Journal of COMPUTER AND FORENSIC SCIENCES

CFS 2023, Vol. 2, Issue 1, pp. 43–52
https://doi.org/10.5937/jcfs2-44741
Original research paper

A System Architecture for Preventing Social Engineering Attacks via E-mail

Milan Brkić[1], Aleksa Maksimović[2], and Aleksandar Miljković[3]

[1] Ministry of Interior of the Republic of Serbia; milan.brkic@mup.gov.rs

[2] Ministry of Interior of the Republic of Serbia; aleksa.maksimovic@mup.gov.rs

[3] Ministry of Interior of the Republic of Serbia; aleksandar.miljkovic@mup.gov.rs

* Corresponding author: milan.brkic@mup.gov.rs

Received: May 30, 2023 • Accepted: June 30, 2023 • Published: July 13, 2023

Abstract: Modern business and the expansion of internet technology have caused a great growth in communication via electronic mail. Bearing in mind that the weakest link in any system is the human, the greatest danger of unauthorized access to ICT resources is recognized in this section of the system [6]. For this reason, the greatest attention regarding the protection of ICT systems should be focused on the users and preventive response to phishing campaigns as the most common form of cyber attack. This paper will present the system architecture for preventive response to phishing campaigns. The architecture itself, which will be explained in the continuation of the text, consists of several different modules integrated into a whole. First, a sender analysis module, which would be based on the blacklist principle; next, an email attachment analysis module, which would perform the functions of static and dynamic analysis of potentially malicious attachments; a link analysis module, which would include the application of Cortex, an open source intelligence service; and finally, a text analysis module, based on statistical models.

Keywords: phishing; Cortex; analysis; cyber attack.

1. INTRODUCTION

Phishing attacks have become one of the most prevalent and insidious forms of cybercrime. Phishing is a social engineering attack that tricks individuals into divulging sensitive information or downloading malware through fraudulent emails, websites, or messages. The increasing frequency and sophistication of these attacks pose a significant threat to individuals, organizations, and society as a whole.

This paper focuses on the prevention of phishing attacks through the use of a novel system. To better understand this system, it is important to first examine the nature of social engineering attacks and phishing in general. Social engineering is a tactic used by cybercriminals to manipulate individuals into divulging sensitive information or performing actions that can lead to unauthorized access or data breaches. Phishing is the most prevalent type of social engineering, which uses deceptive emails, websites, or messages to steal perso-

Citation: M. Brkić, A. Maksimović, and A. Miljković, "A System Architecture for Preventing Social Engineering Attacks via E-mail," *Journal of Computer and Forensic Sciences*, vol. 2, no. 1, pp. 43–52, 2023, https://doi.org/10.5937/jcfs2-44741.

nal or financial information. Phishing attacks can also be used to install malware or ransomware onto a victim's computer, causing significant damage to both individuals and organizations. There are several methods to defend against phishing attacks. One approach is to train individuals to recognize and avoid phishing attempts. This involves educating them about the common tactics used by attackers and how to identify suspicious emails or websites. Another approach is to implement technical defenses, such as spam filters, web filters, and email authentication protocols, which can help detect and block malicious messages or websites. In the second chapter, we are going to talk in more detail about social engineering and phishing, as well as ways to defend against phishing and what is being done in this field.

The novel system we propose uses multiple approaches in combination with machine learning algorithms to analyze incoming emails and identify potential phishing attempts. The system then sends a warning message to the user, advising them to avoid the email or website. The proposed system also includes a reporting mechanism, allowing users to report suspicious emails or websites to IT security personnel. This system is explained in detail in the third chapter. The fourth chapter is reserved for discussion. At the end, we conclude this paper.

