Questions for the Interview

Phishing Fundamentals

1. What is phishing?

Phishing is a type of cyberattack where attackers **pretend to be a trustworthy entity** (like a bank, a major company, or a coworker) to trick victims into revealing sensitive information, such as passwords, credit card numbers, or other personal data.

2. How to identify a phishing email?

You can identify a phishing email by looking for several red flags:

- **Urgency/Threats:** Language that creates panic (e.g., "Your account will be suspended!").
- **Mismatched Links:** The link text looks real, but hovering over it reveals a strange, fraudulent destination URL.
- **Spelling/Grammar Errors:** Poor quality writing that a real company wouldn't send.
- **Generic Greetings:** (e.g., "Dear Customer") instead of your name.
- **Suspicious Sender:** The email address looks slightly off (e.g., paypal@service.net instead of service@paypal.com).

3. What is email spoofing?

Email spoofing is when an attacker **forges the sender address** of an email so it appears to come from someone else. They do this to make the email look legitimate, even though the message actually originated from a different, malicious server.

4. Why are phishing emails dangerous?

Phishing emails are dangerous because they are the primary method used to steal **credentials** (passwords, usernames) that can lead to:

- **Financial Fraud:** Draining bank accounts or making unauthorized purchases.
- **Identity Theft:** Using personal data to open new accounts.
- **Malware Installation:** Tricking you into downloading ransomware or other viruses.

Verification & Response

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

You can verify the sender's authenticity by checking the email's **headers** for three main protocols:

- **SPF (Sender Policy Framework):** Checks if the sender's IP address is authorized to send mail for that domain.
- **DKIM (DomainKeys Identified Mail):** Checks if the email content has been signed and hasn't been tampered with.

- **DMARC:** Specifies the policy for handling emails that fail SPF or DKIM.

If these protocols **fail**, the email is likely fake.

6. What tools can analyze email headers?

You can use free, online tools to analyze email headers:

- **MXToolbox Email Header Analyzer**
- **Google Admin Toolbox Message Header Analyzer**
- **Microsoft Message Analyzer (Header Analyzer)**

You just copy the full message source (header) and paste it into the tool.

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

1. **Do NOT Click Links or Download Attachments.**
2. **Report It:** Use your email client's "Report Phishing" or "Junk" feature, or forward it to your company's IT/Security team.
3. **Delete It:** After reporting, delete the email from your inbox and trash bin.
4. **Verify Separately:** If you're concerned about your account, **do not** use the links in the email. Instead, open a new browser tab and manually navigate to the company's official website.

8. How do attackers use social engineering in phishing?

Attackers use social engineering to exploit **human psychology** to bypass technical security tools. Common tactics include:

- **Urgency/Fear:** Creating a sense of crisis (e.g., "Pay this invoice immediately!") to prevent the victim from thinking rationally.
- **Authority:** Impersonating a boss or CEO to demand sensitive information (known as Whaling or BEC—Business Email Compromise).
- **Curiosity/Reward:** Offering a fake prize or a secret document to entice a click.