1.6 SYSTEM SECURITY

TYPES OF ATTACK

Attack	How it works	How to prevent it
Passive	Network traffic is monitored and then data is intercepted	Encryption so that intercepted data cannot be understood
Active	Someone deliberately attacks a network with malware (eg: a virus)	A firewall and antivirus software
Insider	Someone with network access abuses this to steal information	User access levels to control how much data people can access.
Brute Force	Trial an error until a password is attacked	Making passwords difficult to guess. Locking accounts after failed attempts.
Denial of Service	The network is flooded with useless data so it is too slow to use	This attack is hard to prevent but a firewall can help.
SQL Injection	SQL commands are typed into the input boxes on a website to access data or alter the database	Having strong validation on all input boxes so that only expected data can be entered
Phishing	Emails with links that trick people into entering their personal information	Looking for signs that an email is not from a real company.
Social Engineering	When a person manipulates someone else into handing over sensitive information	Policies and rules for staff about handing over data. Staff training.

NETWORK SECURITY KEY TERMS

Malware: malicious software intended to cause harm.
Penetration Testing: Organisations employ professionals to try and hack their network so that they can find areas of weakness.
User Access Levels: Different employees have different levels of access to programs, websites and data.
Encryption: data is scrambled so that it cannot be understood if intercepted. It can only be decrypted with a key.
Network Forensics: Data packets are captured as they enter the network and analysed to find out the cause of a network attack.

Types of Malware

Virus - attach themselves to files and copy themselves when the user copies or opens a file.

Worm - copy themselves without the user doing anything.

Trojan - malicious software pretending to be a legitimate program.

EXAM QUESTIONS

1. Describe what is meant by “Malware”
2. Describe how a brute force attack works and how to prevent it.
3. Explain how to keep a network secure.
4. Evaluate the benefits and drawbacks of a business using penetration testing