p–ISSN: 2723 – 6609 e-ISSN: 2745-5254
Vol. 6, No. 1, January 2025 http://jist.publikasiindonesia.id/

Controlling Social Engineering and Spear Phishing Attack Security with Technology Solutions in Organizations

Taresa Vindy Oktavia[1*], A Widjajarto[2], Muhammad Fathinuddin[3]
Universitas Telkom, Bandung, Indonesia
Email: taresavindy@student.telkomuniversity.ac.id[1*], adtwjrt@telkomuniversity.ac.id[2], muhammadFathinuddin@telkomuniversity.ac.id[3]

*Correspondence

Keywords: OSINT, phishing, social engineering, technology-based.

ABSTRACT

In the current digital era, protecting information and being alert to the risk of data leaks is very important, especially for confidential data. Efforts to maintain the confidentiality of this information can use appropriate technology to prevent potential security threats. Using Open Source Intelligence (OSINT) can play a role in reducing the risk of phishing attacks by utilizing technology-based methods that involve social engineering activities and implementing spear phishing experiments via email content. This is useful for identifying security weaknesses that must be fixed. This research includes the application of OSINT, social engineering tools, and email content. Experiments involving OSINT and phishing attacks are depicted using Data Flow Diagrams (DFD) to show the flow of attacks carried out. Furthermore, the phishing attack is used as a basis for designing technology-based mitigation. This mitigation involves two technologies, namely email filters on email servers and two-factor authentication (2FA) for websites that are targets of phishing attacks. The addition of the two-factor authentication feature can be done because the target website has input in the form of an account and password text box.

Introduction

In the current digital era, information security and awareness of the risk of data leaks are very crucial in the use of information technology, especially for confidential and strategic data (Alshammary & Ali, 2024). Every piece of information needs to be protected to ensure its security and confidentiality remain protected from various threats, such as access, misuse, disclosure, interference, change, or destruction by unauthorized parties (Sie, 2024). To overcome this challenge, social engineering is often used by criminals as a way to exploit human weaknesses in security systems. Through psychological manipulation, they can trick individuals into providing access to sensitive information that should be carefully guarded (Al Khajeh, 2018).

In this regard, this research takes a novel approach by thoroughly integrating Open Source Intelligence (OSINT) techniques into information security analysis and phishing experiments. Different from previous research that tends to separate OSINT and phishing aspects, this research shows how OSINT can be used more efficiently to strengthen the

understanding of current information security vulnerabilities and improve the efficiency of targeted phishing attacks (Alshammary & Ali, 2024).

In overcoming information security challenges, especially in analyzing data leaks, the use of OSINT tools becomes very important. OSINT is used to collect and analyze data from open sources to detect potential data leaks (Bagheri & Akbari, 2018). For example, in the case of personal data leaks in organizations, OSINT can be utilized to carry out social engineering activities by collecting information from public sources and organizational websites. The information obtained is then used to carry out phishing experiments using spear phishing techniques, which aim to measure the level of security vulnerability of an organization (Anderson & Sun, 2017).

This research lies in the use of Data Flow Diagrams (DFD) to visualize and analyze the flow of phishing attacks. This approach provides a new perspective in understanding the dynamics of cyber-attacks, allowing the identification of critical points in the attack process that can be targeted for mitigation strategies (Lasrado & Kassem, 2021). In addition, this research also developed a method of structured comparative analysis of phishing email content, using comparison tables to identify key factors affecting attack success (Macfarlane et al., 2024).

Organizations can implement mitigation through technology-based methods to deal with phishing attacks. This action aims to strengthen organizational protection and reduce the risk of phishing attacks so that data and information security remain protected. This research is important because it provides practical guidance on the application of the method and helps organizations understand how best to integrate technologies such as email filters and two-factor authentication in security strategies (Cahyani & Abadiyah, n.d.).

By applying experiments to real cases and testing the vulnerability of organizations' websites, this research connects cybersecurity theory and its practical implementation. It also demonstrates the effectiveness of technology-based methods, such as email filters and two-factor authentication (2FA) in improving cybersecurity. This provides important insights for information security practitioners and helps deepen the understanding of security vulnerabilities in organizations.

