

**About malware**

**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.

**How does malware get onto my device?**

A common way that malware could get onto your computer is through a phishing attack. (see guidance [about phishing](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-phishing/)) 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. (see guidance on [about accounts](https://getreadyforcyberessentials.iasme.co.uk/guidance/about-accounts))

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.

**Different types of malware and what they can do**

There are many different forms of malware that cause all sorts of different issues.

**Viruses:** A virus self-replicates and causes problems by damaging programmes and files, this may result in users being unable to access data and possibly becoming locked out of their device. The damage is sometimes irreparable!

**Worms:** This type of programme copies itself and spreads itself to other connected devices on the same network.  Worms cause network systems to slow down by eating up free space, they can also modify or delete files. A device firewall can prevent worms spreading throughout a network.

**Trojan Horse:** With reference to the ancient story of Troy, where Greeks infiltrated the walled city by hiding in a giant wooden horse, this programme sneaks into a device by pretending to be a legitimate programme. A Trojan is designed to damage and also steal data.

**Spyware:** As the name suggests, this software is created to spy on a user! It can gather data held on a device without a user’s knowledge and send it back to the infiltrator**.** This might be web pages that have been visited where personal details have been entered such as credit card details.

**Adware:** This programme is designed to pop up advertisements.  The advertisements are uncontrollable and tend to pop up frequently on screen, it is often difficult to close them.

**Ransomware:** This is a form of malware that encrypts a user’s files. (scrambles the data so it cannot be understood) A payment is demanded via an online process in order to unlock the files, however, it cannot be guaranteed that you will be able to access your files even if you do pay the ransom.

**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, it is strongly advised that users use an additional third-party program to ensure maximum security.

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.

**Additional important tools to protect yourself from malware**

**List of approved software**

Known as a software restriction policy, and found in your security settings, you can create a list of approved software that is permitted on your device. 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.

**Disable autorun**

You can prevent software from automatically opening by itself by disabling Autoplay and AutoRun. This will be effective in stopping malware from trying to secretly attack you. Instead, you will be notified that some software wants to run and you can decide whether to allow it.

**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.

**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 Chrome has been sandboxed since the beginning, Microsoft Edge sandboxes all processes and Apple’s Safari browser runs websites in separate processes.

**Best practice for preventing malware**

* Install anti-malware software.
* Only use manufacturer approved software.
* Only use software that is supported and applied latest patches.
* Create an approved list of software that you use on your device
* Disable Autoplay and AutoRun on your device.
* Run each application in a sandbox.