**TASK-02 INTERVIEW QUESTIONS AND ANSWERS**

**1. What is phishing?**

Phishing is a cyberattack method where attackers send fraudulent messages (often emails) pretending to be from a trusted source to trick people into revealing sensitive information such as passwords, credit card numbers, or installing malware.

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

* Suspicious sender address (often looks similar but slightly off)
* Urgent or threatening language pressuring immediate action
* Poor grammar and spelling mistakes
* Mismatched or suspicious URLs (hover to check real links)
* Unexpected attachments or links
* Generic greetings instead of personal names
* Requests for sensitive info like passwords or financial data

**3. What is email spoofing?**

Email spoofing is when attackers forge the sender’s address in an email to make it appear as if it’s coming from a legitimate or trusted source to deceive the recipient. Eg: An attacker sends an email that appears to come from support@paypal.com but is actually sent from support@paypa1.com or from a completely different server. The attacker has forged the sender address to trick you.

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

They can lead to:

* Theft of personal or financial information
* Unauthorized access to accounts
* Installation of malware or ransomware
* Financial loss or identity theft
* Damage to reputation or company security

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

* Check the full email address carefully (not just the display name)
* Examine email headers for origin IP and domain alignment
* Verify digital signatures like SPF, DKIM, and DMARC records
* Contact the sender via an independent channel (phone or official website)
* Use online tools to check domain reputation

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

* MXToolbox Email Header Analyzer (https://mxtoolbox.com/EmailHeaders.aspx)
* Google Admin Toolbox Messageheader (https://toolbox.googleapps.com/apps/messageheader/)
* MailTester
* Online SPF, DKIM, DMARC checkers

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

* Do not click any links or open attachments
* Report the email to your IT or security team
* Mark the email as spam or phishing in your email client
* Delete the email after reporting
* If you clicked a link or provided info, change passwords immediately and alert your organization

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

Attackers manipulate emotions like fear, curiosity, or urgency to trick victims into taking unsafe actions (e.g., clicking malicious links or sharing credentials) by pretending to be trustworthy sources or authorities.