1. What is phishing?
Phishing is a type of cyber scam where attackers pretend to be a trusted entity to trick people into revealing sensitive info like passwords or bank details. They often use deceptive emails, messages, or websites that look legit.

2. How to identify a phishing email?
Look for mismatched sender addresses, generic greetings, urgent requests, suspicious links or attachments, and poor spelling/grammar. If something feels off or pushes you to act quickly, treat it with caution.

3. What is email spoofing?
Email spoofing is when an attacker forges the 'From' address so a message appears to come from someone you trust. It's a common trick used to make phishing emails look more believable.

4. Why are phishing emails dangerous?
Phishing can lead to credential theft, financial loss, malware infections, or unauthorized access to accounts and systems. Even a single click or reply can compromise personal or company-wide security.

5. How can you verify the sender's authenticity?
Check the full email header, hover over links to preview URLs, confirm with the sender via a known contact method, and look up domain details if unsure. Don't use reply-to addresses or contact info provided inside the suspicious message.

6. What tools can analyze email headers?
Online header analyzers (like MXToolbox), email client header viewers, and specialized forensic tools can parse headers and show the true message path. These help spot spoofed senders, relay hops, and originating IPs.

7. What actions should be taken on suspected phishing emails?
Do not click links or download attachments — mark the message as phishing/spam, report it to your IT/security team, and delete it. If you interacted with it, change passwords and run a malware scan immediately.

8. How do attackers use social engineering in phishing?
Attackers exploit emotions — fear, urgency, curiosity, or trust — to manipulate victims into acting without thinking. They research targets to craft personalized messages (spear-phishing) that are more convincing.