Networks

Network: Multiple computers connected to share information and resources.
Local Area Network (LAN)

- Each device is called a node, On one site (Network is small)
- All network infrastructure is the property of the organisation
- Advantages: Allows people to communicate and share information and peripheral devices digitally.
- Disadvantages: Expensive, needs IT expertise to install and maintain, hackers could access lots of data

Wide Area Network (WAN)

- Covers a large geographical area, Devices may be provided by telecommunication companies

Network Interface Card (NIC): Converts node signals into signals that can be transferred across a network
Hub: Connects nodes together; data packets are transmitted across the whole network (not intelligent)
Switch: Connects nodes together; the network is split into different segments; data packets are transmitted to a single segment (intelligent)
Router: Routes data packets between networks
Wireless Access Point (WAP): Allows you to connect to a network wirelessly

- Client-Server Network:
  - Contains at least one server, Clients ask for services, the server provides
  - Server offers software, data; manages backups, security and updates
- Peer-To-Peer Network
  - All computers have the same status (all called peers)
  - All computers manage their own data, software, backups, security, etc

- Bus Topology: Only one cable (very cheap), If the cable breaks, the whole network stops
  - Data travels both ways along the cable, thus data can collide, slowing the network down
- Ring Topology: Only one cable (very cheap), If the cable breaks, the whole network stops
  - Data travels in only one direction, so no data collisions
- Star Topology: Little cabling (quite cheap), No data collisions
  - If a cable breaks, one node cannot connect to the network
- Mesh Topology: Every Node is connected to every other
  - Lots of cabling (very expensive), If a cable breaks, all nodes can use other routes

Web Hosting: Where companies host websites on their servers.
Host: A computer which offers to serve users over the Internet
Internet Service Provider (ISP): Provides you with your internet connection
URL: A name for a web address
Domain Name System (DNS): Used to exchange a website's URL for its IP address
The Cloud: Servers on the Internet which store data.

DNS:

- Type the URL into the web browser
- The URL is sent to your ISP, who look up the URL in their DNS 'address book'
- They send back the website's IP address, use this to find the server which hosts the website

Cloud Storage:

- Advantages: Multiple people can access your data at any time, from any location, at the same time
  - Work is automatically saved; cheaper than hosting the data yourself
- Disadvantages: A small fee is charged; Requires an Internet connection

Contents of a data packet
Data: Contains the message data
Packet Header: Contains the Sequence Number, the Return Address, and the Destination Address
Sequence Number: Allows the packets to be rearranged into the correct order
Return Address: The address of the transmitting computer
Destination Address: The address of the receiving computer
Error Checking: Fixes minor corruptions

Networks

MAC address: Every NIC has one, hard coded; a physical address (static), It is a 12-digit hexadecimal number
IP Address: A unique number given to every computer on the Internet, 32 bit number written as 4 decimal numbers, Changes each time it joins a network (dynamic)

TCP – Transmission Control Protocol

- Splits data into packets, Adds the sequence number, Encrypts and decrypts data
- At the receiving computer, it asks for missing, and too-corrupted packets to be sent again
- Once all packets have arrived, the message is reconstructed

IP – Internet Protocol: Adds and Removes the Return and Destination IP addresses

Packet switching: The only efficient way to send data on a shared line (everything else)

- Split file into data packets, routers direct packets towards their destination.
- Due to network traffic, different packets may take different routes
- Data gets to the destination as fast as possible, but not necessarily through the shortest distance

Circuit switching: Used with a dedicated communication channel (voice and video calls)

- The data is sent in order; there is no delay in receiving the data
- Massively wastes bandwidth as others cannot use the same communication channels
- Less efficient than packet switching

Protocol: Standard rules that all computers must follow so that they can produce and send data packets in the same standard way, and to allow them to communicate effectively.
HTTP: Governs how web browsers govern websites and web servers
HTTPS: HTTP + encryption
FTP: Governs how you access files stored on a server
POP: Governs how emails are accessed from a server; the email is taken off the server
IMAP: Governs how emails are accessed from a server; the email remains on the server
SMTP: Governs how emails are sent between mail servers.
Physical protocols: Govern the physical mediums through which the data is travelling (wires, wireless)
Logical protocols: Govern the data being sent (packet size, routing)
Handshaking: When two devices decide on what protocols they want to use.

Application Layer: Provides access to applications, websites, files, email
Transport Layer: Provides data transport between devices (TCP)
Network Layer: Provides data routing between devices (IP)
Physical Layer: Provides the physical transport of data through electrical signals

Malware: A small, malicious program which aims to cause physical harm to a computer system.
Pharming: Intends to redirect a website's traffic to a fake site by changing the DNS server's IP address.
Phishing: Where emails try to impersonate legitimate companies and ask you to give sensitive information.
Social Engineering: Manipulating people to make mistakes, compromising a network's security.
Denial Of Service: Uses multiple computers to repeatedly make requests of a server, putting it under extreme pressure and causing it to crash.
SQL Injection: Adding SQL into input boxes, altering the SQL statement, allowing hackers to access other user's accounts

Penetration Testing: Where experts are employed to simulate a range of network attacks, to discover any weaknesses in the system and recommend improvements to their security.
Anti-malware software: Dedicated to finding and destroying malware. Must be up-to-date to be effective.
Firewalls: Analyses data which flows through the ports; either allowed through or rejected.
Encryption: Where data is encrypted before being transmitted so that it is unreadable if intercepted.
User access levels: Users are given different access rights depending on their role in the company
Secure Passwords: Long passwords, with numbers, lowercase letters, uppercase letters, and special characters, will not succumb to Brute Force attacks