Method

Systematics of Problem Solving

Systematic problem-solving is designed as a structured flow that functions as a guide in solving problems that arise during research. This methodology consists of five main stages: initial stage, hypothesis stage, experimental stage, analysis stage, and reporting stage. The following is a diagram illustrating the systematic steps to solve the problem:

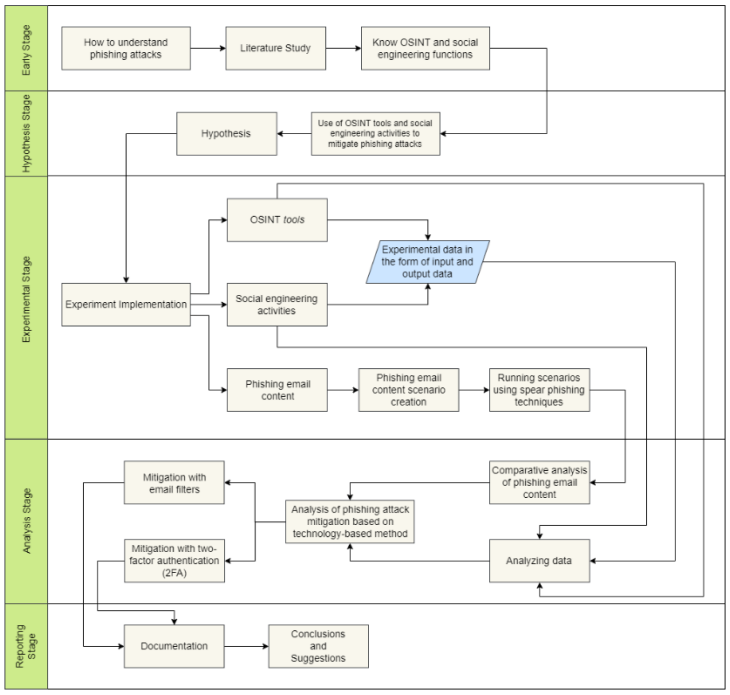

Figure 1
Systematics of Problem Solving

Early Stage

The initial stage of this research involved understanding phishing attacks by referring to literature studies. This literature study aims to deepen understanding of theories related to phishing attacks. Then, an understanding of OSINT functions and social engineering activities is carried out.

Hypothesis Stage

The second stage is the hypothesis stage. At this stage, hypotheses are prepared using OSINT tools and social engineering activities to develop mitigations based on phishing attacks.

Experimental Stage

At this experimental stage, where the implementation of the experiment is carried out and divided into three main stages, namely:

1. Experiment implementation using OSINT tools
2. Experimental implementation of social engineering activities
3. Experimental phishing attack on email content

In a phishing attack experiment on email content, the cloning of an organization's website was carried out through social engineering activities. The results of experimental implementation using OSINT tools and social engineering activities in the form of input data and output data. Then, carry out phishing email content scenarios using spear phishing techniques (Ariani et al., 2024).

Analysis Stage

The fourth stage is the analysis stage. After carrying out experiments using OSINT tools and social engineering activities, the data will be analyzed. Then, after running the phishing email content scenario using the spear phishing technique, a comparative

analysis of the phishing email content will be carried out based on this technique. Next, phishing attack mitigation analysis will be carried out using technology-based methods. This phishing attack mitigation analysis includes several aspects consisting of:

1. Mitigation with email filters
2. Mitigation with two-factor authentication (2FA)

These mitigations add a layer of protection to ensure information security and prevent unauthorized access in an ever-evolving digital environment.

Reporting Stage

The final stage in this research is the reporting stage, where a report on the research results is prepared, including conclusions and suggestions regarding OSINT, social engineering, and mitigation activities.

Results and Discussion

This section explains the experimental process carried out to obtain data, including specifications of the devices used, phishing attack experiment scenarios, as well as mitigation analysis using technology-based methods to determine appropriate preventive measures.

