Email Security and Anti-phishing Measures

Naveen Ajay Karasu
MS in Cybersecurity
UNT

Aiswarya Palla
MS in Cybersecurity
UNT

Abstract

Email security is essential for protecting individuals and organizations from a variety of threats, including phishing attacks. Phishing attacks are fraudulent emails that attempt to trick recipients into revealing sensitive information, such as passwords, credit card numbers, or social security numbers.

They can be very sophisticated and difficult to detect, but there are several email security measures that can be taken to mitigate the risk.

Outline:

Introduction
Email security
What are phishing attacks and how do they work?
Common anti-phishing measures
How to implement effective email security and anti-phishing measures
Conclusion
Reference

Introduction

Email is one of the most widely used communication tools in the world, with billions of emails sent and received every day. Its communication is a critical component of today's organizational infrastructure. It's not just an application which is used to exchanging information through mails but also a potential vulnerability due to been used by pretty much every businesses, governments, and individuals people. The complexity in the email systems often leads to security vulnerabilities

However, email has become a common vector for cyberattacks, particularly phishing attacks. One of such incident is bugs in Gmail causing data loss [4]. The analysis of five popular email systems revealed significant concerns regarding password management and the risk of unauthorized access, emphasizing the need for stringent email security measures

Email security

Definition of email security

As the usage of emails became more and more common so, are the attacks using emails. In order to have control on this we need to have security for emails.

Email security involves protecting emails and communications from Illegal access, loss, or compromise. It should also includes measures to secure both access and content of email accounts or services, thereby ensuring confidentiality, integrity, and availability of email messages. This can be achieved through a combination of organizational policies and technological tools

Importance of email security

The security of the email is very important has they are used for transferring/ sending sensitive/critical information which is may be related to organizational operations. From the recent survey's about 90% attacks that take place on an organization are started with a malicious mail [5]. Due to this, the emails has become prime targets for the hacker to attack. So, Email security play an important role in securing the

organization trade secrets and other sensitive information

Benefits of email security

An effective email security will protect against phishing, spoofing and malware attacks, thereby safeguarding sensitive data and credentials. It also ensures message confidentiality and reduces the risk of identity theft. Additionally, it is important for maintaining regulated industries standards and enhances organizational productivity by reducing disruptions due to cyberattacks.

Phishing attacks

Definition of phishing attacks

They are a type of cyberattack that target individuals/organizations through various communication forms, aiming to trick recipients into revealing sensitive information like login and credit card details or installing malware on their devices. Here we are going to discuss about phishing using email as the medium. The phishing can be done using anything not a mail, we can do it using text message, survey forms etc..,

How phishing attacks work

It typically involves posing as authentic website/ luring the user with offers by sending emails or messages that look exactly as legitimate website would look like. The attacker's goal is to extract personal or financial information from the target, often by invoking a sense of urgency or security loss. These attacks employ social engineering tactics across different methods.

Examples of phishing attacks

In 2016, FACC attack caused has loss of around 42million euros loss to the company. In 2014, Sony pictures has lost a huge amount of 80 million euros to the hacking group called “Guardians of Peace”, according to the report they leaked to 100 terabytes of data from Sony studio [6].

How phishing attack works

Explaining the flow of phishing attack

These type of attacks typically begin with the attacker identifying a target, which can be an individual or an organization. The attacker then tries to gather some information which he uses to crafts a deceptive message, resembling communication from a trusted entity most of the time, to mislead/ trick into the target into performing certain actions. This might involve clicking/opening the malicious link, which can lead to malware installation, system freezing as part of a ransomware attack, or the revealing of sensitive information like usernames, passwords or personal identification information (PII). These emails often exploit human psychology, such as invoking a sense of urgency or fear, to prompt immediate action from the victim. So, the attacker need to have proper knowledge on the victim so, he can create a perfect mail that victim will won’t be having any doubts/suspicious of the mail.

Different steps involved in the attack:

- Confirming the target
- Gather info on the target.
- Generating/creation of fake emails or websites to mimic credible sources.
- Create a mail for sending it to the target.
- Send malicious content mail to the target.
- Making the target into performing actions like clicking on links or downloading attachments from the malicious mail we sent.
- Once target clicks on it, we can have access to his machine, which we can use for different purpose such as stealing sensitive data or installing malware on the target's system.

- The connection can be kept alive or destroyed depending on the attacker's need.

Types of phishing attacks

Attackers use many different tactics to hack email, and some methods too cause considerable damage to an organization's data and/or to its reputation and phishing is one of the attacker favorite techniques for performing the attacks. The phishing attacks can be further classified into different types depending on the attack type or techniques used for performing that phishing attack.

Spear phishing:

Spear phishing is one of the highly targeted form of phishing where attackers focus on specific individuals or organizations. Unlike other phishing attacks, spear phishing involves sending personalized messages to a particular target, often after conducting thorough research on the victim. The personalized nature of these attacks makes them more difficult for the target to detect and hence makes this attack more effective.

HTTPS phishing:

HTTPS phishing is type of phishing, where the attackers tricks you into giving up your PI using a malicious website. To get target to these sites, the attacker will hide the malicious link within an email, often sending them as a link to a legitimate site [7].

Angler phishing

It is a type of phishing attack in which the attacker pretends to be a customer service agent on social media platform. In addition to trying to steal target personal information, the attacker may also try to infect target device with malware [7].

Clone phishing

A clone phishing attack is when an attacker attempts to replicate a legitimate branded email which target may have already received while sneaking in a malicious link or attachment. In some cases, the cloned email may contain something like "reply" or "re-send" to make target think that it is from the original sender [7].

