Phishing Attack Multiple Choice Questions

1. What is the primary goal of a phishing attack?
   A) To steal sensitive information
   B) To test network performance
   C) To improve cybersecurity awareness
   D) To speed up email delivery

2. Which of the following is a common sign of a phishing email?
   A) Perfect grammar and spelling
   B) Urgent or threatening language
   C) Secure company email address
   D) Personalized domain name

3. What should you check first in a suspicious email?
   A) The sender’s address
   B) The background color
   C) The image size
   D) The font type

4. What is spear phishing?
   A) A random attack targeting many people
   B) A targeted phishing attack on a specific individual or group
   C) An automated spam campaign
   D) A network scanning method

5. Which tool can help detect phishing websites?
   A) Web browser security filters
   B) Paint application
   C) Word processor
   D) Music player

6. How can employees be best protected against phishing?
   A) Avoiding all emails
   B) Regular cybersecurity awareness training
   C) Ignoring IT updates
   D) Using outdated antivirus software

7. Why is multi-factor authentication (MFA) effective against phishing?
   A) It slows down email servers
   B) It adds an extra layer of verification
   C) It blocks all emails automatically
   D) It encrypts only the subject line

8. Which of these is a typical payload in a phishing email?
   A) Ransomware link
   B) System update notification
   C) Greeting card
   D) PDF newsletter

9. If you receive a suspicious email, what is the safest action?

A) Click the link to see what it does
B) Reply asking for clarification
C) Report it to IT/security team
D) Forward it to all colleagues

10. What should you do immediately after clicking on a phishing link?

A) Ignore it
B) Disconnect from the internet and report to IT
C) Download the linked file
D) Continue using the system normally