Phishing and Email Threat Analysis – Interview Q&A;

1. What is phishing?

Phishing is a type of social engineering attack where attackers impersonate legitimate entities (like banks, government, or tech companies) through fake emails, messages, or websites to trick users into revealing sensitive information such as passwords, OTPs, credit card numbers, or downloading malware.

2. How to identify a phishing email?

You can identify a phishing email by checking:
- Spoofed sender email address
- Mismatched or suspicious links
- Urgent or threatening language
- Unusual attachments
- Generic greetings
- Grammar/spelling mistakes
- Failed SPF/DKIM authentication

3. What is email spoofing?

Email spoofing is a technique used by attackers to forge the 'From' field in an email header to make it appear as if the message is coming from a trusted source. It exploits SMTP limitations, allowing attackers to impersonate brands or people.

4. Why are phishing emails dangerous?

Phishing emails can:
- Steal sensitive information
- Distribute malware or ransomware
- Lead to account takeovers
- Cause data breaches or financial loss
- Exploit human error using social engineering

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

To verify a sender:
- Check full email address
- Use header analysis tools
- Check SPF, DKIM, DMARC
- Manually visit official website
- Contact the organization directly

6. What tools can analyze email headers?

Some free tools include:
- MxToolbox Header Analyzer
- Google Admin Toolbox – Messageheader

- Mailheader.org

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

- Do not click on links or open attachments
- Report the email to your provider
- Forward to the organization’s phishing email
- Block the sender
- Run a malware scan
- Educate your team or others

8. How do attackers use social engineering in phishing?

Attackers manipulate emotions like fear, urgency, or greed. They may impersonate banks, IT staff, or brands to create trust. Social engineering exploits human trust to bypass security systems.