PHISHING

H A D J A L I B O I R E

https://github.com/571LL01

hadjaliboire

OVERVIEW

01. INTRODUCTION

Phishing is a fraudulent technique designed to lure Internet users into disclosing personal (access accounts, passwords, etc.) and/or banking data by pretending to be a trusted third party.

Attackers' objective: Pretend to be a trusted third party in order to harvest personal information.

Consequences: data theft, identity theft, major financial losses.

02. TYPES OF PHISHING ATTACKS

There are many ways for cybercriminals to execute phishing attacks, but we're going to focus on the 6 most feared.

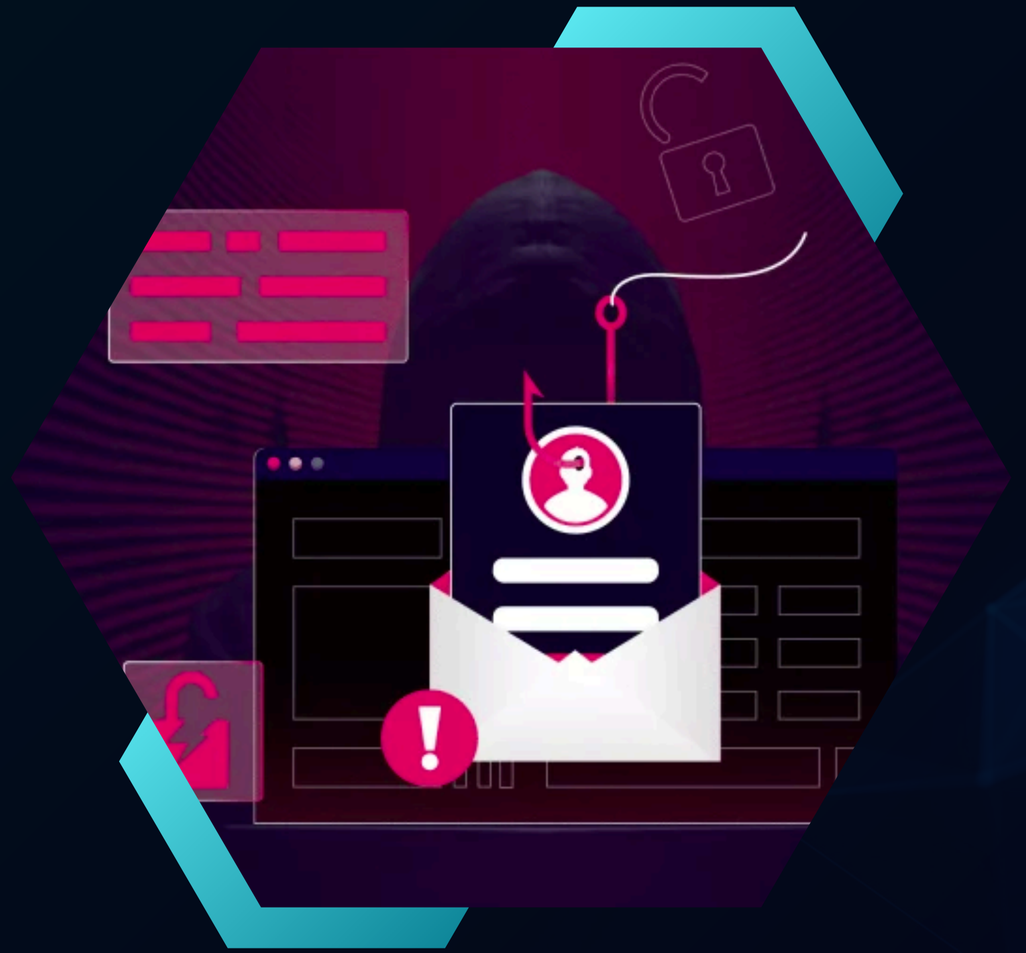
02. TYPES OF PHISHING ATTACKS

02. TYPES OF PHISHING ATTACKS

EMAIL PHISHING

Cybercriminals send fraudulent emails imitating legitimate companies or institutions to trick victims into clicking on malicious links or providing sensitive information.

