

**Cleaning Infected Machines**

September 2021

Version 1.0

**Table of Contents**

[**1.** **Computer Viruses** 3](#_Toc83737206)

[**2.** **Antivirus Software** 3](#_Toc83737207)

[**3.** **Symptoms of Infection** 3](#_Toc83737208)

[**4.** **Disconnect the Device** 3](#_Toc83737209)

[**5.** **Use Safe Mode** 4](#_Toc83737210)

[**6.** **Backups** 4](#_Toc83737211)

[**7.** **Delete Temporary Files** 4](#_Toc83737212)

[**8.** **Run Anti-virus / Malware Scans** 5](#_Toc83737213)

[**9.** **Homepage Settings** 5](#_Toc83737214)

[**10.** **Update Your Devices** 5](#_Toc83737215)

[**11.** **Audit Software Programs** 5](#_Toc83737216)

[**12.** **Reset Compromised Credentials** 5](#_Toc83737217)

[**13.** **Windows Registry** 5](#_Toc83737218)

[**14.** **Clean-up Tools** 6](#_Toc83737219)

[**15.** **Removing Viruses from a Mac** 6](#_Toc83737220)

[**16.** **Email Viruses** 6](#_Toc83737221)

[**17.** **Windows Corruption** 6](#_Toc83737222)

1. **Computer Viruses**

A computer virus is a type of malware (malicious software) designed to make copies of itself and to spread through any connected devices/networks. When a computer virus infects your computer, it may slow it down and stop it working properly.

Your computer could become infected from removable media, like USB sticks, downloaded files from the internet or emails with infected attachments, or clicking spam email links.

Viruses can be classified according to the method that they use to infect a computer:

* File viruses
* Boot sector viruses
* Macro viruses
* Script viruses

1. **Antivirus Software**

Computer viruses are almost always invisible, and without anti-virus protection you may not know you have one. Install anti-virus protection on all your devices.

Antivirus software helps prevent viruses and malware from infecting your device and putting your data at risk. Antivirus software should be installed, set to update automatically, and be actively monitored.

Antivirus and malware protection are a vital security measure and a requirement of Cyber Essentials certification.

1. **Symptoms of Infection**

* Pop-up messages
* Slower boot up or processing speed
* Icons that you do not recognise indicating unauthorised apps or programs
* Apps or programs crashing repeatedly for no apparent reason
* Louder noise from device fans / overheating
* Web browser freezing or becoming unresponsive
* Web pages redirecting to sites you are not intending to visit

1. **Disconnect the Device**

Computer viruses use connections to spread, so disconnect from the internet and network to prevent further damage.

1. **Use Safe Mode**

* Remove CDs and DVDs, and unplug external drives, such as USB drives from your computer. Then shut down.

If any malware is programmed to automatically load when Windows starts, entering safe mode may block the attempt.

* When you restart, **hold down the F8 key before** the Windows logo appears. This should bring up the Advanced Boot Options menu.
* Use the arrow keys to highlight Safe Mode (or Safe Mode with Networking if you need to use the Internet to solve your problem), then press Enter.

1. **Backups**

If you have a backup system in place that automatically backs up your files or system, consider running virus scans on the backups to confirm that they didn’t inadvertently save infections.

If you suspect an infection, consider an **additional** file backup, particularly if your last full backup was some time previously. Be wary of backing up program files, as infections are more likely to be present. Any additional backup must not overwrite previous scheduled backups and should be on **different** backup media.

1. **Delete Temporary Files**

Some viruses are programmed to initiate when the computer boots up.

Use ‘Disk Clean Up’ to delete temporary files:

1. Click the Windows logo or click in the ‘search box’ on the bottom of the task bar.
2. Type ‘Temporary Files’
3. Choose ‘Free up disk space by deleting unnecessary files’
4. In the ‘Files to delete’ select ‘Temporary Internet Files’
5. Click OK
6. Confirm ‘Delete Files’

Deleting temporary files may remove the virus, but it is not safe to assume this is the case.

1. **Run Anti-virus / Malware Scans**

If your on-demand scanner finds an infection, the result will be confirmed via a report informing you what has been found and confirming if the infection has been quarantined / removed.

Some scans may deem legitimate programs as suspect. If you recognise them, you can add them to an exclusions list.

Once you have deleted or quarantined, run the scan again to be sure before restarting your computer into ‘normal’ mode.

1. **Homepage Settings**

Check the homepage settings in the window of your browser.

Whilst malware infections can damage system files, they can also change the homepage on your web browser to display pop-ups, adverts, and make browsing virtually impossible.

1. **Update Your Devices**

Update your operating system, browser, and applications. If there is an update available, ensure you install it. This is known as ‘patching’ and it is an essential part of protecting your systems.

1. **Audit Software Programs**

Audit the software on your systems regularly, updating your software inventory and deleting any programs you no longer use. This reduces the risks to your systems and limits the number of programs malware might utilise to gain access.

This is also a requirement of Cyber Essentials.

1. **Reset Compromised Credentials**

Malware may capture passwords. If you think accounts have been compromised, you should reset all known passwords.

1. **Windows Registry**

Your Windows registry holds details on everything you do on your PC. Registry cleaning should only be undertaken by a professional, as if errors are made it is necessary to reinstall the operating system.

1. **Clean-up Tools**

As well as anti-virus and malware protection, software vendors produce a range of tools to help protect devices and data. If you decide to utilise one:

* Research any potential tools and choose a reputable supplier.
* Do not connect to the internet to download tools with a machine you believe to be infected.
* Do not be tempted to click on any alerts or pop-ups suggesting quick fixes or guaranteeing solutions from given websites.

1. **Removing Viruses from a Mac**

There is a common misconception that Mac computers can’t become infected with a virus. Unfortunately, whist there are fewer viruses that target Mac computers, Mac viruses do exist.

Macs, iPhones, and Android phones can all be affected by malware and anti-malware scans can be run on these devices as well.

If you think your Mac has a virus:

1. Quit the application or software that seems to be affected.
2. Go to ‘Activity monitor’ and search for known Mac viruses such as ‘MacDefender’, ‘MacProtector’, or ‘MacSecurity’.
3. If you find one of these viruses, click ‘Quit process’ before quitting ‘Activity monitor’.
4. Next, go to your ‘Applications’ folder and drag the file into your ‘Trash’.
5. Remember to empty the ‘Trash’ folder afterwards to permanently delete the virus.
6. Now make sure your software and apps are up to date to benefit from the latest security patches.
7. **Email Viruses**

Your computer can become infected with a virus via email, but only if you open attachments within a spam email or click on the links contained in them.

If you receive a spam email mark these as spam or junk and ensure they are deleted. Report suspicious emails following [advice from the NCSC](https://www.ncsc.gov.uk/information/report-suspicious-emails).

1. **Windows Corruption**

If Windows won’t start or work well enough to permit you to back up your files, you may need to reinstall Windows.

Reinstalling Windows will also mean you need to reinstall the programs on the device from discs or download them which have been installed.

Software as a Service (SaaS) applications will be unaffected.