

# Protecting computers

In 2022 it is estimated that over £100 billion will be spent on cyber-security across the world.

This is money being spent to keep computers safe.

What is it being spent on? How does it work?

# Protecting computers

Verizon estimates that the main threats are:

Hacking: 2% of attacks

Malware: 28%

Social engineering: 33%

# Protecting computers

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

# Protecting computers

## Firewalls:

A firewall is a piece of software that checks data coming in to and going out of your computer.

It scans the data to make sure it doesn't contain anything malicious or suspicious.

Sometimes firewalls will stop you downloading things from some websites.

# Protecting computers

## Anti-virus software:

Anti-virus software scans your computer to check for viruses and other malware.

It can quarantine anything it thinks is suspicious.

Hundreds of new malware threats are identified every day, so it's important to keep anti-virus software up to date.

# Protecting computers

## Auto-updates:

Your computer will probably download updates to the operating system fairly regularly.

These fix any vulnerabilities in the system so that hackers or malware can't exploit them.

Having auto-updates turned on means that your device should always have up to date protection.

# Protecting computers

## Secure log-in systems:

Using passwords which are more complex makes them harder to guess or for a brute force attack to exploit.

Fingerprint or facial recognition is even better.

CAPTCHA makes sure it's a person and not a bot

Two-factor authentication can also help

# Protecting computers

## Web browser:

Your web browser might ask you to check that it's OK to download something from a website.

This is to check that you know that there are risks and to make sure that a piece of malware isn't trying to download something malicious without you knowing about it.

# Protecting computers

## E-mail systems:

Your e-mail systems might warn you that an e-mail looks suspicious or that link might lead to a phishing site. This helps make sure you don't download something malicious.

Most e-mail systems have spam filters which put suspicious e-mail in a bin without you having to look at them.