Hardware Specifications

Hardware is a physical component that can be seen and connected directly to a computer system or in its structure that supports computer operations to keep it running. (Salsabilla, 2022). Table 1 presents details of the hardware specifications used during the testing and research process. Following are the details of the hardware used:

Table 1
Hardware Specifications

Component		Information
Main OS Specifications	Processor	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz 2.40 GHz
	Memory	8000MB RAM
	Hard Disk	512GB SSD
	SystemType	64-bit operating system, x64-based processor
	Operating System	Windows 11 Home Single Language
Virtual Machine Specifications	Processor	2 Processors
	Memory	4096MB RAM
	Hard Disk	512GB
	System Type	64-bit
	Operating System	Kali Linux 2022.1 Kali-rolling

Software Specifications

Software is a program that consists of data stored on a computer. Although it is digital data that has no physical form, software can be used by computer users. Examples of software include operating systems, applications such as Microsoft Office, antivirus and so on (Jurnal Publikasi et al., 2022). Table 2 is a table that describes software specifications during the testing and research process. Following are the details of the software used:

Table 2
Software Specifications

Type	Software	Version
Operating System	Kali Linux	2022.1 Times-rolling
OSINT Tools	TheHarvester	4.6.0
	Spiderfoot	4.0.0
	Skymem	Tools used in 2024
	GoogleFU	Tools used in 2024
Phishing Tools	Social Engineering Toolkit (SEToolkit)	8.0.3

Social Engineering Activity Implementation Scenario

In the following implementation scenario, a flow summary is presented explaining how the process of collecting information in the form of data is carried out using OSINT tools to reach the final result (Nasir et al., 2024). Each step in this process plays an important role in ensuring that the information obtained is accurate and useful.

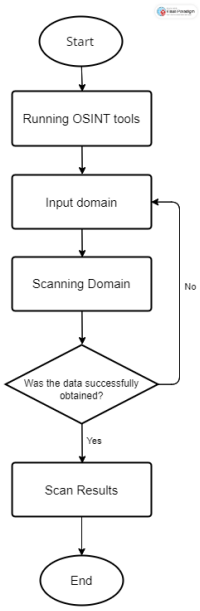

Figure 2
Social Engineering Activity Scenario

Figure 2 shows a scenario of social engineering activities using OSINT tools up to the stage of obtaining data with the following steps:

a. Start by running OSINT tools
b. Enter the target domain
c. Perform domain scanning, to determine whether the data was successfully obtained, if not successful it will return to the previous stage
d. If the data is successfully obtained, it will produce a data scan and the process will be complete

Phishing Attack Experiment Scenario

This experimental scenario summarizes the process flow of collecting sensitive information from targets. This process utilizes SEToolkit, a Python-based open-source pentest tool designed to perform penetration testing and social engineering activities. The main purpose of SEToolkit is to steal credentials, such as username/email and password from the target. SEToolkit is run through the Kali Linux terminal. Several features can be used in social engineering such as cloning websites, phishing, capturing the desktop activity of the target computer, and others (Ramadhaniyati et al., 2024). Each stage in this process is described in detail to provide a clear understanding of how this tool works and the techniques applied in the experiments.

