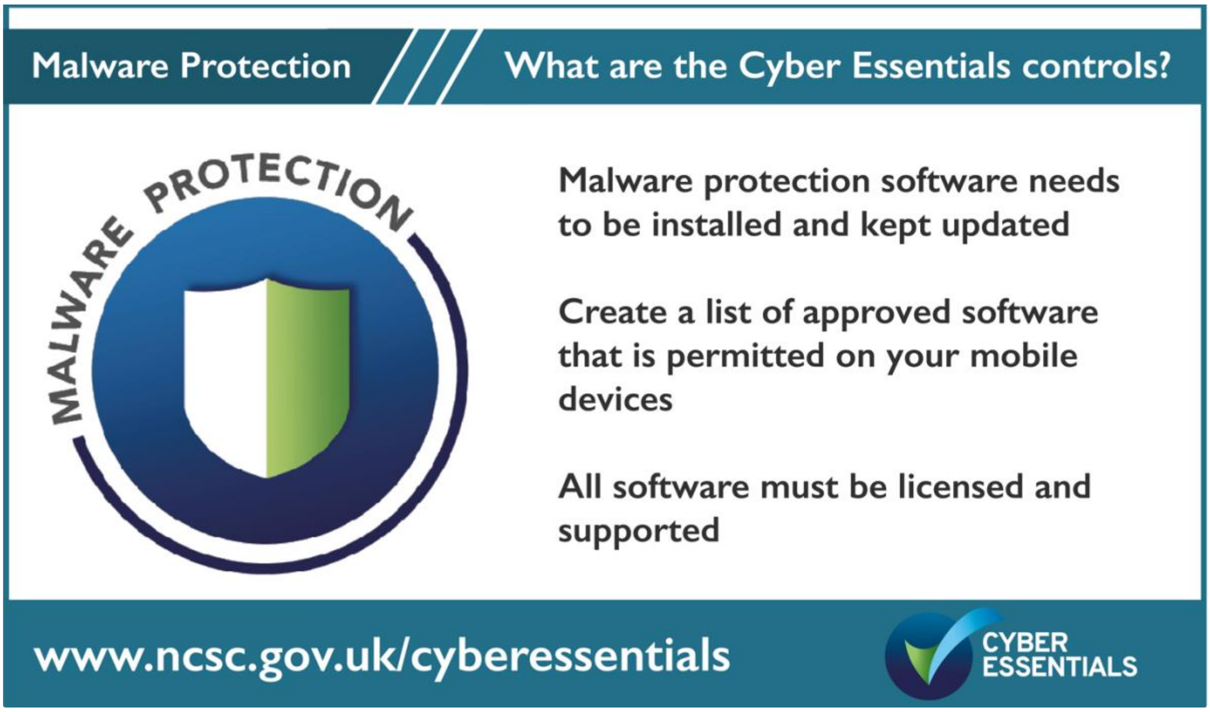
July 2023



Malware Protection

What are the Cyber Essentials controls?

Malware protection software needs to be installed and kept updated

Create a list of approved software that is permitted on your mobile devices

All software must be licensed and supported

www.ncsc.gov.uk/cyberessentials

MALWARE PROTECTION
CYBER ESSENTIALS

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

What is malware?

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, trojan horse, spyware, adware and ransomware are all different types of malware that cause harm in different ways.

To combat these threats, Windows and macOS devices must have a malware protection software program (sometimes called a solution) installed. This program needs to be set to detect and prevent malware from running. Please note that although a virus is just one type of malware, ‘antivirus’ is a commonly used term interchangeable with anti-malware (software) and will combat all types of malware.

For all other devices, smartphones, tablets, Chromebooks etc., you should only use apps that are from a recognised app store and maintain an approved list of trusted apps for carrying out your organisation's work.

How does malware get onto my device?

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, 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.

Protect your laptops, servers and desk top computers with malware protection software

Many operating systems have malware protection software already installed. Windows 10 has a product called 'Defender' which meets the requirements set out in Cyber Essentials. Apple devices were previously considered to be a 'safe bet' and 'immune from viruses'. This is certainly no longer the case and, despite modern Apple Operating Systems containing malware protection mechanisms, it is strongly advised that people use an additional third-party program to ensure maximum security.

Malware protection software will monitor your device for any malicious activity, if it finds anything, it will destroy or secure it before it causes any harm. There are many malware protection products available to download on a subscription arrangement. Some are even free. McAfee, AVG and Sophos are just a few well-known names.

Malware is continually evolving so make sure your malware protection software is set up and configured in line with the vendor's best practise.

Most malware protection software is set to scan files automatically upon access, this means that before any file is downloaded, it will be scanned for malware. Although this is often the default setting, it is worth checking this setting in the software configuration screen.

Malware signature detection is a method of virus detection that involves identifying malware by comparing code in a program to the code of known virus types that have already been encountered, analysed and recorded in a database.

Heuristic detection was developed to spot suspicious characteristics that can be found in unknown, new viruses and modified versions of existing threats. Heuristic analysis is incorporated into malware protection software to detect new threats before they cause harm.

Your malware protection software should have the option for your internet browser to scan web pages you visit and prevent access to known malicious websites. Make sure this is enabled. On Windows 10, SmartScreen can provide this functionality.

Protect mobile devices

For mobile devices, malware protection strategy focuses almost entirely on controls or polices that dictate which applications or apps you allow to be installed on devices that access organisational data and services.

- Only apps which have been **application signed** and provided by the official app stores can be installed.
- Only apps from an **approved software list** can be installed. An approved software list is a list maintained by the organisation identifying reputable trusted sources from which software can be downloaded. This typically includes the Google Play Store and the Apple App Store.

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.

The five controls of Cyber Essentials are:

- User Access Control
- Security Updates
- Secure Configuration
- **Malware Protection**
- Firewall and Routers

Help and support

There are over 300 specially trained cyber security companies around the UK who are licensed to certify against the Government's Cyber Essentials Scheme. They can offer help and support in preparation for the assessment. Find one near you.

For questions and feedback about the Cyber Essentials scheme, contact IASME at info@iasme.co.uk or Tel: 03300 882 752