THE FIVE CORE CONTROLS OF CYBER ESSENTIALS – MALWARE PROTECTION

Identify and immobilise viruses or other malicious software before it has a chance to cause harm.

Malware is short for malicious software, which is software that is designed to cause harm by disrupting, damaging or gaining access to a computer, without the owner's knowledge. Malware typically consists of code developed by cyber attackers, designed to cause extensive damage to data and systems, or gain unauthorised access. Viruses, worms, spyware and ransomware are all different types of malware.

A common way that malware could get onto your computer is through a phishing attack. This could be in the form of an email from someone pretending to be your bank or another trusted institution. The email will generally ask you to open an attachment or click on a link, and if you do, it will try to install the malware onto your device. If you are using your computer with a regular user account as opposed to an administrator account, any malware will not be able to download without the administrator password.

Other common ways to infect a computer device with malware is through clicking on an advert that appears on a website, or downloading software from a non-manufacturer approved source. Your computer could also be infected with malware from a removable storage device such as a USB stick, many companies have banned USBs for this reason.

Protecting your devices – anti-malware software

Many operating systems have anti-malware already installed. Windows 10 has a product called 'Defender' which will help make your computer safer from malware. Apple was previously considered to be a 'safe' bet and immune from virus'. This is certainly no longer

the case and despite modern Apple OS containing anti-malware mechanisms, they only protect a small sub-set of applications and the packages that provide protection do not update frequently. It is necessary to purchase a third party anti-malware software to be fully protected.

Anti-malware software will monitor your device for any malicious activity, if it finds anything, it will destroy it before it causes any harm! There are many anti-malware products available to download on a subscription arrangement. Some are even free. McAfee, AVG and Sophos are just a few well-known names. A good anti-malware product will update its virus and threat protection on a daily basis. It must be noted that there are no true anti-malware software solutions available for mobile devices, so an alternative method must be considered to protect these.

Additional tools to protect yourself from malware

List of approved software

This can be applied through technical controls like a Mobile Device Manager or through written policies where lists are provided to staff of what is and isn't allowed to be added. A list of approved software can be created in the security settings and software not listed, especially malware, cannot be added to your device. You can adjust this list as your needs change. Certain operating systems have options to allow software only from reputable sources, like the official Apple Store and identified developers only.

Sandboxing

Malware tries to steal or damage as much of your data as possible. To limit the amount of data that malware can potentially impact, you can run each application in an isolated area called a 'sandbox'. This means that malware won't be able to reach anything outside of its sandbox or anything inside another sandbox.

This may sound complicated but some of your applications like your web browser are probably in a sandbox already. Google Chromebooks have an operating system that relies on sandboxing as their primary anti-malware protection, Microsoft Edge sandboxes all processes and Apple's Safari browser runs websites in separate processes.

How can it help prevent a cyber attack?

The majority of malware is created to make money illegally through fraud, extorsion and identity theft. Anti-malware can help prevent malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer.

Another way you can prevent malware from trying to secretly attack you, is by disabling Autoplay and Autorun. This will be effective in stopping malicious software from automatically opening. Separating day to day user accounts from privileged access administrator accounts will also reduce the risk of malicious software being able to install itself.

Find out more about getting Cyber Essentials certified here.