Introduction

Phishing attacks

Ashari Binte Ashraf
Cyber Security intern at Code Alpha

What is phishing

Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine.

WHAT IS PHISHING

Deceptive phishing is a popular cybercrime, as it's far easier to trick someone into clicking on a malicious link in a seemingly legitimate phishing email than it is to break through a computer's defences. Learning more about phishing is important to help users detect and prevent it.

How does phishing work ?

Attacker

Attacker Sends an email to the victim

Victim

Victim Clicks on the email and goes to the phihing website

Phishing Website

Attacker Collects Victrim's credentials

Attacker Usera Victim's credentials to access a website

Logitimate Website

TYPES OF PHISHING ATTACK

- Spear phishing attack
- Whaling attacks
- Pharming
- Clone phishing attacks
- Evil twin attacks
- Voice phishing
- SMS phishing
- Calendar phishing
- Page hijack attacks

RECOGNIZING PHISHING EMAILS, WEBSITES AND SOCIAL ENGINEERING TACTICS ?

- Urgent action demands.
- Poor grammar and spelling errors.
- An unfamiliar greeting or salutation.
- Requests for login credentials, payment information or sensitive data.
- Offers that are too good to be true.
- Suspicious or unsolicited attachments.
- Inconsistencies in email addresses, links and domain names.

RECOGNIZING PHISHING EMAILS

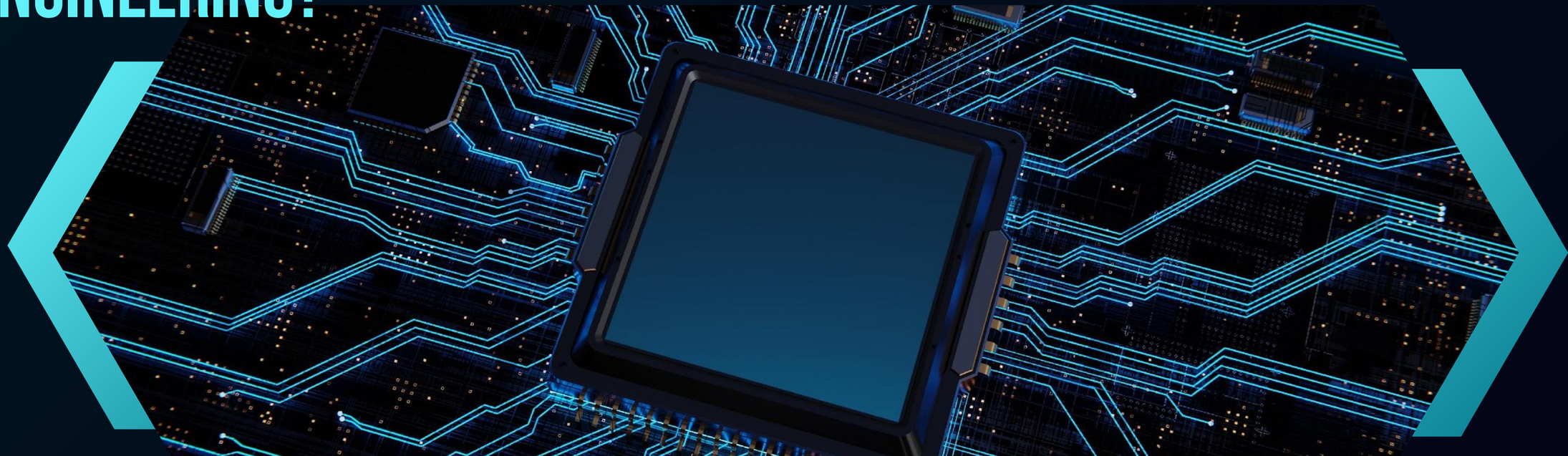
- The email is sent from a public domain.
- The email requests your sensitive information.
- The email has terrible grammar.
- The email has a suspicious attachment.
- The message has made you panic.
- The email says you have won a lottery.
- The email is from a government agency.

