1.4 NETWORK SECURITY

Key Terms

A network is where devices have been connected together so that they can share data and resources. Networks can be wired (Ethernet) or wireless (WiFi).

Local Area Network (LAN)	Cover a small geographical area such as an office. Use their own infrastructure.
Wide Area Network (WAN)	WANs connect LANs together over a large geographical area and make use of infrastructure from telecommunications companies.
Bandwidth	The amount of data that can pass between network devices per second
Server	A device that provides services for other devices (eg file server or print server)
Client	A computer or workstation that receives information from a central server
Peer to peer Network	All of the computers in the network are equal. They connect directly to each other.
Standalone computers	A computer not connected to a network

NETWORK HARDWARE

Network Interface Controller (NIC): built in hardware that allows a device to connect to a network.
Switches: connect devices on a LAN
Router: Transmits the data (packets) between the networks (eg: the internet and your LAN)
Wireless Access Point (WAP): a switch that allows devices to connect wirelessly.
Cables: the cables in a network can be twisted pair cables, coaxial cables or fibre optic cables.

NETWORK PERFORMANCE

These factors can impact on network performance:
Bandwidth: The more bandwidth, the more data that can be transferred at a time.
Number of Users: Having a lot of people using a network means lots of data is being transmitted which can slow it down.
Transmission Media: Wired connections are faster than wireless. Fibre optic cables are faster than copper cables.
Wireless Factors: wireless can be affected by walls, distance, signal quality and interference from other devices.
Topology: The layout of a network can impact on its performance.

VIRTUAL NETWORKS

A virtual network is part of a LAN or WAN where only certain devices can “see” and communicate with each other.

EXAM QUESTIONS

1. Give 3 items of hardware needed for a network
2. Explain the difference between a peer-to-peer network and a client server network.
3. The school’s network has become very slow. Explain two different reasons why this might be.
4. Evaluate the benefits of using a wired connection rather than a wireless one.

1.4 NETWORK SECURITY CONTINUED

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