areas of improvement.	Perform periodic penetration testing and vulnerability assessments	Develop an audit and assessment schedule	ISO/IEC 27001:2013
	7. Establish an incident response plan to handle social engineering incidents effectively.	Create an incident response team and define roles	Document incident response procedures and escalation process	NIST SP 800-61r2
	8. Monitor and log system activities to detect and respond to social engineering attempts.	Implement a security information and event management (SIEM) system	Define logging and monitoring procedures and review logs	ISO/IEC 27001:2013
	9. Provide ongoing security training for IT admins to stay updated on the latest social engineering techniques.	Attend security conferences and webinars	Allocate time and resources for continuous professional development	Various security certifications and industry conferences
	10. Foster a culture of security and encourage reporting of any suspicious incidents or activities.	Promote a reporting mechanism for potential social engineering attacks	Communicate the importance of reporting and establish incident reporting channels	ISO/IEC 27001:2013, NIST SP 800-61r2

For user's guidelines as shown in Table 3, attending regular security awareness training sessions is vital. By actively participating in company-wide security awareness programs, users become knowledgeable about social engineering attempts and are better equipped to recognize and report them. Users should exercise caution when opening email attachments or clicking on links, especially from unknown senders. Verifying the legitimacy of email senders and attachments can help prevent falling victim to phishing attempts. Being cautious about unsolicited phone calls or requests for sensitive information is equally important. Users should never share sensitive information over the phone and should be trained to recognize social engineering tactics. Regularly updating and patching personal devices and applications is another essential guideline for users.

This ensures that known vulnerabilities are addressed promptly. Creating strong, unique passwords and enabling two-factor authentication (2FA) when available adding an extra layer of security to user accounts. Users should also be cautious when sharing personal information on social media platforms, as it can be exploited for social engineering attacks. Regularly reviewing and monitoring financial accounts helps identify any unauthorized transactions or suspicious activities.

Table 3: Guidelines for users

Category	Guideline Description	Example Event/Activity	Step-by-Step Policies	International Standard/Policy/Rules
Users	1. Attend regular security awareness training sessions to recognize and report social engineering attempts.	Participate in company-wide security awareness programs	Establish a training schedule and communication channels	ISO/IEC 27001:2013, NIST SP 800-50
	2. Exercise caution when opening email attachments or clicking on links, especially from unknown senders.	Verify the legitimacy of email senders and attachments		ISO/IEC 27001:2013, NIST SP 800-45
	3. Be wary of unsolicited phone calls or requests for sensitive information.	Never share sensitive information over the phone	Train users on recognizing social engineering tactics and establishing procedures for handling such calls	ISO/IEC 27001:2013, NIST SP 800-50
	4. Regularly update and patch personal devices and applications to address known vulnerabilities.	Install software updates and patches regularly	Provide guidelines on updating personal devices and applications, including automatic updates	NIST SP 800-53, ISO/IEC 27001:2013
	5. Use strong, unique passwords for all accounts and enable two-factor authentication (2FA) when available.	Create complex passwords and enable 2FA where possible	Educate users on password security best practices and the importance of enabling 2FA	NIST SP 800-63B
	6. Be cautious when sharing personal information on social media platforms, as it can be used for social engineering attacks.	Limit the sharing of personal information on social media platforms	Educate users on privacy settings and the potential risks associated with sharing personal information online	ISO/IEC 27001:2013, NIST SP 800-53
	7. Report any suspicious	Notify the IT department about	Establish clear reporting channels	ISO/IEC 27001:2013, NIST

	incidents or requests to the IT department or designated incident response team.	suspicious activities or requests	and provide instructions on how to report potential social engineering incidents	SP 800-61r2
	8. Regularly review and monitor financial accounts for any unauthorized transactions or suspicious activities.	Monitor bank statements and credit card transactions	Encourage users to review financial accounts regularly and report any unauthorized or suspicious activities	Various financial regulations and policies, such as Payment Card Industry Data Security Standard (PCI DSS)

Finally, the guidelines for vendors as presented in Table 4, are quite similar to those for IT administrators. Vendors should establish comprehensive security awareness training programs for their employees, implement MFA for all systems and services, and regularly update and patch their software and systems. Enforcing strict password policies and the use of encryption for sensitive data are equally important. Conducting security audits and assessments, establishing an incident response plan, monitoring and logging system activities, and providing ongoing security training for employees are essential practices for vendors as well. The effectiveness of these guidelines depends on the implementation and enforcement within organizations. It requires commitment from management, adequate resource allocation, and continuous monitoring and improvement. Compliance with international standards, policies, and rules such as ISO/IEC 27001:2013, NIST SP 800-63B, NIST SP 800-61r2, NIST SP 800-53, and others provides a framework for organizations to align their practices with industry best practices.