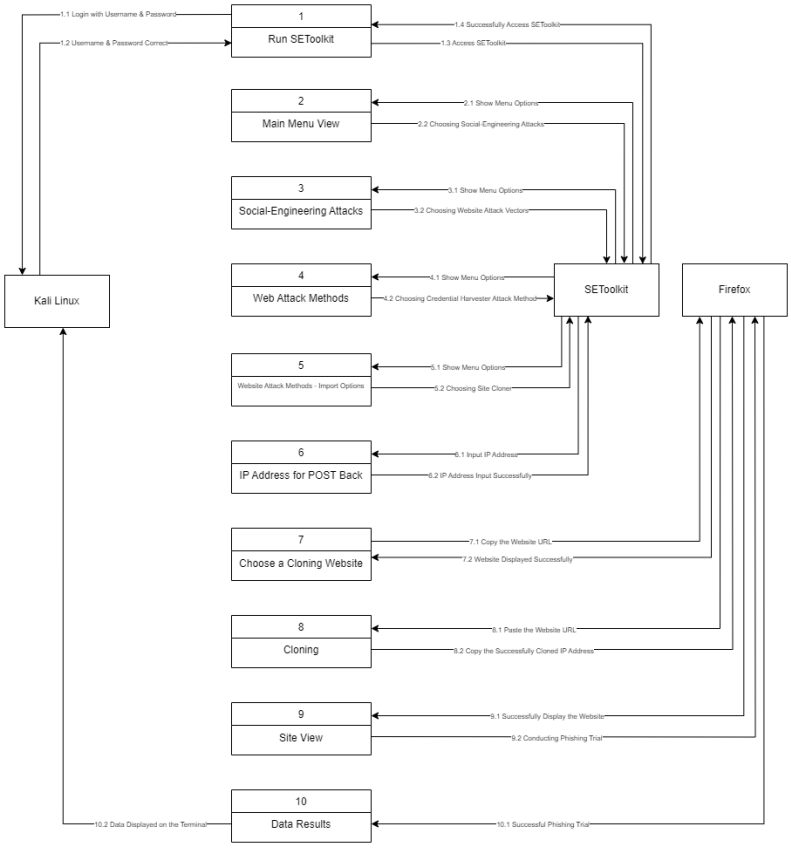

Figure 3
Data Flow Diagram of Phishing Attack Experiment

Figure 3 shows the experimental stages for a cloning experiment on an organization's website, which was obtained through social engineering activities and implemented in a Data Flow Diagram. If the cloning process is successful, the resulting website will be used to continue the phishing attack to collect sensitive information from the target. Next, the data obtained will be displayed via SEToolkit in the Kali Linux terminal.

Phishing Attack Experiment on Email Content

This experiment is designed to send fake emails that appear genuine to targets, to trick them into providing personal information by opening a link sent in the email. The personal information requested is in the form of a username and password or other data.

Phishing Attack Experiment on Website 1 (website1.zzz.xx.aa)

This phishing attack experiment involved sending specially designed emails with this content to divisions in this organization, the information of which was obtained through social engineering activities using OSINT tools. This experiment is an attempt to clone website 1 to test security against this attack using SEToolkit.

Figure 4
Experiment on Website Email Content 1

Figure 4 shows an example of a phishing email designed to obtain login information from a target disguised as an official email from the IT Team to a division in the organization. This experiment can help to understand phishing attack methods and how to avoid similar emails.

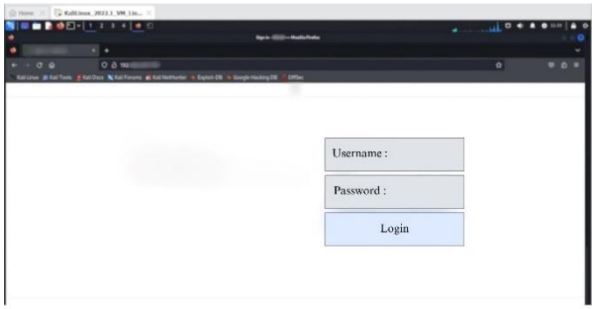

Figure 5
Results Experiments on Website Email Content 1

Figure 5 shows the results of an experiment carried out by displaying a URL similar to the official website contained in the email sent to the target. If the target enters the username and password, they will get personal information and the resulting data will be displayed on SEToolkit. This can be concluded, namely that website 1 was successfully cloned, which indicates that the website has a security gap that is vulnerable to phishing attacks.

Phishing Attack Experiment on Website 2 (website2.zzz.xx.aa)

The phishing attack experiment using SEToolkit involved sending specially designed emails with such content to divisions in this organization by conducting website cloning experiments 2. This aimed to deceive division members by providing sensitive information when accessing the URL provided in the email.

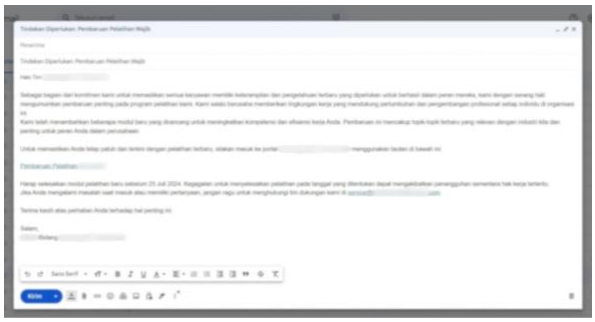

Figure 6
Experiments on Website Email Content 2

Figure 6 shows an example of a phishing email designed to obtain login information from a target disguised as an official email from the Team to a division in the organization. This experiment can help to understand phishing attack methods and how to avoid similar emails.

