Cyber Security

Cyber security is keeping computers, devices and networks safe from digital attacks.

Attacks could include:

- hacking
- malware
- social engineering

Cyber Security

Hacking is trying to get **unauthorised access** to a computer system

People do this:

- to steal data
- to disrupt services
- to make money

Hacking can be done using a **brute force attack**. This simply tries possible password combinations to get in to a system. This is much harder if passwords are made more complex.

Hacking is illegal. Hackers can be fined or even end up in prison.

Cyber Security

Malware is **mal**icious soft**ware**.

It might try to:

- disable your computer
- steal your data or passwords
- lock your computer until you pay a ransom

Malware includes **computer viruses**, which spread by copying themselves.
Trojans are a type of malware which looks like a legitimate download but contains a virus or other type of malware.
Ransomware will lock up a system and demand a payment to allow users back in.
Spyware will send data from a system - for example, a keylogger sends the keys someone presses which can be used to steal passwords.

Cyber Security

Social engineering is when someone is tricked into giving up their personal details.
These can then be used to work out passwords.

Phishing is when fake e-mails or text messages contain links to try to get you to give up personal details or enter passwords.

Blagging is when someone tries to convince you to do something you shouldn't. This might be done by a phone call or an e-mail.

Shoulder surfing is when someone looks over your shoulder to get your password or PIN. It can happen at cashpoint machines or with door entry codes.

The most important way to stop social engineering is to **educate people** about the threats. If people know about scammers sending e-mails or texts or phoning people, they are less likely to fall for the scam.

Cyber Security

There are different ways we can protect computers and computer networks:

- firewalls
- anti-virus
- auto-updates
- secure log-in systems
- web browsers
- e-mail systems

Cyber Security

A **firewall** checks data coming in to and going out of a computer. It scans the data to make sure it doesn't contain anything malicious or suspicious.

Anti-virus software scans your computer to check for viruses and other malware. It can quarantine anything it thinks is suspicious.

Auto-updates mean that a computer will download updates regularly. These fix any vulnerabilities so that hackers or malware can't exploit them.

Complex passwords makes them harder to guess or for a brute force attack to exploit. Fingerprint or facial recognition is even better.

Web browsers check that you want to download something from a website. This makes sure that a piece of malware isn't trying to download something malicious without you knowing about it.

E-mail systems warn when an e-mail looks suspicious or that a link might lead to a phishing site. Most e-mail systems have spam filters which put suspicious e-mail in a bin without you having to look at them.