Pharming

It is a type of phishing method that utilizes malicious code and software to steal target information. Once the malicious code is in place, target's web traffic will be directed to fake and malicious websites without the knowledge or approval from the target.

Watering hole phishing

It is known as targeted phishing attack in which a attacker compromises a website that is used by a specific group of people/targets. In these attacks, the hacker is trying to infect the targeted users' devices with malware to gain access to private information.

Whaling

It is a type of attack when a attacker impersonates a top executive at a company hoping to steal money or private information from another high-level executive at the same company. This is also known as "executive phishing."

Pop-up phishing

It is a type of attack that leverages adware and pop-up ads to trick target into downloading malware onto their devices. These type of attacks include fake virus alerts and scare tactics to get you to click without thinking.

Evil twin phishing

It is a type of phishing attack, which is designed to steal target information using a fake Wi-Fi network. If you join an attacker's malicious network then they can monitor target web traffic and capture any login credentials target uses while connected. It's basically performed by looking the traffic in the network.

Search engine phishing

In this type of phishing attacks, the attacker attract targets/user's using fake product pages. When a potential customer is searching for a product online, they may come across one of the hacker's counterfeit pages using a search engine. The catch is that instead of being able to purchase the product, they're handing over their payment information to a scammer.

Image phishing

Image phishing is an attack in which hackers disguise malicious code or different types of malware using image files. These images may be included in the body of an email or linked as an attachment. If you click on the image, you may accidentally be putting your cybersecurity at risk.

Smishing

It stands for sending words over short message services (SMS). Similar to phishing emails, these phishing text messages usually use social engineering tactics and contain malicious links.

Email Security

Email security best practices

Best practices for enhancing email security include the following:

- Regular employee training on latest practices.
- Encrypted data when transferring over network.
- Using strong passwords.
- Unique passwords for each account
- Enabling two-factor or multi-factor authentication.
- Avoid accessing email over unsecured Wi-Fi networks.
- Continuous monitoring and
- Updating the email security, policies and tools

These are some of the steps an organization can follow to adapt to evolving threats on email.

Countermeasures for Phishing attack

Anti-phishing solutions

Countermeasures against phishing attacks include deploying advanced anti-phishing solutions that can identify and block phishing attempts. This may involve the use of SPAM filters that detect malicious emails, blank senders, or virus-laden messages.

Continuous learning and adaptation to new phishing techniques are critical, as phishing methods are constantly evolving. Additionally, games and educational tools like Anti-Phishing Phil have shown effectiveness in improving users' ability to identify phishing web pages. Implementing such interactive and engaging training methods can significantly enhance users' skills in recognizing phishing attempts

Organization need to be careful about what information is shared online or made publicly available. The suspicious emails should never be accessed to click on links or open attachments. The mails can be treated has suspicious due to many factors. They are tools available in the market to filter them using Machine learning models.

Conclusion

The comprehensive analysis on email security and the nature of phishing attacks and its types gives the critical importance of implementing robust security measures in the

digital age. Email, it is a fundamental communication tool for both personal and professional areas, which presents a significant attack vector for attackers/hackers. The complexity and ubiquity of email systems make them more vulnerable to various threats, including attacks like phishing attacks that can lead to significant data breaches, financial losses, and compromise of sensitive information.

The key takeaways include the understanding that email security is not a one-time solution but a continuous process involving multilayer of defense. The best practices for email security, such as regular training for employees, using strong passwords coupled with multi-factor authentication, and keeping software updated, are essential in mitigating the risk of cyberattacks. We think user awareness training emerges as a particularly vital component, equipping individuals with the knowledge and skills to recognize and respond to potential threats effectively.

Phishing attacks, with their various forms like spear phishing, whaling, and clone phishing, highlight the need for constant vigilance and adaptation to evolving tactics used by attackers. The deployment of anti-phishing solutions, along with proactive educational and training initiatives, forms a critical part of a comprehensive defense strategy against these threats.

In conclusion, the battle against email-based cyber threats is an ongoing challenge that requires a dynamic and multi-faceted approach. Organizations and individuals must stay informed about the latest threats and continuously evolve their security practices. By combining technological solutions like pervious data, machine learning model along with informed user behavior, the risks posed by email security threats can be significantly reduced, leading to a safer and more secure digital environment.

Reference

[1] https://mailinabox.email/
Microsoft. 2023 Phishing Protection Report. Microsoft Phishing Protection Report. 2023. https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/submissions-users-report-message-add-in-configure?view=o365-worldwide

[2] Halouzka, K., Kozak, P., Buřita, L., & Matoulek, P. (2021, June). Personal cyber security in email communication. In *2021 International Conference on Military Technologies (ICMT)*.10.1109/ICMT52455.2021.9502740

[3] Nemavarkar, A., & Chakrawarti, R. K. (2015). A uniform approach for multilevel email security using image authentication, compression, OTP & cryptography. In 2015 International Conference on Computer, Communication and Control (IC4) (pp. 1-5). DOI: 10.1109/IC4.2015.7375661

[4] Li, T., Mehta, A., & Yang, P. (2017). Security Analysis of Email Systems. In 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud) (pp. 91-96). doi:10.1109/CSCloud.2017.20

[5] https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/why-email-security-is-important/#:~:text=Why%20Email%20Security%20is%20Important%3F,the%20lack%20of%20tight%20security
[6] https://www.itgovernance.eu/blog/en/the-5-biggest-phishing-scams-of-all-time
[7] https://us.norton.com/blog/online-scams/types-of-phishing#:~:text=,twin%20phishing%20Search%20engine%20phishing