■ Cyber Security Trainer — Knowledge Check Quiz

15 Multiple Choice Questions | Free Trainer Resource | trainerresources.com

Instructions: Circle or tick the correct answer for each question. This quiz covers key knowledge areas for the **Cyber Security Trainer** course. Pass mark: 12/15 (80%). Answers are provided on the final page.

Q1. What is phishing?

A) A fishing technique
B) A fraudulent attempt to obtain sensitive information by disguising as a trustworthy entity
C) A type of malware
D) A network attack

Q2. What is a strong password?

A) Your name and date of birth
B) At least 12 characters with uppercase, lowercase, numbers and symbols
C) A word from the dictionary
D) Your pet's name

Q3. What is two-factor authentication (2FA)?

A) Two passwords
B) A security process requiring two forms of verification before granting access
C) Two usernames
D) A double firewall

Q4. What is malware?

A) A software update
B) Malicious software designed to damage, disrupt or gain unauthorised access to systems
C) A type of hardware
D) An antivirus program

Q5. What is ransomware?

A) A type of phishing
B) Malware that encrypts files and demands payment for decryption
C) A network scanner
D) A password manager

Q6. What is social engineering?

A) Building social networks
B) Manipulating people into revealing confidential information or performing actions
C) A type of malware
D) A network protocol

Q7. What should you do if you receive a suspicious email?

A) Open all attachments to check
B) Do not click links or open attachments — report to IT security
C) Forward it to colleagues

D) Delete it without reporting

Q8. What is the UK GDPR?

A) A marketing regulation
B) UK General Data Protection Regulation — governs how personal data is collected, stored and used
C) A cyber security standard
D) An IT industry guideline

Q9. What is a data breach?

A) A system update
B) A security incident where personal data is accessed, disclosed or lost without authorisation
C) A network failure
D) A software bug

Q10. What is a VPN?

A) A type of virus
B) Virtual Private Network — encrypts internet traffic and hides IP address
C) A video platform
D) A verification process

Q11. What is the principle of least privilege?

A) Giving all users admin access
B) Users should only have access to the data and systems they need for their role
C) Restricting all access
D) A password policy

Q12. What is a firewall?

A) A physical barrier
B) A network security system that monitors and controls incoming and outgoing traffic
C) An antivirus program
D) A data backup system

Q13. What should you do if you suspect a cyber attack?

A) Ignore it
B) Report immediately to IT security, disconnect affected systems, do not attempt to fix yourself
C) Try to fix it yourself
D) Turn off the computer and go home

Q14. What is the Cyber Essentials scheme?

A) A government tax scheme
B) A UK government-backed certification scheme helping organisations protect against common cyber threats
C) An IT training course
D) A software product

Q15. What is a zero-day vulnerability?

A) A vulnerability in old software
B) A previously unknown vulnerability in software that has not yet been patched
C) A vulnerability that takes zero days to fix

D) A type of malware

Answer Key

Q1: B Q2: B Q3: B Q4: B Q5: B Q6: B Q7: B Q8: B Q9: B Q10: B Q11: B Q12: B Q13: B Q14: B Q15: B