1. What is phishing?

Phishing is a type of cyberattack where attackers trick users into giving sensitive information (passwords, OTPs, bank details) by pretending to be a trusted person or organization, usually through email, messages, or fake websites.

2. How to identify a phishing email?

You can identify a phishing email by checking for:

- **Suspicious sender address** (like random numbers or misspelled company names).
- **Urgent or threatening language** (“Your account will be closed!”).
- **Unexpected attachments or links**.
- **Spelling/grammar mistakes**.
- **Links that don’t match the real website** (hover to check).
- **Requests for personal information**.

3. What is email spoofing?

Email spoofing is when attackers fake the “From” address to make the email look like it came from someone you trust.
Example:
A hacker sends an email that looks like it's from **info@bank.com**, but it’s not.

4. Why are phishing emails dangerous?

Phishing emails are dangerous because they can:

- Steal your **passwords**, **bank info**, or **personal data**.
- Install **malware** or **ransomware** on your device.
- Give attackers access to your accounts.
- Lead to financial loss or identity theft.

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

You can verify authenticity by:

- Checking the **full email address**, not just the name.
- Hovering over **links** to see real URLs.
- Looking at the **email header** (shows real server IP/domain).
- Contacting the sender through **official channels** (not by replying).
- Checking for **DKIM**, **SPF**, and **DMARC** authentication results.

6. What tools can analyze email headers?

Common tools for analyzing email headers include:

- **Google Admin Toolbox → Message Header Analyzer**
- **MXToolbox Header Analyzer**
- **Microsoft Message Header Analyzer**
- **Header Security Tools in email clients** (e.g., Outlook, Gmail)

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

You should:

- **Do NOT click** links or open attachments.
- **Report** it to your company/IT team or email provider.
- **Mark it as spam/phishing**.
- **Delete** the email immediately.
- If you clicked it accidentally, change your **passwords** and run a **security scan**.

8. How do attackers use social engineering in phishing?

Attackers use social engineering by manipulating human emotions such as:

- **Fear** ("Your account will be blocked").
- **Curiosity** ("Payment invoice attached").
- **Urgency** ("Respond in 2 hours").
- **Trust** (pretending to be your boss, bank, or friend).