Cyber Security

What does cybersecurity mean?

Cyber:

- Something relating to computers or networks, for example the internet.

Security:

- Freedom from danger and freedom from fear/anxiety. For example downloading an antivirus software.

Cyber security:

- Cybersecurity is the organisation and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems.

The hacking process

Aims and motives of hackers

To conduct cyber attacks for financial gain.

They want to understand where the vulnerabilities lie.

Steal personal information.

Performing corporate espionage (spies to gather more information.

To prove their social, religious, or political views. Usually done by defacement of website.

To stop other hackers from stealing information. These hackers are called white hat hackers. They do this to protect websites and personal information.

Cyber security threats

Phishing:

A legitimate looking email is sent to the user that contains a link to an unsecured website. When the user clicks onto the link and enters their personal details into the fake website, the personal information is stolen by the hacker.

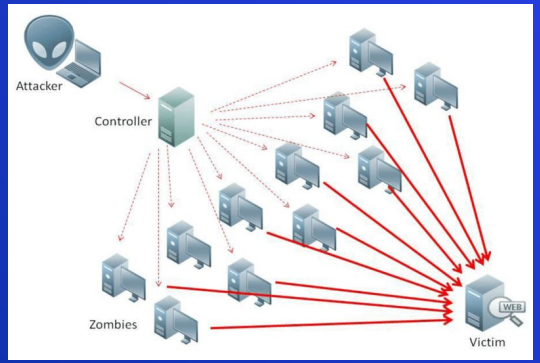
Pharming:

A software is installed on the user's device without their knowledge that redirects the user to a fake website when a legitimate URL is entered. The user is encouraged to enter personal details on the website so that the hacker can steal the personal information.

Cyber security threats

Denial of service attack:

Many requests are sent to the web server from a computer. It becomes flooded with traffic. It can't handle the requests, therefore it fails.



Brute force attacks:

An example of this is guessing passwords. This works by using trial and error where every possible combination of password is tried to enter and steal data.

Cyber security threats

Malware:

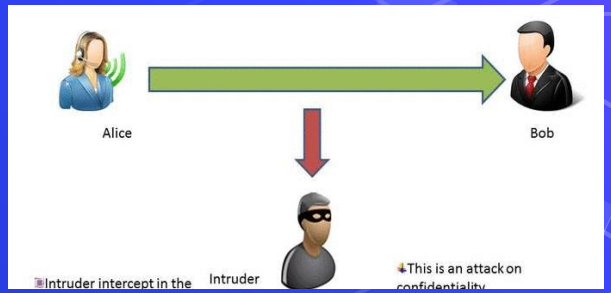
Virus: it can damage programs, delete file, and steal information.

Worm: it spreads copies of itself from computer to computer which could lead to the computer crashing.

Trojan: it is disguised as a real operational programs like a computer game, which enters the computer and can take control over the

Data interception:

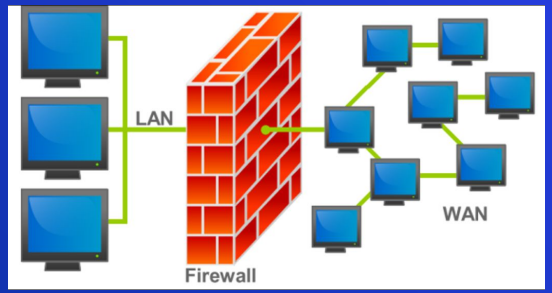
Hackers use a software called a packet sniffer which focuses on the data packets sent around the network. The software gathers the information and sends it to the hacker so the information is stolen.



Solutions to cyber security threats

Firewall:

It monitors the incoming and outgoing traffic in the network. It checks whether the traffic meets the given set of criteria. It can block any traffic that doesn't meet the criteria.



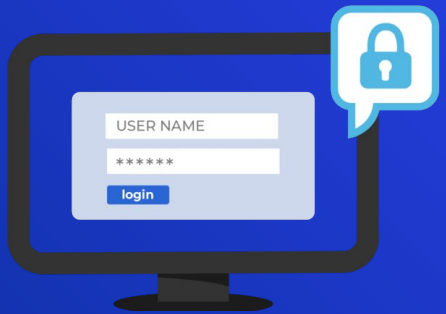
Anti-virus software:

It detect and remove the malware (virus). The anti-virus filters will also help to block spam emails. This software runs in the background and provides protection against virus attacks.

Solutions to cyber security threats

Authentication:

Examples include strong passwords and biometrics. This prevents the hacker from gaining access to the system as its difficult to guess strong passwords.



URL and privacy settings:

- Check the padlock sign next to the URL. And a URL scanner can be used which would detect any suspicious links.
- You could avoid cookies being stored by adjusting the privacy settings to prevent personal information being stored.