2. MATERIALS AND METHODS

2.1. Phishing and Social Engineering

When talking about social engineering and its application from the cyber security point of view, as well as from the data and information security point of view, one must first understand what is meant by social engineering, when it occurs, and where and how it is applied in the everyday lives of the individual and the community. Once we understand these basic concepts related to social engineering, we can try to understand in what way the "bad guys" in the field of cyber security use these techniques that lead to unauthorized access to data and information that can be misused.

Social engineering is a technique or method of human manipulation that has been named in the world of computers and cyber security social engineering, but before the emergence of the cyber world, it existed and was used in various fields, such as marketing, trade, espionage, and everyday life. The very name of this method tells us a lot about it. The two words that describe this method, social and engineering, can be used for the most appropriate definition of it.

The word social makes it clear that we are talking about everyday human life, in a private or professional sense. Society is a collection of living beings connected by the same way of life, an accidental or intentional gathering of several persons, or an association. In this sense, society is defined as the totality of social phenomena, processes, and relationships. This definition of the first word of the name of this method tells us that it is based on man and is closely related to society, at all levels.

The second word in the name of this method is engineering. We can best understand this as a defined way of acting in the execution of a task through certain steps in order to reach the goal. In other words, it is usually possible to represent the method through some kind

of algorithm. However, this method is considered a non-technical type of hacker attack, and can be considered a form of art.

The social engineering process typically includes the following phases:

- Examination – The scanning phase is part of the reconnaissance phase, which comes before the examination phase in the social engineering process. During the reconnaissance phase, the attacker gathers information about the target organization, including identifying potential vulnerabilities and weaknesses.
- Development phase of a social engineering attack involves selecting individual targets within the organization being attacked and forming a relationship with the selected targets. However, the claim that attackers usually select people who show signs of being frustrated, overconfident, arrogant, or somehow easy to extract information from is not entirely accurate. While attackers may target individuals who have access to the desired information or object, they may also target individuals who are perceived as helpful or trusting. Attackers may use a variety of tactics, such as building rapport, flattery, or creating a sense of urgency, to manipulate their targets into providing the desired information or taking an unauthorized action. In the development phase, the attacker creates a plan of attack tailored to the selected targets, which may involve creating a pretext, preparing the necessary tools, and practicing the attack.
- Exploitation phase – Attackers use a closer relationship technique with the aim of extracting information, gaining access to a certain ICT system, or achieving the goals they have in mind. However, the claim that if the exploit is successful, the only thing left is to get things done without raising suspicion is not entirely true. After the exploitation phase, attackers may need to maintain access to the compromised system or continue to extract information. Attackers may need to cover their tracks to avoid detection by the target organization's security measures. This may include erasing digital prints, ensuring no items or information are left behind, and taking steps to prevent being identified as an attacker. However, it is important to note that covering one's tracks is not always possible, and there is always a risk of being caught or identified during or after an attack.

To obtain information and fulfill their goal, attackers use several types of techniques to motivate employees to provide information, and those are: authority, social proof, urgency, and scarcity. Attackers are different, and they may have different motives, attributes, and attack characteristics. Some attackers may be motivated by financial gain, while others may be motivated by ideology or revenge. Attackers may also have different skill levels, resources, and access to tools and techniques. There are several common types of phishing attacks [1]:

- Whaling – Whaling is a form of social engineering attack that targets senior executives and high-profile individuals in organizations. It is a type of phishing attack that uses personalized messages and tactics to trick the target into divulging sensitive information or taking an unauthorized action. Whaling attacks may involve impersonating a trusted individual, such as a CEO, to gain the target's trust and obtain sensitive information or access to the organization's systems. Whaling attacks often use sophisticated techniques, such as spear-phishing and social engineering, to create a sense of urgency and manipulate the target into taking the desired action. Whaling attacks can have

serious consequences for the targeted organization, including data breaches, financial loss, and damage to the organization's reputation.

