TASK 2

PHISHING AWARENESS TRAINING

Presentation about phishing attacks and to educate others about recognizing and avoiding phishing emails,websites, and social engineering tactics

What is phishing?

- Phishing is a common type of cyber attack that targets individuals through email, text messages, phone calls, and other forms of communication. A phishing attack aims to trick the recipient into falling for the attacker's desired action, such as revealing financial information, system login credentials, or other sensitive information.
- The information is then used to access important accounts and can result in identity theft and financial loss.
- The goal is to steal sensitive data like credit card and login information, or to install malware on the victim's machine. Phishing is a common type of cyber attack that everyone should learn about in order to protect themselves.

TYPES OF PHISHING

- Email phishing
- Spear phishing
- Whaling
- Smishing and vishing
- Angler phishing

INFORMATION ABOUT PHISHING

1. Email phishing

- Most phishing attacks are sent by email. The crook will register a fake domain that mimics a genuine organisation and sends thousands of generic requests.
- The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.
- In other cases, the fraudsters create a unique domain that includes the legitimate organisation's name in the URL. The example below is sent from 'olivia@amazonsupport.com'.
- The recipient might see the word 'Amazon' in the sender's address

  and assume that it was a genuine email.
- There are many ways to spot a phishing email, but as a general rule

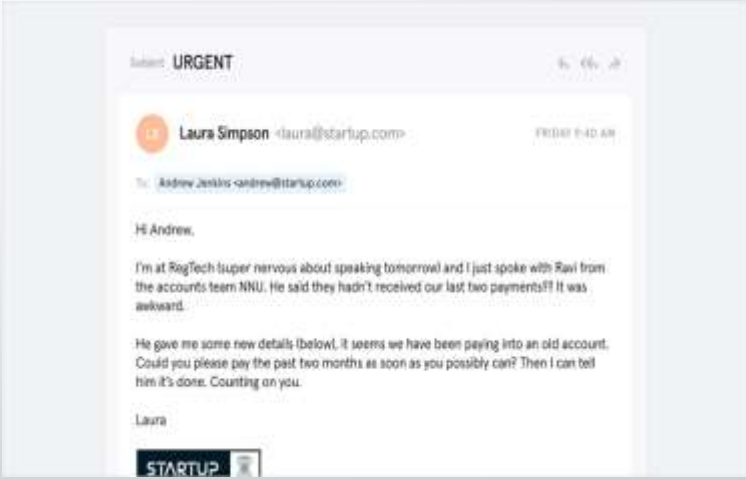
  you should always check the email address of a message that asks

  you to click a link or download an attachment.

2. Spear phishing

- There are two other, more sophisticated, types of phishing involving email.
- The first, spear phishing, describes malicious emails sent to a specific person. Criminals who do this will already have some or all of the following information about the victim:
- Their name.
- Place of employment.
- Job title.
- Email address; and
- Specific information about their job role.
- The fraudster has the wherewithal to address the individual by
- name knows that their job role involves making

  bank transfers on behalf of the company.
- The informality of the email also suggests that the sender is a native English speaker and creates the sense that this is a real message rather than a template.

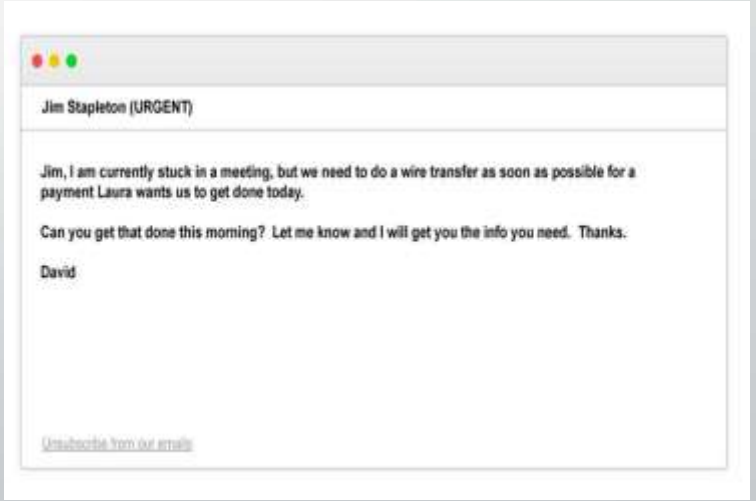


3. Whaling

- Whaling attacks are even more targeted, taking aim at senior executives. Although the end goal

of whaling is the same as any other kind of phishing attack, the technique tends to be a lot subtler.

- Tricks such as fake links and malicious URLs aren't helpful in this instance, as criminals are attempting to imitate senior staff.
- Whaling emails also commonly use the pretext of a busy CEO who wants an employee to do them a favour.
- Emails such as the above might not be as sophisticated as spear phishing emails, but they play on employees' willingness to follow instructions from their boss.



4. Smishing and vishing

- With both smishing and vishing, telephones replace emails as the method of communication.

- Smishing involves criminals sending text messages (the content of which is much the same as with email phishing), and vishing involves a telephone conversation.
- One of the most common smishing pretexts are messages supposedly from your bank alerting you to suspicious activity.
- In this example, the message suggests that you have been the victim of fraud and tells you to follow a link to prevent further damage. However, the link directs the recipient to a website controlled by the fraudster and designed to capture your banking details.
- **5. Angler phishing**
- A relatively new attack vector, social media offers several ways for criminals to trick people. Fake URLs; cloned websites, posts, and tweets; and instant messaging (which is essentially the same as smishing) can all be used to persuade people to divulge sensitive information or download malware.
- Alternatively, criminals can use the data that people willingly post on social media to create highly targeted attacks.

HOW TO PREVENT PHISHING

- Never provide your personal information in response to an unsolicited request.
- Never provide your password over the phone or in response to an unsolicited Internet request.
- Protect your computer by using security software. Set the software to update automatically so it will deal with any new security threats.
- Protect your accounts by using multi-factor authentication
- Protect your data by backing it up back up data on your computer to an external hard drive or in the cloud.
- Install an Anti-Phishing Toolbar, Use Firewalls , Use Antivirus Software Be Wary of Pop-Ups, Never Give Out Personal Information .