Interview Questions & Answers

1. What is phishing?
Phishing is a cyberattack that involves sending fraudulent messages (usually via email) that appear to come from a legitimate source to trick users into revealing sensitive information like passwords, credit card numbers, or personal data.

2. How to identify a phishing email?
Phishing emails can be identified by:

- Mismatched or spoofed sender addresses
- Spelling or grammar mistakes
- Urgent or threatening language
- Suspicious links or attachments
- Generic greetings instead of personalized names

3. What is email spoofing?

Email spoofing is the act of forging the sender address in an email to make it appear as though it's coming from someone trusted (like a bank or service provider) to deceive the recipient.

4. Why are phishing emails dangerous?
They can lead to identity theft, unauthorized access to accounts, financial loss, malware infections, or data breaches by tricking users into clicking malicious links or submitting confidential information.

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

By checking:

- The sender's email domain
- Email headers (SPF, DKIM, DMARC)
- The actual link behind anchor text
- Whether the message is personalized
- Contacting the organization directly (not via email links)

6. What tools can analyze email headers?

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

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

- Do not click links or download 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

8. How do attackers use social engineering in phishing?

They exploit human emotions like fear, urgency, curiosity, or greed. For example, warning that your account will be suspended unless you act fast, or offering fake rewards or refunds to lure clicks.