•Vishing – Vishing is a type of social engineering attack that uses Voice over IP (VoIP) technology to trick victims into divulging sensitive information or taking an unauthorized action. The term "vishing" is a combination of "voice" and "phishing". In a vishing attack, the attacker typically poses as a trusted authority, such as a bank representative or IT support technician, and uses a recorded or live voice message to create a sense of urgency or fear in the victim. The message may instruct the victim to call a phone number or visit a website to verify their account information or resolve a security issue. When the victim responds, they are prompted to enter their personal or financial information, which the attacker can then use for fraudulent purposes. Vishing attacks can be difficult to detect as they often appear to be legitimate messages from a trusted source. To avoid falling victim to a vishing attack, it is important to be cautious of unexpected or suspicious phone calls and to verify the authenticity of the message before sharing any sensitive information.

•SMS phishing – SMS phishing, also known as smishing, is a type of phishing attack that uses text messages to trick the victim into divulging sensitive information or taking an unauthorized action. The attacker sends a text message with a message that appears to be urgent or important, such as a security alert or account notification, to create a sense of urgency and encourage the victim to act quickly. The message may contain a link or phone number that the victim is instructed to click on or call, which leads to a fake website or automated voice system that prompts the victim to enter their personal or financial information. Once the attacker has obtained this information, they can use it for fraudulent purposes, such as identity theft or financial fraud. SMS phishing attacks can be difficult to detect as they often appear to be legitimate messages from a trusted source. It is important to be cautious of any unexpected or suspicious text messages and to verify the authenticity of the message before taking any action.

Social engineering attacks via email (or phishing emails) are becoming increasingly common and can have devastating consequences for both individuals and organizations. In the case of this method, the attacker usually writes an email, which should convince the victim to access a malicious link, download a file or a document. Such e-mails are sent to many e-mail addresses, and whoever clicks on that link and downloads the file or document is considered infected. One of the possible techniques used by attackers is the farming technique, in which the attacker executes malicious programs on the computer so that all URL traffic is redirected to the attacker's malicious website, thereby enabling the theft of credentials or obtaining some benefit.

In cases where a specific company or network is targeted, the email addresses of its members are targeted. If one takes into account that most companies assign e-mail addresses to their employees based on the first name.surname principle @name_of_the_company.com, the attacker has no problem attacking if they know the names of the workers.

Unlike an ordinary phishing attack, spear phishing attacks are not based on probability but are carefully constructed to be as believable as possible to the victim. This type of attack depends to a large extent on the information gathering stage, as well as on the bait being good enough for the victim to fall for the attack. Email spoofing and website cloning are two common techniques used by scammers to trick victims into divulging sensitive

information or taking an unauthorized action. In email spoofing, the attacker falsifies the "From" section of the email to make it appear as if the message is coming from a trusted source, such as that of a bank or a colleague. The message may contain a sense of urgency or a request for personal information, such as login credentials or financial details. If the victim falls for the scam and responds to the email, the attacker can use the information for fraudulent purposes. In website cloning, the attacker creates a fake website that looks identical to a legitimate one, such as a bank or online retailer. The victim is directed to the fake website through a link or email and may be prompted to enter their personal information.

Some of the most common emails that are sent are usually promises of a big prize, or some kind of discount, and all the victims must do is fill out a prompt or enter a website. In these situations, the attacker can be very creative. Events are also known when the attacker allegedly sends a summons to the court via email and asks the user to enter the page to confirm that they received the email. These are some of the more sophisticated attacks. Such attacks are mostly automated due to the huge number of attacks that target large masses of people based on probability theory. This type of attack must be supported from the technical side. The existence of a virus, malware, or malicious site is required. For this type of attack, as well as for most others, a group of tools is most often used called The Social-Engineer Toolkit (SET) created by TrustedSec which is an open-source project. This type of tool allows attackers to carry out social engineering attacks without much technical knowledge.

2.2. Defending against Phishing Attacks

In order to prevent these types of attacks, it is important to have a system in place that can detect and prevent them before they do any damage. Here are some strategies that can be used to prevent social engineering attacks via email.

