THE FIVE CORE CONTROLS OF CYBER ESSENTIALS – SECURITY UPDATE MANAGEMENT

SECURITY UPDATES

Security Updates

What are the Cyber Essentials controls?

Don't let software vulnerabilities be the access point for criminals.

Check that your software is still supported by the vendor.

Enable your software to automatically update or apply the patches within 14 days.

www.ncsc.gov.uk/cyberessentials

CYBER ESSENTIALS

Prevent cyber criminals using the vulnerabilities they find in software as a way to get into your system.

If hardware is the computer's physical components, software is the set of instructions or programs that 'run' on a computer. There are three main categories of computer software:

- **System software** is what is used to manage a computer, an example being the operating system which might be MacOS, WindowsOS or AndroidOS.
- **Firmware** is the software that is installed on all devices, including routers, modems, computers and mobile devices.
- **Application software** is any programme that enables the user to complete tasks. Every programme that you use on your device is application software. Examples are Microsoft Word, Excel, internet browsers such as Google Chrome and Safari and video games.

Software is made up of thousands of lines of code which is how the computer interprets information to complete its functions. In every 1000 lines of code there is on average 10-15 errors. Most of these errors are not noticeable to you as the user, however, each error is a potential opening for cyber criminals to access your data. These openings are often called 'vulnerabilities'.

Within a piece of software's functioning life span, as soon as an error or 'vulnerability' is discovered, the manufacturer creates some additional code to correct and close the opening. This is known as 'patching' or security updates. All modern software will need to 'update' on a regular basis as part of its maintenance which ensures that vulnerabilities are patched within 14 days of the update, and other 'bugs' (faults) corrected.

Unsupported software

When software that is considered 'end of life' or no longer viable with modern technology, the manufacturer will cease to create security updates. This means applications becomes a 'legacy software' and is no longer supported and therefore no longer secure. Not only are the vulnerabilities left un-patched, but they become common knowledge for hackers, and therefore easy to exploit. It is important to replace all software with a supported version and remove any software prior to it becoming unsupported.

Automatic updates

In the System Preferences setting you can find 'software updates' and enable automatic updates. This will ensure that as soon as software manufacturers release their security updates, your computer will apply them automatically and you will be protected from known security issues.

Manufacturer approved software

You should only use software that is from an official source that is approved by the manufacturer/vendor. This way, you can be confident that the thousands of lines of code are not designed to harm your device or data. Some examples of official sources include the Google Play store and the Apple app store. Software acquired from questionable sources may be counterfeit and unlicensed. Not only will it be of an inferior quality and unable to receive ongoing support, but there is also a high chance it will contain malware.

How can it help prevent a cyber attack?

There has been a significant rise in cyber attacks probing for unpatched software vulnerabilities, with hundreds of thousands of automated scans and attacks per day. Hackers can access computers through one of the vulnerabilities that they find on an automated scan and use this to develop an exploit that would allow them to gain access and steal or alter information or deliver malware such as ransomware.

Check that your software is still supported by the manufacturers i.e. is continuing to receive security updates and look in settings to enable your operating system and other software to automatically update or apply the software patches.

Find out more about getting Cyber Essentials certified here.