PHISHING ATTACK

ABOUT:

- Phishing is a type of cyberattack where attackers try to trick individuals into revealing sensitive information, such as usernames, passwords, and credit card details, by impersonating legitimate entities.
- Recognizing and reporting phishing attacks is crucial because they can lead to significant financial losses, identity theft, and data breaches.
- Training goals related to phishing awareness include improving the ability to identify phishing attempts, understanding the techniques used by attackers, and knowing how to respond appropriately to protect oneself and the organization.

WHAT IS PHISHING ATTACK?

Phishing is a form of social engineering where attackers use deception to manipulate individuals into taking actions that compromise their security.

Types of Phishing Attacks:

- Email Phishing: Deceptive emails designed to trick recipients into revealing sensitive information or clicking malicious links.
- SMS Phishing (Smishing): Phishing attacks conducted through text messages.
- Voice Phishing (Vishing): Phishing attacks carried out over the phone.
- Spear Phishing: Highly targeted phishing attacks aimed at specific individuals or organizations.

RECOGNIZATION PHISHINNG ATTACK

Common Red Flags:

- Misspelled Domains: Attackers often create email addresses that closely resemble legitimate ones but contain subtle misspellings (e.g., "amaz0n.com" instead of "amazon.com").
- Urgent or Threatening Language: Phishing emails frequently use language that creates a sense of urgency or fear, prompting recipients to act without thinking (e.g., "Your account will be suspended if you don't verify your information within 24 hours").
- Unusual Attachments or Links: Be cautious of unsolicited emails with attachments or links that seem out of the ordinary or unexpected.
- Poor Grammar or Formatting: Many phishing emails contain grammatical errors, spelling mistakes, or a layout that looks unprofessional, unlike legitimate emails from reputable organizations.
- Generic Greetings: Legitimate businesses usually address recipients by name. Phishing emails often use generic greetings like "Dear Customer" or "Dear User".
- Requests for Personal Information: Never share sensitive information like passwords, credit card details, or social security numbers via email.
- Suspicious Sender Address: Always verify the sender's email address carefully. Phishing emails may use addresses that are similar to legitimate ones but with slight variations.

Visual Example:

- A real email from a microsoft, for instance, would likely have:

A professional, clear layout. A sender address that matches the bank's domain name (e.g., support@microsoft.co.uk).
A personalized greeting using the recipient's name.
No urgent or threatening language.

- A phishing email mimicking the microsoft might have:

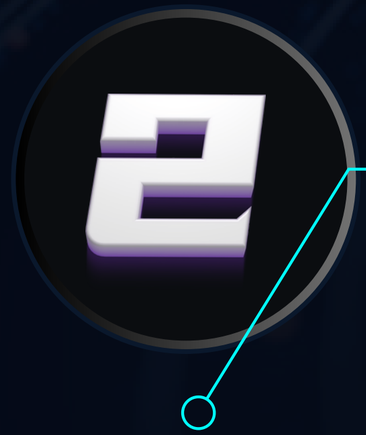
A casual message, unlike message .
A sense of urgency with a threat of account closure.
A suspicious link asking for personal information.

DECODING FAKE WEBSITES:

What to Look For in the URL’s

Poor Quality and Grammar:

Fake websites often look hastily put together.



Requests for Excessive Information:

If a website asks for an unusual amount of personal information upfront, or data that doesn't seem relevant to its purpose, that's a huge red flag.

SOCIAL ENGINEERING TACTICS

Common Social Engineering Tactics:

- Impersonation:

Threat actors pretend to be someone they are not, such as a high-level executive, a trusted colleague, or a customer service representative, to gain access to systems or information.

- Pretexting:

Creating a fabricated scenario to trick victims into revealing information or performing an action.

- Phishing:

Sending deceptive emails, messages, or other communications designed to trick users into clicking malicious links, opening infected attachments, or revealing sensitive information.

- Baiting:

Offering something enticing (e.g., a free download, a giveaway) to lure victims into a trap, potentially leading to malware installation or credential theft.

- Scareware:

Using fear and intimidation to pressure victims into taking immediate action, such as purchasing fake security software or revealing personal data.

- Quid pro quo:

Offering a service or assistance in exchange for something, such as login credentials or access to systems.

- Honeytraps:

Building a fake online relationship to gain trust and exploit the victim for financial gain or access to sensitive information.

