1. What is Phishing?
   Ans: Phishing is an attempt by cybercriminals posing as legitimate institutions, usually via email, to obtain sensitive information from targeted individuals.

2. How to identify a phishing email?
   Ans: Phishing email often hide malicious and unexpected attachments or links whose real URL differs from the visible anchor text. They frequently come from unfamiliar senders, use vague greetings, or contain suspicious addresses/domains that don't match the purported sender. Poor spelling or grammar and unusual file attachments are also key red flags indicating a phishing attempt.

   3.What is email spoofing?
   Ans: Email spoofing is a threat that involves sending email messages with a fake sender address. Email protocols cannot, on their own, authenticate the source of an email. Therefore, it is relatively easy for a spammer to change the metadata of an email.

   4.Why are phishing emails dangerous?
   Ans: Phishing is dangerous because it can lead to malware infections, such as ransomware , which can sabotage systems and organizations. It can also trick users into revealing sensitive information, like passwords or financial data, or transferring money to attackers. Phishing attacks can hit organizations of any size and type, causing financial losses, data breaches, and reputational harm.

   5. How can you verify the sender's authenticity?
   Ans: You can verify a sender's authenticity by analyzing SPF records, which confirm if the email was sent from an authorized server or that domain, Digital signatures(like DKM or PGP) ensure the message hasn't been tampered with and truly comes from the claimed sender. Adavanced methods like blockchain verification and metadata analysis add further layers of trust and automation, quickly detecting spoofed or fraudulent emails.

   6.What tools can analyze email headers?
   Ans: MXToolbox Email Header Analyzer, Wireshark help trace email origins, detect spoofing and analyze delivery paths or unusual behaviour.

   7.What actions should be taken on suspected phishing emails?
   Ans: If you receive a suspected phishing email, do not click any links or download attachments and never respond with personal information. Instead check for secure website indicators and finally report to the email to your IT/Security team or mark it as phishing in your email client to help prevent future attacks.

   8.How do attackers use social engineering in phishing?
   Ans: Attackers use social engineering in phishing to trick victims into divulging sensitive information by creating fake trust and urgency. This exploits human psychology, bypassing technical security measures.