TRAINER RESOURCES

CYBER SECURITY TRAINING

Knowledge Check Quiz

Name: _____ **Date:** _____ **Score:** _____ / 8

CIRCLE THE CORRECT ANSWER FOR EACH QUESTION

Q1. What is phishing?

A. A type of malware that encrypts files
B. A fraudulent attempt to obtain sensitive information by disguising as a trustworthy source
C. A network vulnerability
D. A type of firewall attack

Q2. What is multi-factor authentication (MFA)?

A. Using multiple passwords
B. A security process requiring two or more verification methods
C. Logging in from multiple devices
D. A type of encryption

Q3. What should you do if you receive a suspicious email?

A. Delete it immediately
B. Forward it to colleagues to warn them
C. Report it to IT and do not click any links
D. Reply to ask if it is genuine

Q4. What is ransomware?

A. Software that monitors employee activity
B. Malware that encrypts files and demands payment for the decryption key
C. A type of spam filter
D. A network monitoring tool

Q5. What does UK GDPR require organisations to do with personal data?

A. Store it indefinitely for security purposes
B. Process it lawfully, fairly and transparently with appropriate security measures
C. Share it freely between departments
D. Delete it after 30 days

Q6. What is social engineering?

A. Building relationships with colleagues
B. Manipulating people into revealing confidential information or performing actions
C. Managing social media accounts
D. Workplace team building

Q7. How long should a strong password be?

A. 6 characters
B. 8 characters
C. At least 12 characters
D. Exactly 10 characters

Q8. What should you do before connecting to public Wi-Fi for work?

A. Connect freely — public Wi-Fi is safe
B. Use a VPN to encrypt your connection
C. Change your password first
D. Disable your firewall

Answer Key (Trainer Use Only): Q1:B Q2:B Q3:C Q4:B Q5:B Q6:B Q7:C Q8:B