BEST PRACTICES AND PREVENTION TIPS

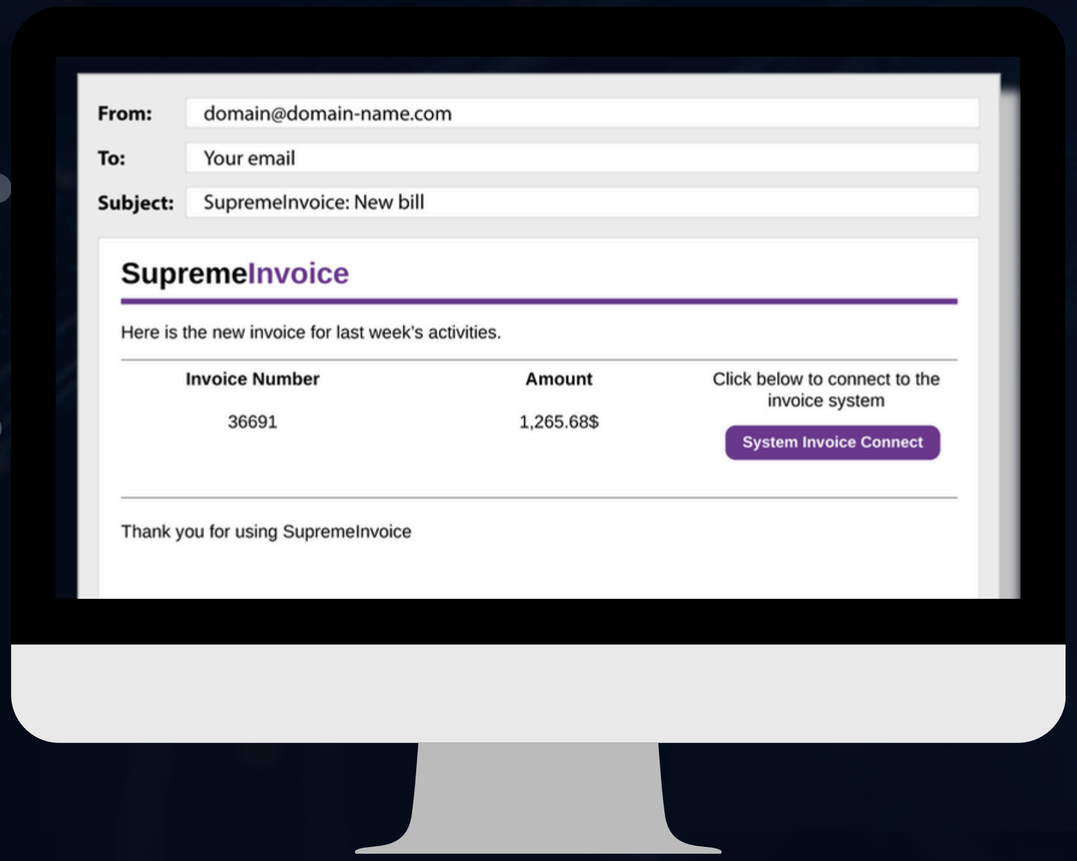
For Individuals:

- Be cautious of unsolicited emails: Don't trust messages that create a sense of urgency or demand immediate action.
- Verify the sender: If you're unsure about an email's authenticity, contact the sender through a verified channel (e.g., a known phone number or website).
- Avoid clicking suspicious links: Instead, manually type the website address into your browser or use a search engine to find the correct site.
- Don't open attachments from unknown senders: Attachments can contain malware.
- Keep software and operating systems updated: This includes your web browser, email client, and operating system.
- Use strong passwords: Create complex passwords that include a mix of uppercase and lowercase letters, numbers, and symbols.
- Enable multi-factor authentication: This adds an extra layer of security by requiring a second verification method in addition to your password.
- Be mindful of personal information: Never share sensitive information like passwords, credit card details, or social security numbers in emails.
- Use anti-phishing tools: Install and update anti-spam, anti-phishing, and anti-malware software.
- Report suspicious emails: Report them to your email provider and relevant authorities.

For Organizations:

- Provide phishing awareness training: Educate employees on how to identify and avoid phishing attacks.
- Use spam filters and secure email gateways: These tools can help block or filter out phishing emails.
- Enable multi-factor authentication for all accounts: This can help prevent unauthorized access even if a password is compromised.
- Implement email authentication protocols like SPF, DKIM, and DMARC: These protocols help verify the authenticity of email senders.
- Use endpoint protection solutions: These tools can help prevent, detect, and remove malware that enters the system through phishing attacks.
- Keep IT assets and systems updated: This helps minimize vulnerabilities that attackers can exploit.
- Conduct regular security audits: This can help identify and address any weaknesses in your security posture.
- Report phishing attempts: Report any suspicious activity to the relevant authorities.

REAL-WORLD EXAMPLES



A cyber criminal creates a fake Google Docs login page and then sends a phishing email to trick someone into logging into the fake website. The email might read something like,

“We’ve updated our login credential policy. Please confirm your account by logging into Google Docs.”

The sender’s email address is a fake Google email address:

accountupdate@google.org.com.

INTERACTIVE QUIZ

- What is phishing?

(a) A type of computer virus.
(b) A way to boost website traffic.
(c) An attempt to obtain sensitive information by disguising as a trustworthy entity.
(d) A type of encryption.

- Which of the following is NOT a common tactic used in phishing attacks?

(a) Sending emails with urgent requests.
(b) Impersonating trusted organizations.
(c) Providing clear and transparent communication.
(d) Using malicious links or attachments.

- What is spear phishing?

(a) A general email sent to a large number of people.
(b) A targeted attack aimed at specific individuals or organizations.
(c) A type of malware that steals data.
(d) A way to improve website security.

- What is the primary goal of a phishing attack?

(a) To improve website performance.
(b) To gather user feedback.
(c) To steal sensitive information or credentials.
(d) To promote a brand.

- Which of the following is a sign of a potential phishing attack?

(a) The email is addressed to you by name.
(b) The email contains a clear and concise message.
(c) The email asks you to verify your account information via a link.
(d) The email is from a known and trusted source.

SUMMARY

Do:

- check the sender's email address carefully for any inconsistencies.
- hover over links to see the actual destination URL before clicking.
- keep your software and security tools updated.
- report phishing attempts to the appropriate authorities according to CISA.

Don't:

- click on links or open attachments in suspicious emails.
- be pressured by urgent or threatening language in emails.
- trust emails with poor grammar or spelling errors.
- reply to suspicious emails.

Reference :

www.proofpoint.com

THANK YOU.