PHISHING ATTACKS

Recognize, Avoid, and Report Phishing Attempts

Done By: Judy Ammar Hallak

Student Id: CA/S1/5866

Date: September 16 2024

WHAT IS A PHISHING ATTACK?

Phishing is a type of cyberattack that uses fraudulent emails, text messages, phone calls or websites to trick people into sharing sensitive data (e.g., passwords, credit card numbers, personal data, downloading malware or otherwise exposing themselves to cybercrime. It's based on the word fishing, which works on the concept of baits.

HOW DO PHISHING ATTACKS WORK

Step-by-Step Process:

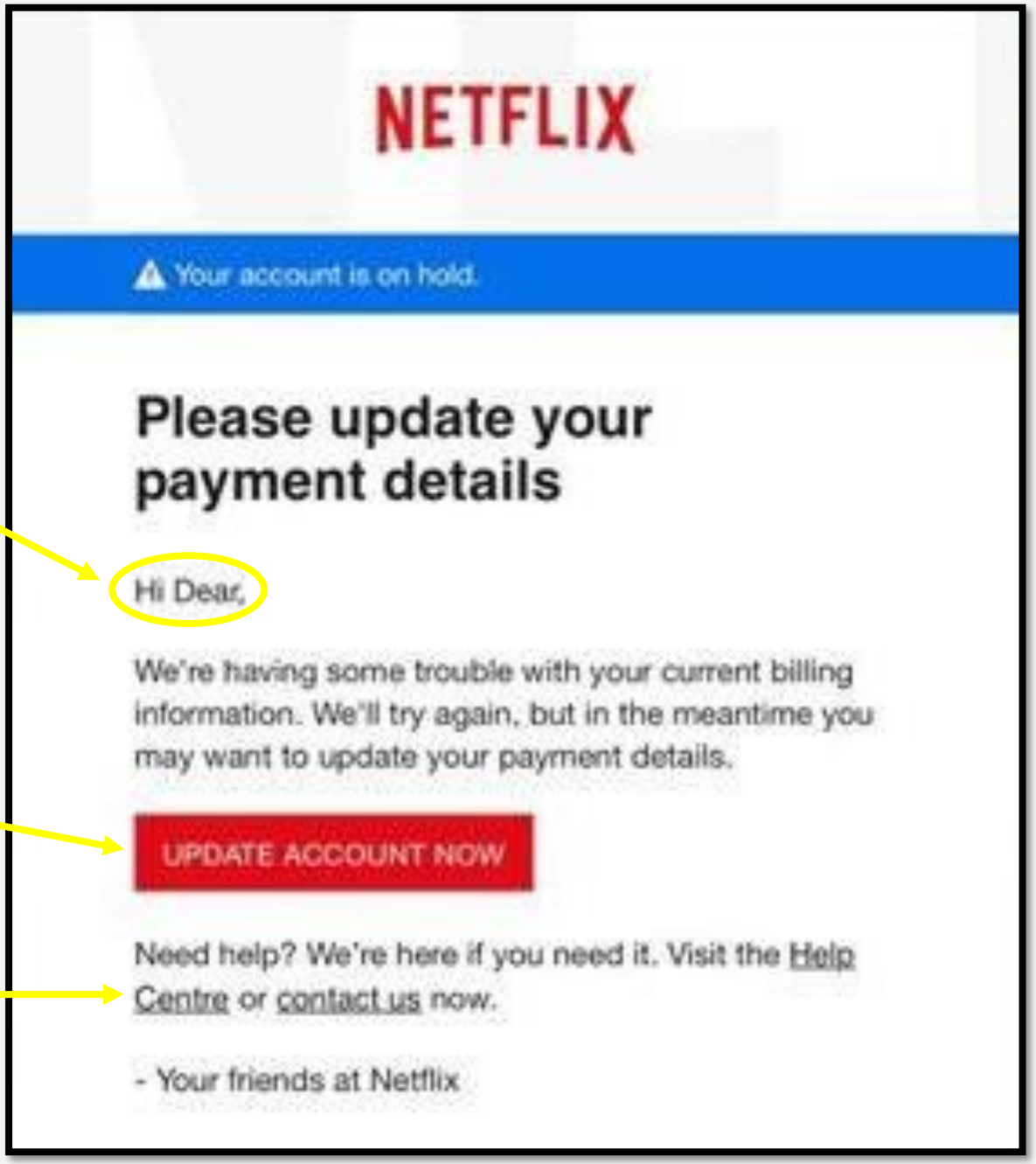
1. **Bait:** The attacker sends a fraudulent message (email, SMS, etc.) to the target.
2. **Deception:** The message appears to be from a trusted entity (e.g., bank, service provider).
3. **Lure:** The message prompts the recipient to take an action, such as clicking a link or opening an attachment.
4. **The Trap:** The link leads to a fake website (which are designed to look more authentic than possible) or installs malware.
5. **The Outcome:** The victim provides sensitive information, which the attacker exploits.