Example : A fake bank email requesting account verification.



02. TYPES OF PHISHING ATTACKS

SPEAR PHISHING

More targeted attack, aimed at a specific person or organization. Messages are often personalized with real information to increase the credibility and success of the attack.

Example : Email targeting an employee with specific company details.

02. TYPES OF PHISHING ATTACKS

SMISHING

Phishing via SMS or text messages. Attackers send messages containing links or call-back numbers to steal personal or financial information.

Example : An SMS claiming you've won a prize and asking you to click on a link.

02. TYPES OF PHISHING ATTACKS

VISHING

Vishing, or voice phishing, is a type of phishing attack where scammers use phone calls to trick individuals into revealing personal information, such as passwords or credit card numbers, by pretending to be a legitimate entity.

Example : A telephone conversation in which the attacker poses as a bank officer.

02. TYPES OF PHISHING ATTACKS

WHALING

A whaling attack is a sophisticated type of phishing attack specifically aimed at high-profile individuals within an organization, such as executives or senior management.

Example : Fraudulent email sent to the CEO of a company with an urgent request.

02. TYPES OF PHISHING ATTACKS

CLONE PHISHING

Attackers duplicate a legitimate email, but replace the links or attachments with malicious versions, then resend the email claiming it is an “update” or “patch email”.

Example : A hacker clones a legitimate software update request e-mail sent by the IT department to an employee. The hacker modifies the link to redirect the employee to a malicious site. The employee, thinking the e-mail is genuine, clicks on the link, which may compromise his or her credentials or the organization's security.

03. DETECTION OF PHISHING ATTACKS

Suspicious e-mail addresses or numbers

There are two types of suspicious sender addresses: misspelled or slightly altered domains, such as “support@bankl.com” instead of “support@bank.com”, are red flags as they are often used to impersonate people or brands, but you should also be wary of generic e-mail addresses from Gmail, Yahoo and Outlook, especially if they don't match who they claim to be.

Spelling and grammar errors

Email phishing and smishing often contain spelling and grammatical errors, which can be a sign of attack. Despite the use of AI and proofreaders, these errors persist because attackers don't always master their victims' language.This criterion can also apply to Vishing, where the language or tone of the call may appear unusual.

03. DETECTION OF PHISHING ATTACKS

Pressure mechanisms: Urgency and threats

Phishing attacks exploit pressure mechanisms, such as urgency or threats, to provoke a rapid emotional response. They use tactics such as “Your account will be suspended” to incite immediate action, a common technique in spear phishing, whaling and vishing attacks.

Suspicious links and attachments

Before clicking, check links by hovering the mouse over them to see if the URL is legitimate. Unusual attachments, especially with unknown extensions, are also red flags.This detection technique applies particularly to Clone Phishing, where links or files are modified.

