

Software Updates and AntiVirus

Why? To protect from malware – aka Malicious software – aka viruses and spyware.

What? Malware is the catch-all term used to describe any sort of software or web-based content that can damage your personal and business IT system. The most well-known are viruses which automatically replicate themselves within your system to cause chaos and steal information. The software is clever enough to recognise things like passwords, bank or credit card details and can even transfer control of your computer to the hacker. Sometimes the hacker will demand a ransom in return for restoring your system. In this case, never agree to pay the ransom. You have no guarantee of it working and will be more liable to future attacks.

Who? It can target anyone. The use of Malware is rarely personal. Similar to the practice of phishing, malware will frequently be targeted at many thousands of systems with the objective of accessing those with the weakest cybersecurity.

Must Do:

- Anti-virus software should be enabled on all machines. Most of the time it comes already loaded onto the device. But you must make sure the option to use it is turned on.
- Make sure that all your devices have enabled 'auto-update' for the software updates (aka patches) provided by the software developers. These updates are produced in response to recently identified weak spots or in anticipation of new viruses being circulated.