Phishing

Phishing is a type of cyberattack where attackers disguise themselves as trustworthy entities to trick individuals into providing sensitive information, such as usernames, passwords, credit card numbers, and other personal details. These attacks are typically carried out via email, social media, or other communication channels, where the attacker creates a sense of urgency or legitimacy to prompt the recipient to act.

Alt text: *Phishing mail in the inbox*

Key Characteristics of Phishing

1. **Impersonation:**
   - Attackers often pretend to be from reputable organisations such as banks, email providers, or online services.

   Example: An email claiming to be from your bank asking you to verify your account details.

2. **Urgent or Threatening Language:**
   - Phishing messages frequently create a sense of urgency or fear to compel quick action.

   Example: "Your account has been compromised. Verify your identity immediately to avoid suspension."

3. **Deceptive Links:**
   - Phishing emails include links that look legitimate but direct users to fake websites designed to steal information.

   Example: A link saying "Click here to verify" that leads to a phishing site.

4. **Suspicious Attachments:**
   - Emails may contain attachments that, when opened, can install malware on the recipient's device.

   Example: An attachment named "Invoice.pdf" that is actually a malicious file.

5. **Requests for Personal Information:**
   - Legitimate organisations rarely ask for sensitive information via email.

   Example: An email asking for your social security number or password.

Common Types of Phishing

Phishing attacks come in various forms, each designed to deceive users into providing sensitive information such as usernames, passwords, credit card details, or other personal information. Here are some common types:

a. Email Phishing
b. Spear Phishing
c. Clone Phishing
d. Whaling

a. Email Phishing:
   - The most common form, where attackers send mass emails to many potential victims.

   Example: An email from "PayPal" asking you to confirm your account details.

b. Spear Phishing:
   - This targeted form of phishing aimed at a specific individual or organisation, often personalised to increase its credibility.

   Example: An email addressed specifically to you, mentioning details relevant to your job or personal life.

c. **Clone Phishing:**

- Attackers create a nearly identical copy of a legitimate email previously sent, but with malicious links or attachments.

Example: Re-sending a real email from your bank but with a harmful link.

d. **Whaling:**

- This type of phishing targets high-profile individuals like executives or key decision-makers within an organisation.

Example: An email **purporting** to be from the CEO requesting sensitive company information.

Example of a Phishing Email

Subject: Urgent: Verify Your Account Information From: support@amaz0n.com (Note the misspelling of "amazon") Message: Dear Customer, we have detected unusual activity in your account. To secure your account, please verify your information by clicking the link below: [Verify Now] (phishing-link.com) Thank you, Amazon Support Team Protecting Against Phishing

1. **Verify the Sender:**

- Check the sender's email address for slight misspellings or unusual domains.

Example: An email from "support@amaz0n.com" instead of "support@amazon.com".

2. **Hover Over Links:**

- Hover over links to see the actual URL before clicking.

Example: Hovering reveals "phishing-link.com" instead of "amazon.com".

3. **Look for Personalisation:**

- Legitimate emails from reputable organisations often include your name or other personal details.

Example: "Dear John" instead of "Dear Customer".

4. **Beware of Attachments:**
   - Avoid opening attachments from unknown or suspicious sources.

   Example: An unexpected attachment named "Invoice.zip".

5. **Report Suspicious Emails:**
   - Most email providers have options to report phishing emails.

   Example: Use the "Report Phishing" button in Gmail.

Understanding phishing is crucial for protecting yourself and your information online. By recognising the signs and following best practices, you can reduce the risk of falling victim to these attacks.

Tools and Resources

Tools and resources are available to help individuals and organisations combat phishing threats. These include:

a. **Email Headers:** Learn how to view email headers to analyse the sender's IP address and email path. Specific guides are provided for Gmail and Outlook email header analysis, empowering users to:
   - Gain a deeper understanding of how emails travel.
   - Troubleshoot email delivery problems.
   - Verify the authenticity of emails.
   - Examine the security measures used during email transmission.

b. **Online Phishing Awareness Training**: This likely refers to non-profit organisations or resources focused on phishing education and awareness, such as:
   - Phishing.org
   - KnowBe4 Phishing

By following the steps on these platforms, you can effectively identify and analyse phishing emails and recognise suspicious elements.