National Cyber Security Centre

Protecting devices

From viruses and malware

This page contains tips about how to protect your computers, laptops, smartphones and tablets from the damage caused by viruses and other types of malware. Following these steps will help keep your devices - and the information stored on them - free from harm. For more information, please refer to **www.ncsc.gov.uk/antivirus** .

Viruses are a type of malicious software that can harm devices such as computers, laptops, smartphones and tablets.

Once your device has been infected, this **mal**icious soft**ware** (also known as **malware**) can steal your data, erase it completely, or even prevent you from using your device.

Devices can become infected by accidentally downloading an email attachment that contains malware, or by plugging in a USB stick that is already infected. You can even get infected by visiting a dodgy website.

For these reasons, it's important that you **always use antivirus software on your laptops and PCs**. Smartphones and tablets don't need antivirus software, provided you **only install apps and software from official stores** such as Google Play and Apple's App Store.

Turn on your antivirus product

Antivirus (AV) products detect and remove viruses and other kinds of malware from your computer, laptop or MAC, and should always be used.

Make sure your AV product is turned on and up to date. Windows and iOS have built-in tools that provide suitable AV.

New computers often come with a trial version of additional AV software. You may want to carry out your own research to find out if these products are right for you.

Make sure your AV software is set to automatically scan all new files, such as those downloaded from the internet or stored on a USB stick, external hard drive, SD card, or other type of removable media.

You don't need AV products on your smartphone or tablets, provided you only install apps from official stores.

If you think your computer has been infected, open your AV software, and run a full scan. Follow any instructions given.

If you receive a phone call offering help to remove viruses and malware your computer, hang up immediately (this is a common scam).

Keep all your IT devices up to date

Don't put off applying updates to your apps and your device's software; they include protection from viruses and other kinds of malware.

Applying software updates is one of the most important things you can do to protect your devices. Update all apps and your device's operating system when you're prompted.

Set all software and devices to update automatically, including your AV software.

You should consider replacing devices that are no longer supported by manufacturers with newer models. You can search online to see how long your current device will be officially supported.

Only install official apps

Download on the App Store

GET IT ON Google Play

Only download apps for smartphones and tablets from official stores (like Google Play or the App Store). Apps downloaded from official stores have been checked to provide protection from viruses and malware.