1. What is phishing?

Phishing is a cyberattack where attackers impersonate legitimate entities via email, messages, or websites to trick individuals into revealing sensitive information such as passwords, credit card numbers, or personal details.

2. How to identify a phishing email?

Phishing emails often:

- Contain generic greetings ("Dear user")
- Urge immediate action or threats
- Have suspicious links or attachments
- Use poor grammar or spelling
- Come from spoofed or unusual email addresses

3. What is email spoofing?

Email spoofing is the creation of email messages with a forged sender address. It is used in phishing attacks to make the email appear as if it comes from a trusted source.

4. Why are phishing emails dangerous?

They can:

- Steal sensitive data (e.g., login credentials, financial info)
- Infect devices with malware or ransomware
- Compromise business or personal accounts
- Lead to financial loss or identity theft

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

- Check the email address carefully
- Hover over links to inspect their URLs
- Use digital signatures or PGP for verification
- Contact the sender through a trusted method

6. What tools can analyze email headers?

Tools include:

- Google's Message Header Analyzer
- MXToolbox
- Microsoft 365 Message Header Analyzer
- Mailwasher
- Built-in tools in email clients (e.g., Outlook, Gmail)

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

- Do not click on any links or attachments
- Report the email to your IT or security team
- Mark it as spam or phishing in your email client
- Delete the email

8. How do attackers use social engineering in phishing?

Attackers manipulate emotions such as fear, urgency, or curiosity to trick users into taking unsafe actions-like clicking a link or sharing personal data-by pretending to be trusted figures (e.g., banks, managers, government officials).