WHAT IS A
FIREWALL?

Firewalls monitor connections travelling to and from the network and blocks any connections that are unauthorised.

They act a bit like a bouncer at a nightclub, if someone underage tries to get in they are turned away. So for example, when you browse the internet, everything you search for gets checked by the firewall first before it gets to your computer. If the website is unrecognised or harmful you will be blocked from access; and similarly if an intruder tries to break in, they will be blocked from access; the same with malware.

Firewalls have a set of rules to check against, which helps to determine what action it should take. You can update these rules so that the firewall works around your circumstances, allowing trusted content to get through with ease, or stick with the default options, which will block everything apart from exceptions.

There are software firewalls, which protect the device it's installed on.

Windows and Apple Operating Systems have built in firewalls, you just need to make sure it is turned on. Or you can invest in a third-party provider- firewall settings are often part of an antivirus package. Software firewalls are great if you are working on the move. Hardware firewalls sit between your devices and the internet, or a network you want to be protected from, but once you leave the premises your device is no longer protected.

Antivirus Extra Features

The primary purpose of antivirus is to detect and remove malware. Standard features found on reputable platforms include:

- Realtime scanning of systems
- Automatic updating of the platform
- Quarantine of harmful files
- Report on findings

There is built in antivirus for Windows and Apple Operating Systems, you just need to make sure it is switched on, or you can invest in a third-party provider. Antivirus can offer a whole host of extra features, often as part of free packages and occasionally at extra cost. Do your research and identify an antivirus that is best suited to your organisation's needs and budget. You may find you have many security controls in place with only one tool!
Here are some of the many features antivirus platforms have to offer:

1 Safe Web Search

Blocks you from reaching known malicious websites when browsing the internet, this includes malware infected websites and scam websites looking to steal personal information.

2 Removeable Media Scan

On insertion of removeable media, the software will scan for malware before allowing you to open the inserted media.

3 Application Firewall

A firewall monitors and blocks unauthorised connections to the network.

4 Built-in Password Manager

Saves the password for your online accounts and automatically applies them each time you login. This feature encourages more complex and unique passwords for every account. Password Managers will only provide login details for the legitimate website to which you signed up, preventing copycat websites from stealing your credentials.

Antivirus Extra Features

5 VPN Services

Provides a secure network connection that encrypts data as it travels across the network.

6 Individual File Scan

Checks independent files for malware. This is particularly helpful when you receive an attachment or need to download a file.

7 Webcam Protection

Blocks unknown and malicious applications from trying to access your camera without your consent.

8 Cloud storage

A backup facility to store data separately from your network.

9 Dark Web Scanning

Scanning the dark web for any personal information, financial information and credentials, notifying you of its presence should anything be found. You have the option to investigate the alert and take the necessary action to prevent ongoing repercussions. Actions could include updating information, particularly credentials; securing vulnerable areas by implementing 2-setp verification and strengthening privacy settings; and informing "need to know parties" (such as your bank).