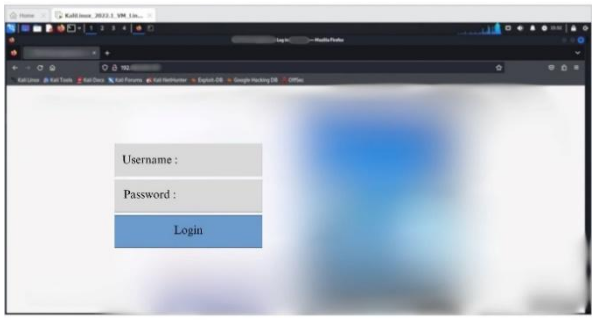

Figure 7
Results Experiments on Website Email Content 2

Figure 7 displays the results of an experiment that shows a URL that resembles an official website in an email sent to the target. If the target enters a username and password, the personal information will be obtained and displayed in SEToolkit. From these results, it can be concluded that website 2 was successfully cloned, indicating that the site has a security vulnerability to phishing attacks.

Email Content Comparison Table

This table is part of a report that discusses the comparison of email content aimed at deceiving targets. Table 3 serves to identify factors that have an impact on the security and vulnerability of a system or website.

Table 3
Comparison of Email Content

Factor

No.	Target	Website information	Website cloning results		Website vulnerability after cloning	
			Succeed	Not successful	Strong	Weak
1	Website1 (website1.zzz.xx.aa)	✓	✓	-	-	✓
2	Website2 (website2.zzz.xx.aa)	✓	✓	-	-	✓

Table 3 displays the comparative results of information search and website cloning experiments on two different target organizations. Overall, both websites show weaknesses in security against phishing attacks, so improvements to the security system are needed.

Relationship between Data Flow Diagrams and Email Content Experiments

The relationship between the Data Flow Diagram (DFD) and email content experiments lies in the DFD which describes the process flow, starting from the website cloning stage until successfully obtaining the target login information. In table 4 DFD plays a role in designing preventive mitigations according to the type of attack carried out, thus ensuring that more appropriate security measures can be implemented based on experiments carried out through phishing email content scenarios.

Table 4
Relationship of Data Flow Diagram to Experiment

No.	Stage in DFD	Attack Type	Mitigation
1	The ninth stage	Website cloning	Two-factor authentication (2FA) implementation
2	Seventh stage	URL link in email	Use of email filters

Mitigation in the Use of Email Filters

An email filter is an automated mechanism that categorizes emails based on certain criteria, such as sender, subject, or content, to ensure only safe emails arrive in a user's inbox. This filter is tasked with checking incoming emails to detect spam, malware attacks, and suspicious links. Additionally, email filters play a role in organizing emails into appropriate folders to ensure that email content does not contain sensitive or malicious content.

With this technology, email filters can detect and stop suspicious or potentially dangerous emails before they reach the user's inbox. These, email filters are also related to mitigation to prevent data leaks against phishing attacks. Table 5 explains the relationship between the effectiveness of email filters in detecting threats and the increased mitigation capabilities gained through implementing this technology.

Table 5
Relationship between Email Filter Use and Mitigation

Interrelationship of Email Filters and Mitigation		
No.	**Email Filters**	**Mitigation**
1	Domain and sender analysis	Email filters evaluate sender domains and email addresses to identify suspicious sources frequently used in phishing attacks.
2	Reporting and alerts	Email filters can alert users when phishing emails are detected, enabling immediate response for mitigation.
3	Blocks dangerous links	The filter can detect and block links in emails that direct users to websites or contain malware.

Mitigation in Two-Factor Authentication (2FA) Implementation

Two-factor authentication (2FA) is a security method that requires two steps of verification before users can access certain accounts or services. The goal is to provide additional protection beyond the use of passwords. Passwords are often vulnerable to phishing attacks, but with two-factor authentication, the risk can be minimized. In this method, users need to enter an additional verification code. The code is known only to the user and is sent by the associated application or website. With this, two-factor authentication (2FA) is related to mitigation to reduce various security risks faced by users. Table 6 explains two-factor authentication which is an important component in mitigation, especially in dealing with threats such as password hacking and phishing attacks.

