1. What is phishing?

Phishing is a cyberattack where attackers impersonate a legitimate entity (like a bank, company, or colleague) via email, message, or website to trick users into revealing sensitive information such as passwords, credit card numbers, or personal data.

2. How to identify a phishing email?

Look for these signs:

- Generic greetings (e.g., "Dear User")
- Spelling/grammar mistakes
- Urgency or threats ("Your account will be locked!")
- Suspicious links or attachments
- Email address mismatch (Display name may differ from the real sender's email)
- Unusual sender requests, like asking for login details or financial information.

3. What is email spoofing?

Email spoofing is when an attacker forges the "From" address in an email header to make it appear as if it was sent from someone else-usually a trusted source. It's commonly used in phishing attacks.

4. Why are phishing emails dangerous?

Phishing emails can:

- Steal sensitive data (credentials, bank info)
- Install malware or ransomware
- Compromise entire networks
- Lead to identity theft or financial loss

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

- Check the full email address, not just the display name

- Hover over links to inspect the real URL

- Use tools to analyze email headers (e.g., IP address and domain)

- Contact the sender through a trusted method (phone or verified email)

- Look for SPF/DKIM/DMARC authentication in the email header

6. What tools can analyze email headers?

- Google's Message Header Analyzer

- MxToolbox Email Header Analyzer

- Microsoft Message Header Analyzer (Add-in for Outlook)

- MailHeader.org

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

- Do not click links or open attachments

- Report the email to your IT/security team or email provider

- Mark it as spam/phishing in your email client

- Delete the email after reporting

- Educate users on the risks and patterns

8. How do attackers use social engineering in phishing?

Attackers manipulate human psychology to trick victims. Common tactics include:

- Pretending to be someone in authority (CEO, HR, IT)

- Creating a sense of urgency or fear

- Exploiting trust by mimicking known contacts

- Using emotional appeals or fake rewards