Table 4: Guidelines for Vendors

Category	Guideline Description	Example Event/Activity	Step-by-Step Policies	International Standard/Policy/Rules
Vendors	1. Establish comprehensive security awareness training programs for employees to recognize social engineering tactics.	Conduct regular phishing simulation exercises	Develop and implement a training curriculum	ISO/IEC 27001:2013
	2. Implement multi-factor authentication (MFA) for all systems and services.	Enforce MFA for accessing company email accounts	Configure MFA settings for all relevant systems	NIST SP 800-63B
	3. Regularly update and patch all software and systems to address known vulnerabilities.	Apply security updates promptly and regularly	Establish a patch management process	ISO/IEC 27001:2013
	4. Implement strict password policies requiring strong,	Enforce password complexity and expiration	Define password policy	NIST SP 800-63B

	unique passwords.	requirements	guidelines	
	5. Enforce the use of encryption for sensitive data in transit and at rest.	Encrypt data stored on company servers and databases	Implement encryption protocols and technologies	ISO/IEC 27001:2013
	6. Regularly conduct security audits and assessments to identify vulnerabilities and areas of improvement.	Perform periodic penetration testing and vulnerability assessments	Develop an audit and assessment schedule	ISO/IEC 27001:2013
	7. Establish an incident response plan to handle social engineering incidents effectively.	Create an incident response team and define roles	Document incident response procedures and escalation process	NIST SP 800-61r2
	8. Monitor and log system activities to detect and respond to social engineering attempts.	Implement a security information and event management (SIEM) system	Define logging and monitoring procedures and review logs	ISO/IEC 27001:2013

5. Conclusion

Based The proposed guidelines cover various aspects of social engineering, including security awareness training, multi-factor authentication, software and system patching, password policies, encryption, security audits, incident response planning, system monitoring, and ongoing training for IT administrators, users, and vendors. These guidelines are designed to address the technical and human-centric aspects of social engineering, providing organizations with a comprehensive defense framework. By adopting these guidelines, organizations can enhance their security posture and improve their resilience against social engineering attacks.

References

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science, 3,* 1-23.

Allodi, L., Chotza, T., Panina, E., & Zannone, N. (2020). The need for new Antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy, 18*(2), 23-34.

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, 21*(1), 2-35.

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of social engineering attacks on social networks. *Procedia Computer Science, 198*, 656-661.

Incident statistics. (2023). *Cyber Security Malaysia*, MyCert.

Kaushalya, S., Randeniya, R. M., & Liyanage, A. D. (2018). An overview of social engineering in the context of information security. *2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 22-23 November 2018, Bangkok, Thailand.

Klein, G., Zwilling, M., & Lesjak, D. (2022). A Comparative Study in Israel and Slovenia Regarding the Awareness, Knowledge, and Behavior Regarding Cyber Security. *Advances in Human and Social Aspects of Technology*, 424-439.

Krejcie, R. V., & Morgan, D. W. (1970). Determining Sample Size for Research Activities. *Educational and Psychological Measurement*, *30*(3), 607-610.

Obuhuma, J., & Zivuku, S. (2020). Social Engineering Based Cyber-Attacks in Kenya. *2020 IST-Africa Conference (IST-Africa),* Africa.

Rajendran, T., & Mohd Shah, D. (2020). Students' perception on Gamification: The use of Kahoot. *International Journal of Scientific and Research Publications (IJSRP), 10*(05), 773-783.

Selvaganapathy, S., Sadasivam, S., & Ravi, V. (2021). A review on Android malware: Attacks, countermeasures and challenges ahead. *Journal of Cyber Security and Mobility, 10*(1), 177-230.

Timans, R., Wouters, P., & Heilbron, J. (2019). Correction to: Mixed methods research: what it is and what it could be. *Theory and Society, 48*(3), 509-510.

Wang, Z., Zhu, H., & Sun, L. (2021). Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods. *IEEE Access, 9,* 11895-11910.