9.3 Cyber security

SOCIAL ENGINEERING: this is a way of gathering sensitive information or illegal access to networks by influencing / manipulating people.

PHISHING / SMISHING: sending emails or text messages (SMs) claiming or appearing to be from a bank/ e-commerce site asking for personal details and/or credit card details.

TROJAN software is malware that is disguised as legitimate software.

SHOULDERING: involves finding passwords and pins by watching people enter them. This could happen in a busy office or at a distance using binoculars or recording equipment.

BLAGGING: involves a criminal inventing a scenario to persuade a victim to give out information.

Organisations should have acceptable use policies which employees must read, sign and abide by.

It should include security issues such as:

- Users must not use their own devices as they may contain malware (e.g. USB drives).
- Users should not download files from the internet (as they may contain malware).
- Users must have strong passwords which should be changed frequently to prevent brute force attacks.
- Users should not leave themselves logged on.

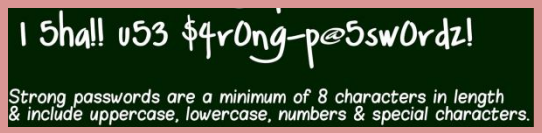
User access levels should be applied to ensure that only the people who require access to sensitive data have it.

PEN TESTING: testing a computer system to find weaknesses that a hacker could exploit.

Testers take the role of hackers to gain unauthorised access. Assess the security awareness of users and tests the effectiveness of network policies.

Anti-virus software is designed to detect and block attacks from malware.

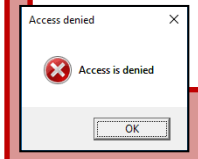
Norton by Symantec · McAfee Proven Security · AVG Anti-Virus



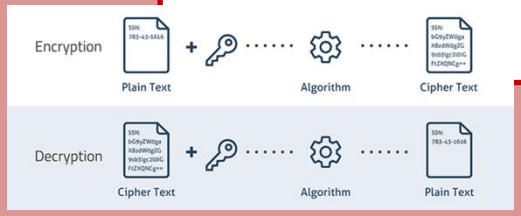
A firewall monitors connections to and from your computer. If it spots something suspicious, it closes the connection or disconnects it.

Most operating systems include a firewall and it should be turned on by default.

USER ACCESS LEVELS: controls which users or groups of the network users or groups of users can access.



ENCRYPTION: coding data into an unreadable format so that unauthorised users cannot understand. Only decoded with a decryption key.



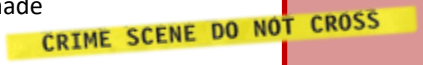
A GOOD NETWORK POLICY:

- ❑Use passwords.
- ❑Enforce user access levels.
- ❑Encrypt sensitive data.
- ❑Regularly test the network to find & fix weaknesses.
- ❑Install anti-malware & firewall software.

NETWORK FORENSICS:
Monitoring, recording and analysis of network activity :

- Who has logged on
- How many unsuccessful attempts have been made
- What users have done
- What has been deleted.

Network forensics can be used as legal evidence if illegal activity is detected.



9.3 Cyber security

What I need to know:

What is social engineering?			
What is phishing /smishing?			
What is shouldering?			
What is blagging?			
What 5 things should a network policy enforce?			
What things might be included in an acceptable use policy?			
Explain what pen-testing is and how it helps protect a network.			
Explain what network forensics is and how it can help with security.			
What is antivirus software?			
What is a firewall?			
What are user-access levels?			
What is encryption?			
What advice would you give someone to create a strong password?			