03. DETECTION OF PHISHING ATTACKS

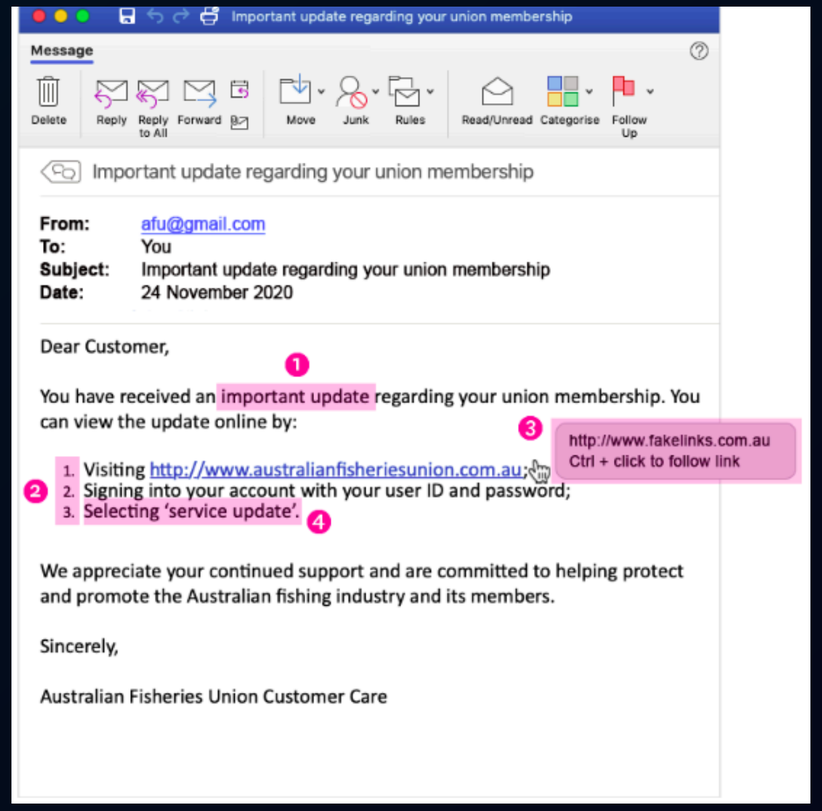
Example

1. It is unexpected or creates a sense of urgency for you to do something.

2. It asks you to click on a link, open an attachment or refers you to a website that asks you to enter your information.

3. The link suggests that it will take you to a legitimate website, but when you hover your mouse over it, it indicates that it's actually another website.

4. It asks for information that the real or legitimate sender doesn't necessarily need to know.



04. PREVENTION OF PHISHING ATTACKS

Training and raising awareness among employees and users

Phishing awareness training should combine theory and practice, with simulations to help employees detect and report phishing attempts. It should reinforce detection reflexes, particularly in the face of pressure mechanisms, and teach reporting procedures to alert potential threats. Hands-on learning is essential for changing behavior in the face of social engineering attacks.

Password management and multi-factor authentication (MFA)

To protect against phishing, two key practices are recommended: using a password manager to create and store unique passwords, and enabling multi-factor authentication (MFA) to add an extra layer of security. Together, these measures strengthen account protection and reduce the risk of compromise.

04. PREVENTION OF PHISHING ATTACKS

Use spam filters and security software :

Activate a phishing filter in your inbox and use up-to-date security software to block fraudulent e-mails before they reach your inbox.
This helps prevent mainly Email Phishing and Clone Phishing attacks.

Do not click on links or attachments

It is essential never to click on links or open attachments from suspicious e-mails or SMS messages. Always check the sender before acting, even if the e-mail seems legitimate, as a crucial preventive measure against phishing attacks,

05. WHAT TO DO IN THE EVENT OF PHISHING

- If you think you've received a phishing e-mail, here are the steps to follow. You can also share this process with your employees, if you don't already have one in place.
- Don't interact with the phishing e-mail: don't reply, click on links or execute attachments.
- Report the phishing attempt to the appropriate parties, using a report button if applicable.
- If you have interacted with the phishing e-mail and its contents, explain what you have done to the parties concerned so that they can trace and possibly remedy any leaks or vulnerabilities introduced.

06. PHISHING DETECTION TOOLS

Microsoft Defender for Office 365, Proofpoint and Barracuda Essentials are widely used email security solutions that include phishing detection features.

URLScan.io and VirusTotal allow users to inspect suspicious links without visiting them directly.

Avast Online Security , Bitdefender TrafficLight and Norton Safe Web, they analyze web pages in real time and warn users of potential phishing risks.

REFERENCES

- https://www.fortinet.com/resources/cyberglossary/types-of-phishing-attacks
- https://www.strongboxit.com/what-are-the-types-of-phishing-attacks/
- https://www.ba-info.fr/spear-phishing-comprendre-et-prevenir-ces-attaques-devastatrices/
- https://arsen.co/en/resources/phishing
- https://arsen.co/en/blog/phishing-detection

THANK YOU