What **is phishing**  
Social-engineering attack where an attacker impersonates a legitimate service to steal credentials or deliver malware.

**How to identify a phishing email**  
Check sender address, hover links, inspect headers (SPF/DKIM/DMARC), note urgency/generic greetings and spelling errors.

**What is email spoofing**  
Forging email headers/display names so a message appears to come from someone else.

**Why are phishing emails dangerous**  
They steal credentials, deliver malware, facilitate fraud, and can lead to account takeover.

**How can you verify the sender’s authenticity**  
Check full headers, SPF/DKIM/DMARC results, confirm domain ownership, and verify with the sender by an independent channel.

**What tools can analyze email headers**  
MXToolbox Email Header Analyzer, dmarcian header analyzer, email client “Show original”; plus dig/nslookup for DNS checks.

**What actions should be taken on suspected phishing emails**  
Report to provider/security team, don’t click links/download attachments, save evidence, block sender, and delete.

**How do attackers use social engineering in phishing**  
They create urgency, mimic trusted brands, exploit fear/greed, and craft believable pretexts.