Employee education: One of the most effective ways to prevent social engineering attacks via email is to educate employees on the various types of scams and how to identify them. This can include providing training on phishing emails, suspicious links, and other common tactics used by scammers.

Employees should be trained to handle emails carefully [5]:

- To verify that a link within an email points to the correct URL, one can hover their mouse over the link without clicking it. This will display the URL destination in the bottom left corner of the browser window. If the URL looks suspicious or does not match the expected website, one should not click on the link. Instead, one should type the website's address directly into the browser or contact the sender to verify the legitimacy of the email. It is also a good practice to avoid clicking on links within unsolicited emails or emails from unknown sources.
- While it is true that clicking on links in emails can be a risky activity, it is not always necessary to avoid them altogether. However, it is important to exercise caution and verify the legitimacy of the email and the link destination before clicking on any links. One should never write down or share passwords under any circumstances.

- Training users not to give their passwords to anyone is an important aspect of cybersecurity awareness. This is because password sharing can lead to unauthorized access to sensitive information and increase the risk of data breaches.
- One should not open an attachment that seems suspicious; it should be sent to the CERT team for analysis.

Spam filtering: Email spam filters can be used to prevent many social engineering attacks from ever reaching an employee's inbox. This can include filtering out messages from suspicious or untrusted sources or blocking messages with certain keywords or phrases.

Two-factor authentication: Implementing two-factor authentication can help prevent attackers from gaining access to email accounts by requiring a secondary form of identification beyond just a password.

Email encryption: Encrypted email systems can help prevent attackers from intercepting and reading sensitive email communications. This is why it is important to use encryption protocols such as Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to secure email communications. These protocols encrypt the data in transit, making it difficult for attackers to intercept and read the messages.

Regular updates and patches: Keeping email systems up-to-date with the latest security patches and software updates can help prevent attackers from exploiting known vulnerabilities.

Security awareness testing: Regular security awareness testing can help organizations identify areas where employees may be vulnerable to social engineering attacks via email and provide targeted training to help them improve their security posture. One of the better ways to check training success is the Gophish tool [4].

Gophish is an open-source phishing simulation tool that allows organizations to test and improve their employees' awareness of phishing attacks. It can be used to create and send simulated phishing emails to employees, track their responses, and provide training and education to help them recognize and avoid phishing attacks. With Gophish, organizations can create realistic phishing campaigns that mimic common attack techniques, such as social engineering, spear phishing, and phishing emails with malicious attachments or links. The tool includes customizable templates for emails and landing pages, as well as detailed analytics and reporting to track the success of the campaigns and identify areas for improvement. Gophish is designed to be user-friendly and easy to set up, with a web-based interface that allows administrators to manage campaigns, track results, and generate reports. It is available for free and can be downloaded from the Gophish website or from GitHub.

By implementing these strategies, organizations can significantly reduce the risk of falling victim to social engineering attacks via email. It is important to note, however, that no system is foolproof, and it is always important to remain vigilant and report any suspicious activity to IT or security personnel.

3. PROPOSED SYSTEM

The system is divided into three key segments:

- Applications for sending emails for analysis;
- System for processing and classifying emails; and
- Systems for training, updating, and improving models.

Each of the segments is described in more detail in the rest of the document and is viewed as a separate system unit that communicates through web services in a controlled network environment.

