Forms of Attack	
Active	An attempt to modify or delete data, or to stop the network from operating correctly.
Passive (Eavesdropping)	An attempt to find information about the network or retrieve information without changing anything.
Internal	An attack by someone inside the organisation.
External	An attack by someone outside the organisation.

Qualities of a Strong Password

- At least eight characters
- Include upper case and lower case
- Include special characters
- Include numbers
- Does not include a name
- Does not contain a complete word
- Relates to an acronym

Types of Malware	
Viruses	Malicious software hiding within another application. Designed to harm a network or computer system
Worms	Similar to viruses but not hidden within other files. Replicates through a network to spread to other computers
Trojans	Programs which pretend to be legitimate but are malware. Often disguised as email attachments. Cannot spread by themselves and so deceive a user into installing them.
Spyware	Monitors user activities and send the information back to an attacker.
Ransomware	Blackmails users into making a payment to an attacker. Some will only try to frighten users into paying, others will encrypt files

1.4 - Network Security

Threats to a Network	
Social Engineering	Where users do not follow policies, make a mistake such as using their name as password, or are tricked into giving out information. Phishing emails trick users into giving away information. Pretends to be a genuine message with a link to a website that looks like the real company.
Brute force	Trial and error. Tries all possible passwords until the correct one is found.
Denial of service (DOS)	Overloads a computer or network with traffic by bombarding it with requests.
Data interception and theft	Looking at data travelling over a network, often using software called a packet sniffer.
Structured query language (SQL) injection	Affects websites which use a SQL database. SQL code is entered into a data input field on the website to look at or modify data stored in the database.
Malware	Malicious software designed to cause harm to a system or network. Users are often tricked into running malware.

Identifying and Preventing Vulnerabilities

- **Penetration testing** - The network is scanned for security weaknesses, vulnerabilities and poor configuration to find problems before an attacker can. Software is often used to automate this process. Allows organisations to find and fix threats before attackers can use them.
- **User access levels -** Controls which parts of a system users can access. Users should only be given access to parts of a system they need. Limits the actions a user can take. Reduces the risk of both deliberate data theft, but also the damage that can be cause by social engineering attacks or malware.
- **Secure passwords -** Passwords should not be easy to guess, should be long and include numbers and symbols. Passwords should not be shared. Defence against brute force attacks, these take much longer with secure passwords.
- **Encryption -** Data is translated into code so that only those with the key can read it. Means that if data is intercepted it cannot be read. Defence against data interception and theft.
- **Anti-malware Software -** Prevents malware from being installed and removes any that is installed. Includes anti-virus software, anti-phishing tools and anti-spyware software. Scans all the files on a computer and checking them against a list of known malware.
- **Firewalls -** Monitors traffic going into and out of a computer or network, and either allows or blocks it. Forms a barrier between a system and the attacker.
- **Physical Security –** Controls access to servers, networking equipment and other important hardware. May take the form of security guards, locks, CCTV or swipe cards.