**Interview Questions**

**1) What is phishing?**

Phishing is a type of cyber attack where attackers impersonate legitimate organizations or people to trick victims into revealing sensitive information (passwords, credit-card numbers, OTPs) or to get them to install malware. Attacks commonly arrive as deceptive emails, messages, or fake websites.

**2) How to identify a phishing email?**

Common signs:

* Sender address doesn’t match the displayed name or the organization’s official domain.
* Urgent or threatening language (e.g., “verify now or account will close”).
* Suspicious links (hover to reveal real URL) or shortened/obfuscated URLs.
* Unexpected attachments, especially .exe, .zip, .docm, .xlsm, .js.
* Poor spelling/grammar or odd formatting.
* Requests for credentials, payment, or sensitive data.
* Authentication failures in headers (SPF/DKIM/DMARC show fail).

**3) What is email spoofing?**

Email spoofing is forging parts of an email (usually the From: address or headers) so the message appears to come from someone else. Attackers use spoofing to increase credibility and bypass basic filters. Authentication standards (SPF, DKIM, DMARC) help detect/prevent spoofing.

**4) Why are phishing emails dangerous?**

Because they can:

* Lead to credential theft and account takeover.
* Deliver malware/ransomware that infects systems.
* Cause financial loss via fraudulent payments or wire transfers.
* Enable data breaches and long-term access for attackers.
* Damage organizational reputation and require costly response/forensics.

**5) How can you verify the sender’s authenticity?**

* Inspect full email headers (Received, Return-Path, Authentication-Results).
* Check SPF, DKIM, and DMARC results in headers.
* Verify the sending domain (whois, check official website).
* Don’t trust display name — examine the envelope-from.
* Contact the organization via an independent channel (official phone number, website) — do not reply to the suspicious email.
* Look up the sender’s email in threat feeds/virus scanners or internal allow/block lists.

**6) What tools can analyze email headers?**

Common tools and services:

* Online header analyzers (e.g., MXToolbox Message Header Analyzer, Google’s “Show original” + Authentication-Results).
* VirusTotal / URLScan for URLs and attachments.
* Mail server logs and SIEM for correlation.
* dig / nslookup / whois for DNS and domain checks.
* Local tools: openssl (check certs), grep/sed for parsing, or email clients that show raw source.

**7) What actions should be taken on suspected phishing emails?**

Immediate steps:

* Don’t click links or open attachments. Quarantine the email.
* Block sender email and source IP/domain if confirmed malicious.
* Report to your security team, open an incident/ticket, and add IOCs to detection systems.
* Notify affected users; force password resets and enable/verify MFA if credentials were exposed.
* Preserve evidence (.eml/.msg, headers, attachment hashes) for forensics.
* Scan endpoints for signs of compromise and update protections (email filters, blocklists).
* If financial loss or data breach suspected, escalate to management and legal/compliance (and report to CERT if required).

**8) How do attackers use social engineering in phishing?**

Attackers exploit human psychology—fear, curiosity, urgency, authority, and trust—to manipulate victims. Examples: fake “security alert” to create fear, impersonating a boss to request wire transfer (authority), offering rewards or invoices (greed/curiosity), or creating time pressure (“respond within 1 hour”). Well-crafted personalized phishing (spear-phishing) uses public info (LinkedIn, social media) to increase credibility.