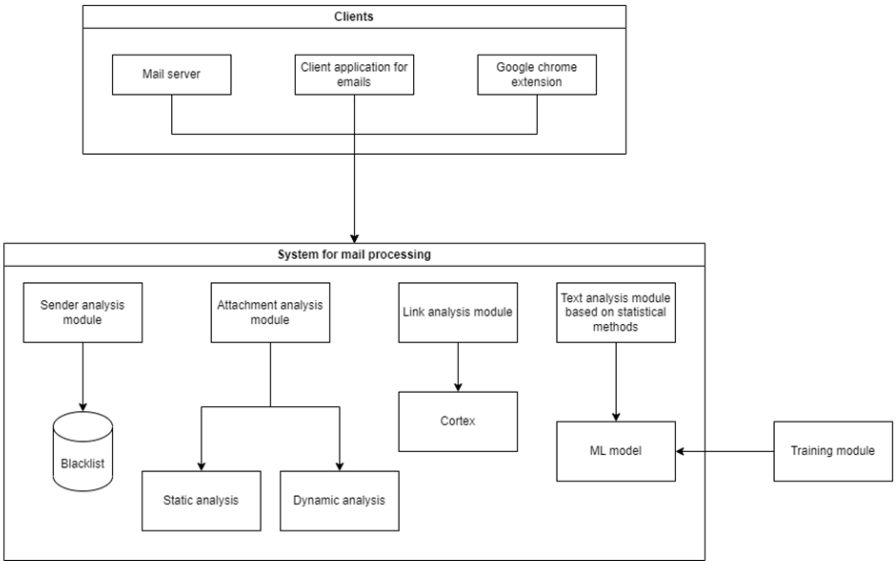

Figure 1. *Architecture of the proposed system.*

3.1. Applications for Sending Emails for Analysis

In order to send an email to the system for analysis, it is necessary to provide a mechanism that will allow the user to log in to this protection system, that is, to be logged in by the system maintainer.

- Browser extensions – A solution exclusively for using a web client for emails. The user decides which email they want to be sent for analysis. This solution can be demanding on the client-side. It also offers the possibility of analyzing emails on the client machine, but there is a security risk if the computer is compromised, that is, if the attacker comes up with statistical models that classify the email, they can modify the attacking email to bypass these rules.
- Server application that automatically analyzes e-mails – An application that automatically listens to the e-mails of users who sign up for this service and sends each e-mail for analysis.

- A client desktop application that does the same thing as a server application but only on the client-side.
- An email address to which clients could send emails they consider risky. This is a situation when the user decides which email they want to be sent for analysis by forwarding it to an email address that listens and forwards incoming emails for analysis.

3.2. System for Processing and Classifying Emails

The email processing system is conceived as a series of services that would be divided into several segments, each of which would be in charge of one part of the system.

- Sender analysis module – List of senders known to have already sent malicious emails, (i.e., black list). It is regularly updated by the system owner.
- Attachment analysis module – The attachment in the email can be analyzed dynamically and statically. Static could be both hash value analysis and file content analysis, while dynamic would represent the launch of attachments in a sandbox environment and monitoring of work.
- Module for link analysis – Cortex solution offers analysis of hyperlinks on the web.
- Text analysis module – The text analysis module would process the text of the email and perform a classification based on a statistical model trained on previously detected spam emails.

In the next part of the text, we would like to emphasize the importance of implementing the Cortex module when responding to phishing emails for analyzing and correlating security data from multiple sources. Cortex is an open-source intelligence platform. It is designed to help security teams automate the analysis and response to security incidents and threats, reducing the time and effort required to investigate and mitigate security incidents. By using Cortex, one gets the possibility to check whether a specific link is on the black list, i.e., the IP address of the server from which the email arrived, as well as other useful information that can be checked using the Cortex module in order to check for malicious content.

Cortex can help security teams automate and streamline their incident response and threat intelligence processes, reducing the time and effort required to investigate and respond to security incidents. It allows users to ingest and correlate data from multiple sources, such as SIEMs, threat intelligence feeds, and security tools, and uses a range of built-in and custom analyzers to perform automated analysis and trigger responses as needed [3].

3.3. Systems for Training, Updating, and Improving Models

This system should allow updating the configuration of each of the models as well as their maintenance and retraining of statistical models:

- Based on the sender analysis, blacklist is updated;
- Based on the attachment analysis, the lists of hash values and links to sandboxes are updated;

- To analyze the link path to Cortex;
- For text analysis, training a new statistical model, and updating the existing one.