TYPES OF PHISHING ATTACKS

- **Deceptive Phishing:** fraudulent attempt to obtain sensitive information by impersonating a legitimate entity through fake emails or messages.
- **Email Phishing:** Fraudulent emails mimicking legitimate companies.
- **Spear Phishing:** Targeted attacks on specific individuals using personalized information.
- **Vishing (Voice Phishing):** Phone calls pretending to be from trusted sources.
- **Smishing (SMS Phishing):** Phishing attacks through text messages.
- **Whaling:** is a phishing attack that targets a senior executive. These individuals often have deep access to sensitive areas of the network, so a successful attack can result in access to valuable info.
- **Pharming:** the victim gets malicious code installed on their computer. This code then sends the victim to a fake website that resembles the original counterpart designed to gather their login credentials.

SIGNS OF PHISHING EMAILS

- **Suspicious Sender:** Look at the email address carefully; it may have slight misspellings.
- **Generic Greetings:** "Dear Customer" instead of using your name.
- **Urgency or Threats:** Messages claiming urgent action is required or you'll face penalties.
- **Request for Personal Information:** Legitimate organizations never ask for sensitive information via email.
- **Links or Attachments:** Hover over links to check the URL, or avoid downloading unexpected attachments.



RECOGNIZING PHISHING WEBSITES

1. **URL Check:** Verify if the URL starts with "https://" and look for security certificates (padlock icon).
2. **Look for Misspellings:** Phishing sites often have small typos or poor grammar.
3. **Design Quality:** Poorly designed or misaligned logos, images, and layout can be red flags.
4. **Requests for Personal Info:** Be cautious if the site asks for personal or financial information without a valid reason.
5. **Check Domain Name:** Fraudulent websites often use similar-looking domain names (e.g., facebok.com instead of facebook.com).

SOCIAL ENGINEERING TACTICS

Pretexting

Attackers create a fabricated scenario to trick victims into providing information.

Quid Pro Quo

Promising a service or benefit in exchange for information.

Baiting

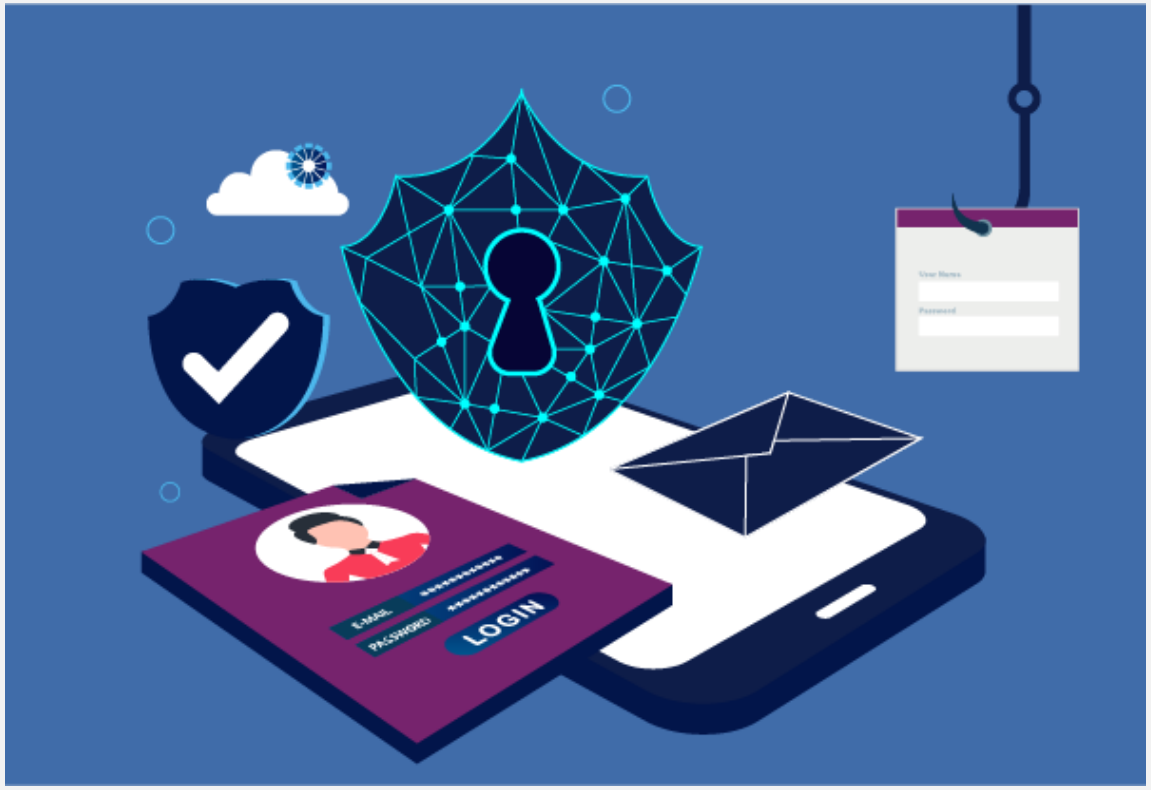
Offering something enticing to the victim, such as a free download, to get them to take action.

