EMAIL PHISHING INTERVIEW QUESTION AND ANSWERS

1. What is phishing?

Phishing is a **cyberattack where attackers impersonate trusted entities** (like banks, companies, or colleagues) through fraudulent emails or messages to **trick victims into revealing sensitive information** (passwords, financial data) or **performing actions** (clicking malicious links, downloading malware).

2. How to identify a phishing email?

- **Suspicious sender addresses** (e.g., `support@paypa1.com` instead of `support@paypal.com`).
- **Urgent or threatening language** (*"Your account will be suspended immediately!"*).
- **Generic greetings** (*"Dear user"* instead of your name).
- **Links that don't match** (hover to check real destination).
- **Unexpected attachments** or requests for personal information.

3. What is email spoofing?

Email spoofing is when **attackers forge the "From" field** of an email so it appears to come from a trusted sender. It's often used in phishing attacks to **bypass initial suspicion** and trick victims into opening the email or clicking links.

4. Why are phishing emails dangerous?

- **Credential theft** – Attackers can access accounts (bank, email, work systems).
- **Malware infection** – Attachments or links may install ransomware, spyware, or trojans.
- **Financial fraud** – Stolen details are used for unauthorized transactions.
- **Data breaches** – Can lead to organizational compromise.

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

- **Check the full email address & domain** (not just the display name).
- **Inspect email headers** (look for the actual sending server).
- **Hover over links** before clicking to check the real URL.
- **Call or contact the sender directly** using official contact information.

6. What tools can analyze email headers?

- **MXToolbox** – For checking sender details, domain, and server info.
- **Google Toolbox Messageheader** – To analyze routing and identify spoofing.
- **Microsoft Message Header Analyzer** – For Office 365/Outlook emails.

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

- **Do not click links or open attachments.**
- **Report the email** to your IT/security team or email provider.
- **Block the sender** (if confirmed as malicious).
- **Delete the email** after reporting.

8. How do attackers use social engineering in phishing?

- **Impersonation** – Pretending to be someone trusted (boss, bank, colleague).
- **Urgency & fear** – Forcing quick action (*"Act now or lose access!"*).
- **Temptation** – Offering rewards (*"You've won a prize!"*).
- **Authority** – Using fake official-looking communication (government, company).