1. What is phishing?

Phishing is a cyberattack where attackers impersonate legitimate organizations through email, messages, or websites to trick users into revealing sensitive information such as passwords, credit card numbers, or login credentials.

2. How to identify a phishing email?

Look for suspicious sender addresses, urgent or threatening language, generic greetings, unexpected attachments or links, poor grammar or spelling mistakes, and mismatched URLs.

3. What is email spoofing?

Email spoofing is when attackers forge the 'From' address in an email to make it appear as if it's coming from a trusted source to trick recipients into trusting and acting on the message.

4. Why are phishing emails dangerous?

They can steal sensitive data, install malware or ransomware, lead to identity theft or financial loss, and compromise entire networks.

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

Check the full email address, hover over links to see actual URLs, look for domain errors, use header analysis tools, and contact the organization directly via official channels.

6. What tools can analyze email headers?

Tools include Google Admin Toolbox Messageheader, MxToolbox Header Analyzer, Microsoft Message Header Analyzer, and HetrixTools Header Analyzer.

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

Do not click links or download attachments, do not reply, report it to your email provider, forward it to the impersonated organization, delete the email, and warn others.

8. How do attackers use social engineering in phishing?

They manipulate psychology using urgency, authority, fear, trust, curiosity, and brand mimicry, often leveraging personal data to craft convincing messages.