4. DISCUSSION

There are several problems that the development of such a system would face. Some of the key issues are:

- Training a word processing module is only as good as the training set is representative. The implementation of such a solution would first involve training the model, so that phishing emails that are detected on one's system are examined, using a certain set of words that are repeated in phishing emails, which finally results in a model that is adapted to one's system and needs. Such an approach provides the possibility of a preventive response and reduces the possibility of false positives, because the existing models available on the internet are not sufficiently adapted to the specificities of certain speech areas. Therefore, the goal of this paper and future work is to encourage cyber experts to potentially create a model that will overcome the problems of specific dialects and work on creating a global model that will detect phishing campaigns.
- For dynamic analysis, it is necessary to set up a number of sandboxes that could serve the system. The use of sandbox solutions in this system raises several questions, but one of the most important is the time it takes for the sandbox to analyze a potentially malicious file found in a phishing email, because responding to phishing e-mails requires a prompt reaction in order to prevent data leaks and unauthorized access to the e-mail system.
- Regular training of the text analysis system is required, as well as regular updating of blacklists of malicious senders and hash values of malicious files.
- By regularly updating the model, as well as the database that the system uses to check the status of the email sender's IP address, and the hash value of the file contained in the phishing email, it is possible to receive timely information about current phishing campaigns that aim to harm information systems.

5. CONCLUSION

With the expansion of internet technologies, we are increasingly exposed to cyber attacks. The most frequent type of attack on ICT systems is phishing because it is based on human error, and we all know that humans are the weakest link in the ICT system. Due to all of the above, there was a need to develop a system to protect against phishing attacks.

This paper presents a proposal for system architecture for preventive response to phishing campaigns. As explained in more detail in the "Proposed System" section, the architecture itself is divided into two parts. On the client-side, it would represent an add-on for the client application for working with emails, and an extension for the internet browser, in this case the Google Chrome extension. The architecture also includes a system for processing emails, which would be made up of several modules.

First, a sender analysis module would be based on the blacklist principle. Next, an email attachment analysis module would perform the functions of static and dynamic analysis of potentially malicious attachments. A link analysis module would include the application of Cortex, an open source intelligence service, and finally, a text analysis module would be based on statistical models.

In conclusion, phishing attacks continue to be a significant threat to individuals and organizations worldwide. This paper has outlined the nature of social engineering attacks and the various ways to defend against them. It has also proposed a novel system for preventing phishing attacks, which can help organizations better protect their sensitive information and assets. By implementing a comprehensive approach to preventing phishing attacks, organizations can reduce their risk of falling victim to these insidious cybercrimes.

FUNDING:

This research received no external funding.

INSTITUTIONAL REVIEW BOARD STATEMENT:

Not applicable.

INFORMED CONSENT STATEMENT:

Not applicable.

CONFLICTS OF INTEREST:

The authors declare no conflict of interest.

REFERENCES

[1] G. Weidman, Penetration testing: a hands-on introduction to hacking. San Francisco, CA: No Starch Press, 2014.

[2] C. Hadnagy and M. Fincher, Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails. Hoboken, NJ: Wiley, 2015.

[3] TheHive-Project/Cortex. [Online]. Available: https://github.com/thehive-project/Cortex/. [Accessed: June 15, 2023].

[4] Gophish [Online]. Available: https://github.com/gophish/gophish. [Accessed: June 15, 2023].

[5] N. M. Shekokar, C. Shah, M. Mahajan, and S. Rachh, "An Ideal Approach for Detection and Prevention of Phishing Attacks," Procedia Computer Science, vol. 49, pp. 82–91, 2015.

[6] G. Nikhita Reddy, G.J. Ugander Reddy, "A study of cyber security challenges and its emerging trends on latest technologies," ArXiv preprint arXiv:1402.1842, 2014.