1. What is phishing?

Phishing is like a digital con artist "fishing" for your private information. They send fake emails or messages that pretend to be from a company you trust (like your bank, Google, or PayPal) to trick you into giving them your passwords, credit card numbers, or other personal details.

2. How to identify a phishing email?

Look for these simple red flags:

- **The Sender's Address is Fishy:** The email might say it's from "PayPal," but the actual email address is something weird like support@pay-pal-security-alert.net.
- **The Link is a Lie:** The email might have a button that says "Click here to log in," but if you hover your mouse over it, the actual link goes to a strange website, not the real one.
- **It Tries to Scare You:** It uses urgent or threatening language like "Your account will be suspended!" or "Suspicious activity detected!" to make you panic and click without thinking.
- **It Has Mistakes:** It often contains bad grammar or spelling mistakes. Big companies usually don't make those errors.
- **It Asks for Personal Info:** Legitimate companies will almost never email you to ask for your password or credit card number directly.

3. What is email spoofing?

Email spoofing is **faking the sender's address**. It’s like writing a fake return address on a letter to make it look like it came from someone else, like your boss or your bank, when it really came from an attacker.

4. Why are phishing emails dangerous?

They are dangerous because if you fall for the trick, bad things can happen:

- **They Steal Your Passwords:** Attackers can get into your email, social media, or bank accounts.
- **They Steal Your Money:** They can trick you into sending them money or use your stolen credit card details.
- **They Install Viruses:** The links or attachments can install malware or ransomware on your computer, locking up your files until you pay a ransom.

- **They Attack Your Company:** If you use a work computer, a single phish can let attackers into your company’s entire network.

5. How can you verify the sender's authenticity?

There are two main ways:

- **The Quick Way:** Carefully check the sender's email address for any misspellings or strange domains. Is it service@apple.com or service@appie.com?
- **The Technical Way:** Look at the email **header**. Tools like MXToolbox can check the header for SPF and DKIM records. If these checks **fail**, it's definitive proof the email is fake.

6. What tools can analyze email headers?

The easiest way is to use free online tools. You just paste the email header into them. The most popular ones are:

- **MXToolbox Email Header Analyzer**
- **Google Admin Toolbox Messageheader**

7. What actions should be taken on suspected phishing emails?

Follow these four steps:

1. **Don't Click Anything.** Do not click any links, buttons, or open any attachments.
2. **Don't Reply.** Replying confirms to the attacker that your email address is active, and they will target you more.
3. **Report It.** Use the "Report Phishing" or "Report Junk" button in your email client (like Gmail or Outlook). This helps the email provider block future attempts.
4. **Delete It.** After reporting it, delete the email from your inbox.

8. How do attackers use social engineering in phishing?

Social engineering is the main trick behind phishing. It's about **manipulating human emotions**, not hacking computers. Attackers pretend to be trustworthy and use feelings like:

- **Fear:** "Your account has been hacked! Click here to fix it!"
- **Urgency:** "This offer expires in one hour! Act now!"
- **Trust:** "This is your IT department. We need you to verify your password."

- **Greed:** "You've won a prize! Click here to claim it."
- **Curiosity:** "An invoice is attached for your review." (You open it because you want to see what it is).