Tailgating, Piggybacking

Physically following someone into a restricted area to gain unauthorized access.

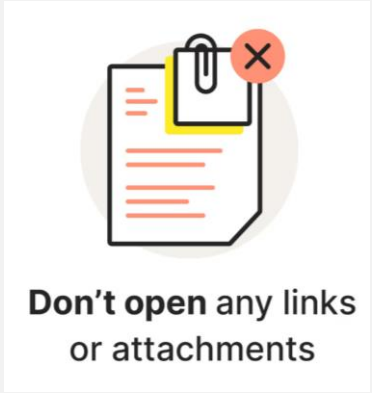
HOW TO AVOID PHISHING ATTACKS

- **Verify Sources:** Always verify the sender's email or website URL.
- **Hover Before Clicking:** Hover over links to preview URLs.
- **Don't Share Personal Information:** Never provide sensitive information via email, text, or phone unless you're certain of the recipient's legitimacy.
- **Use Strong Security Measures:** Enable multi-factor authentication (MFA) and use strong, unique passwords.
- **Keep Software Updated:** Regularly update your software, especially security patches.
- **Be Wary of Attachments:** Avoid opening unexpected or suspicious attachments.

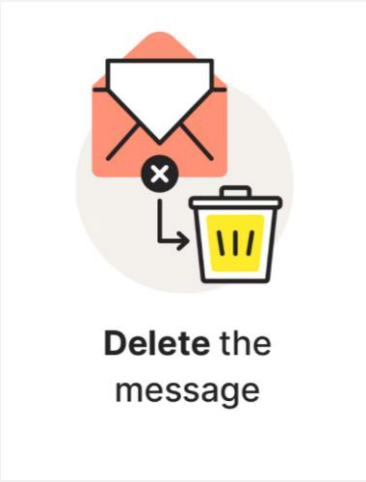


WHAT TO DO IF YOU RECEIVE A PHISHING EMAIL

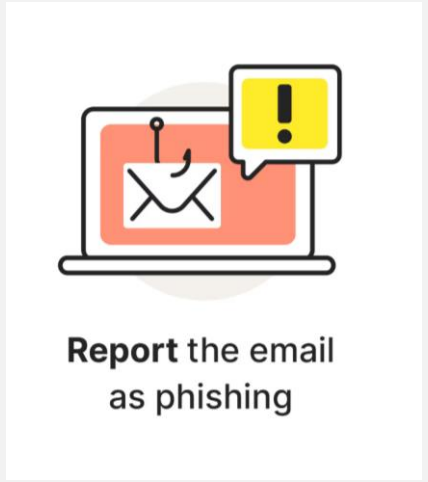
Avoid engaging with the sender.



This could download malware or direct you to a malicious website.



