Cyber Security

Malware	Malware is malicious software. Any software that has been intentionally designed to cause damage to a computer system falls under the umbrella term malware.
Virus	A piece of code that is self replicating designed to cause damage to a computer system by destroying data or corrupting the system.
Worm	Stand alone malware computer program that does not need to be attached to a file. Worms use computer networks to spread, and relies on poor security systems.
Trojan	**Think Romans!** Trojan is a malicious program that "hides" within a file and works around misleading the user to download the item. Common Trojans are found in attachments sent through email.
Spyware	Software designed to spy on a person or group of people, gathering data about them and sending it to a 3rd party without the consent of the data owner.
Ransomware	Software that is designed to threaten the infected user with threats of blocks and leaking of data unless the user meets the software requirements. **Example was the NHS in 2017**
Brute Force	This is when a hacker would try every single password combination until access has been granted. Depending on the complexity of the password this may take seconds or years.
DOS	Denial of server attack. This is cyber attack which is focused around disrupting a target with unneeded requests to slow down their services, which in turn costs the target money.
Social Engineering	**People are weak.** This is a form of psychological manipulation getting confidential information out of people to aid in conducting unlawful actions.
Phishing	The concept of tricking someone. Phishing emails are emails that pretend they are someone important like your bank account to try and trick the target into providing important information.
Shouldering	**Shouldering** (also known as **shoulder surfing**) is an attack designed to steal a victim's password or other sensitive data. It involves the attacker watching the victim while they provide sensitive information, for example, over their shoulder.
Blagging	An attack in which the perpetrator invents a scenario in order to convince the victim to give them data or money. This attack often requires the attacker to maintain a conversation with the victim until they are persuaded to give up whatever the attacker asked for.
Name generator	The victim is asked in an app or a social media post to combine a few pieces of information or complete a short quiz to produce a name. Attackers do this to find out key pieces of information that can help them to answer the security questions that protect people's accounts.

Cyber Security

Prevention Methods	
Network Policy	This is a document that outlines the rules for a network. A policy will outline rules linked to access and acceptable use of the network.
Penetration Testing	This is the practice of testing a computer network looking for vulnerabilities in the networks security so these can be patched up to aid in preventing future attack attempts.
Network forensics	This is the process of monitoring and analysing a computer network and the traffic through it.
Physical Security	Examples of physical security are lock and key, keypads, swipe cards, RFID, bio metric etc.

Logical Security Methods	
Passwords	Passwords are a common method for securing important data and files. Strong passwords will contain numbers, symbols, capital letters and lower case. Usually there are a maximum number of attempts to log in before an account is locked.
CAPTCHA	A type of challenge–response test used in computing to determine whether or not the user is human.
Biometrics	Physical or behavioural human characteristics to that can be used to digitally identify a person to grant access to systems, devices or data. Examples of these biometric identifiers are fingerprints, facial patterns and voice.
Two-factor authentication (2FA	A method of confirming users' claimed identities by using a combination of two different factors: 1) something they know 2) something they have or 3) something they are.
Access Levels	It is important to only give users information that is required for their role to ensure there is no leak of data and unauthorised access to important files. Access levels aid in restricting users from accessing specific data unless they have the correct access.
Firewalls	Controls the packets that enter and leave a network to ensure that malicious software or unauthorised access to important files isn’t conducted.
Anti-Malware	Software that is designed to detect and deal with malware that your computer system may interact with. Anti-malware software, also known as anti virus software, is designed to protect your computer system.
Encryption	Encryption is when the data is “scrambled” so if the data was intercepted as it was being sent across a network or the internet the hacker would struggle to read the contents.