Table 6
The Link between Two-Factor Authentication Implementation and Mitigation

The Interrelationship of Two-Factor Authentication and Mitigation		
No.	**Two Factor Authentication**	**Mitigation**
1	An additional layer of security	Two-factor authentication adds a layer of verification beyond passwords, providing extra protection and significantly reducing the risk of unauthorized access.
2	Reduction of phishing risk	Two-factor authentication reduces the risk of phishing attacks. If a user accidentally provides a password via phishing, the attacker still needs a second authentication factor.
3	Prevention against password hacking	Even if a user's password is successfully cracked, the attacker still needs a second authentication factor, which is usually only available to authorized users, such as a code

	from an authentication application or a text message.

Conclusion

Spear phishing utilizes OSINT tools to collect detailed information used in social engineering activities. Under a fake identity, such as a coworker or IT team, a legitimate-looking email is sent, containing a link to the organization's website to steal login credentials. This attack is effective because the message appears convincing, making the target more likely to reveal sensitive information. OSINT, Data Flow Diagrams, and Social Engineering are interrelated in implementing phishing attacks. OSINT tools used to collect additional information are TheHarvester, Spiderfoot, Skymem, and GoogleFU. With that in mind, implement effective mitigation based on the results of email phishing experiments using technology-based methods. There are two technologies used, namely email filters and two-factor authentication (2FA). Email filters act as a first line of defense by detecting and blocking malicious emails, while two-factor authentication (2FA) provides an additional layer of protection, reducing the risk of unauthorized access even if passwords are stolen. The combination of email filters and two-factor authentication (2FA) increases security and reduces the risk of phishing attacks.

Bibliography

Al Khajeh, E. H. (2018). Impact of leadership styles on organizational performance. *Journal of Human Resources Management Research*, *2018*(2018), 1–10.

Alshammary, F. M., & Ali, D. A. (2024). Role of Knowledge Management Process in Fostering Employee Performance: Assessing the Moderating Effect of Smart Technologies. *International Journal of Religion*, *5*(3), 111–127.

Anderson, M. H., & Sun, P. Y. T. (2017). Reviewing leadership styles: Overlaps and the need for a new 'full-range'theory. *International Journal of Management Reviews*, *19*(1), 76–96.

Ariani, D., Riswandi, R., & Maulina, D. (2024). Development of a Model of Transformational Leadership Behavior and Ethical Leadership of Elementary School Principals in Creating Excellent Schools. *IJORER: International Journal of Recent Educational Research*, *5*(4), 835–851.

Bagheri, A., & Akbari, M. (2018). The impact of entrepreneurial leadership on nurses' innovation behavior. *Journal of Nursing Scholarship*, *50*(1), 28–35.

Cahyani, K. D., & Abadiyah, R. (n.d.). *Entrepreneurship Leadership, Entrepreneurship Culture, Entrepreneurship Orientation on Employee Performance of IKM Tas Tanggulangin Sidoarjo: Entrepreneurship Leadership, Entrepreneurship Culture, Entrepreneurship Orientation terhadap Kinerja Karyawan IKM Tas Tanggulangin Sidoarjo*.

Lasrado, F., & Kassem, R. (2021). Let's get everyone involved! The effects of transformational leadership and organizational culture on organizational excellence. *International Journal of Quality & Reliability Management*, *38*(1), 169–194.

Macfarlane, B., Bolden, R., & Watermeyer, R. (2024). Three perspectives on leadership in higher education: traditionalist, reformist, pragmatist. *Higher Education*, 1–22.

Nasir, M., Arief, M., Alamsjah, F., & Elidjen, E. (2024). Systematic Literature Review: The Role of Innovation and Competitive Advantage of Micro, Small, and Medium Enterprises as Mediation Variables. *Quantitative Economics and Management Studies*, *5*(3), 600–612.

Ramadhaniyati, R., Subekti, E. S., Widiasari, W., Lizein, B., & Ahmad, S. Y. (2024). Implementation of Human Resource Management at Smk Negeri 1 Cisarua. *Journal of Multidisciplinary Global*, *1*(2), 135–148.

Sie, S. (2024). The Role of Digital Leadership on Service Excellent in Palm Oil Industry. *Journal of Current Research in Business and Economics*, *3*(1), 2704–2723.