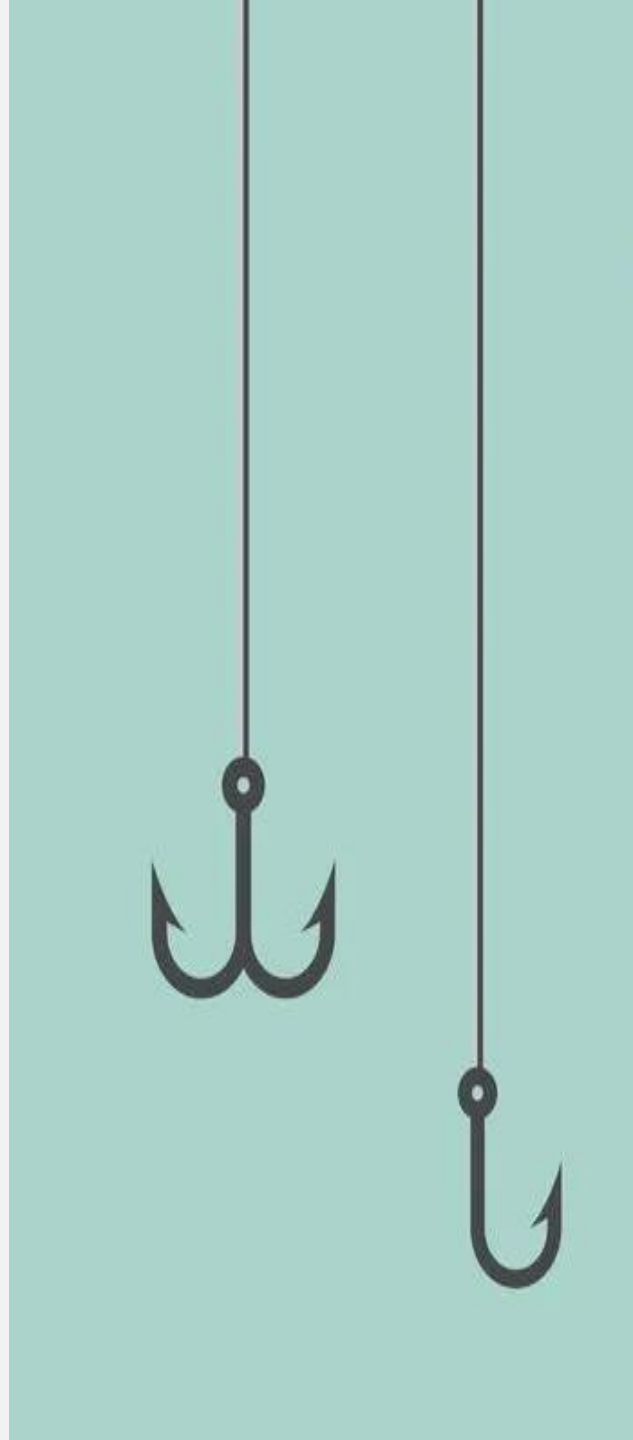
After reporting, remove it from your inbox.



Report phishing emails to your IT department or the appropriate authority (e.g., your email provider or anti-phishing organizations).

WHAT TO DO IF YOU'VE BEEN PHISHED

- **Change Your Passwords:** Immediately change any passwords that may have been compromised.
- **Contact Financial Institutions:** Inform your bank if financial information has been compromised.
- **Monitor Your Accounts:** Keep an eye on your accounts for any suspicious activity.
- **Report the Incident:** Report the phishing attempt to authorities such as the Federal Trade Commission (FTC) or Anti-Phishing Working Group (APWG)

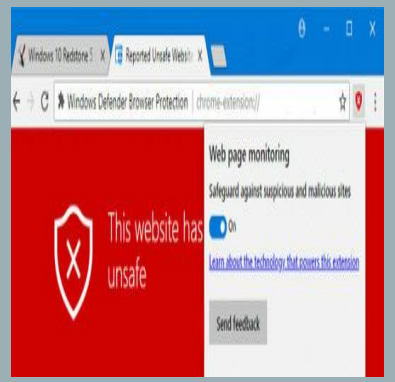


TOOLS TO HELP DETECT PHISHING

Email Filtering Software: Filters that identify and block phishing emails.

Browser Security Settings: Enable security features in your web browser to block malicious sites

Security Awareness Training: Regular training for employees to recognize phishing threats



Anti-Phishing Toolbars and Plugins: Many browsers offer plugins to alert users about phishing sites.

EXAMPLE OF A PHISHING ATTACK

An email from PayPal arrives telling the victim that their account has been compromised and will be deactivated unless they confirm their credit card details. The link in the phishing email takes the victim to a fake PayPal website, and the stolen credit card information is used to commit further crimes.

CONCLUSION

- **Stay Vigilant:** Phishing attacks are constantly evolving, so it's important to stay informed about the latest tactics.
- **Report Suspicious Activity:** If you suspect phishing, don't hesitate to report it.
- **Be Proactive:** Implement preventive measures and educate others to avoid becoming victims of phishing attacks.

RESOURCES

- FTC - How to Recognize and Avoid Phishing Scams
- APWG - Anti-Phishing Working Group
- Microsoft - Phishing Prevention and Tips
- US-CERT - Avoiding Phishing Attacks
- StaySafeOnline - Phishing

THANK YOU!