**TASK 2**

**Interview Question**

**1. What is phishing?**

Phishing is a cyberattack where attackers send fake emails or messages pretending to be trusted sources to steal sensitive data like passwords, bank details, or install malware.

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

* Generic greeting (e.g., “Dear user”)
* Urgent or threatening tone
* Misspelled or fake sender address
* Suspicious links or attachments
* Poor grammar or formatting
* Requests for personal or financial information

**3. What is email spoofing?**

Email spoofing is forging the sender’s address or domain to make the email appear as if it’s coming from a trusted source.

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

They can lead to data theft, financial fraud, identity theft, and malware or ransomware infections.

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

* Check full sender address and domain
* Hover over links to inspect URLs
* Review SPF/DKIM/DMARC results in headers
* Contact the sender through official channels
* Never share credentials via email

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

* MXToolbox Email Header Analyzer
* Google Message Header Tool
* Mailheader.org
* Microsoft Header Analyzer / SpamCop

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

* Don’t click links or download attachments
* Report to IT/security team
* Mark as phishing/spam
* Change passwords if compromised
* Run antivirus or security scan

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

They exploit human emotions like trust, fear, and urgency — pretending to be an authority (bank, boss, government) or offering rewards to make victims act without thinking.

**I have developed a Phishing detection Project**

<https://github.com/govardhanhl/typosquattingDetection>