WHAT TO DO IF YOU THINK YOU ARE A VICTIM?

- Change Passwords
- Report the Incident
- Scan for Malware
- Contact Financial Institutions
- Monitor Accounts
- Educate Others
- Educate Others

HOW TO PROTECT YOURSELF AGAINST PHISHING AND SOCIAL ENGINEERING?

1. **Educate Yourself and Others:** Stay informed about the latest phishing techniques and social engineering tactics. Educate colleagues, friends, and family members to enhance collective awareness.
2. **Use Multi-Factor Authentication (MFA):** Enable MFA whenever possible. This adds an extra layer of security, making it more difficult for attackers to gain unauthorized access.
3. **Implement Security Software:** Utilize reputable antivirus and anti-phishing software to detect and prevent malicious activities. Keep software and security systems updated regularly.
4. **Report Suspicious Activity:** If you encounter a potential phishing attempt, report it to the relevant authorities or IT support team. Quick reporting can help prevent others from falling victim to the same attack



GUIDELINES TO KEEP YOURSELF SAFE FROM PHISHING ATTACKS

- ❑ New phishing attack methods are developed all the time. Therefore, keep yourself informed about the latest ones.
- ❑ Do not click on a link in an email or instant message unless you are sure that it is genuine.
- ❑ Download an anti-phishing toolbar that will alert you every time you are about to enter a known phishing site.
- ❑ Keep your browser up-to-date and check your online accounts regularly for traces of phishing attempts.
- ❑ Use high-quality firewalls as a shield between you, your computer, and outside intruders to reduce the odds of phishing attempts.
- ❑ Be cautious of pop-up windows as they often redirect to malicious websites. Do not click on the "cancel" button, as those buttons often lead to phishing sites. Click the tiny 'x' in the upper corner of the browser instead.
- ❑ Get into the habit of regularly changing your password to lock out potential attackers.
- ❑ Do not share your personal information anywhere over the Internet.
- ❑ Train your employees to adopt the best anti-phishing practices.

IDENTIFYING PHISHING EMAILS

01

Dodgy Greetings

Phishing emails often use generic greetings like 'Dear user' instead of addressing the recipient by their name or business title.

02

Overpayment Scam

Some phishing emails may claim that the user has been overpaid and needs to send money back to a fake account.

03

Suspended Account

Phishing attempts may claim that the user's account will be suspended if they do not take immediate action.

04

Attachments

PayPal does not send downloadable attachments, so if an email includes an attachment, it is likely a phishing attempt.

05

Verify Account

If a seller receives a suspicious email, they should check their payment page in a separate browser tab or window to see if their account has any alerts.

Preventing Phishing Scams

To prevent phishing scams, sellers should take the following precautions:

- ✔ Open the payment page in a separate browser tab or window to check for account alerts.
- ✔ Do not download any attachments from suspicious emails.

PayPal encourages users to report any suspicious activity to help monitor and prevent phishing attempts. Staying vigilant and following security guidelines can help prevent users from falling victim to phishing scams.

WORK-RELATED PHISHING SCAMS

CEO Wire Transfer Scam

- Scammers impersonate the CEO or another high-level executive and send an urgent email to the finance department requesting a wire transfer.
- They often use the CEO's name, email signature, and even the company's logo to make the email appear legitimate.
- The email may claim that the transfer is for a confidential acquisition or urgent business matter, pressuring the recipient to act quickly without verifying the request.

Manager Phone Scam

- Malicious actors call employees, posing as their manager, CEO, or CFO, and request sensitive information or instruct them to perform certain actions.
- They may claim that there is an urgent issue that needs to be resolved, such as a security breach or a confidential project.
- The scammers use social engineering techniques to manipulate the employee into disclosing sensitive information or executing malicious tasks, such as downloading malware or sharing login credentials.

THANK YOU