

7 - AntiVirus Software

What precautions should I take against getting a virus?

If you receive a suspicious email containing an attachment, be cautious even if it comes from someone whom you know. The safest option is to delete the message immediately

WARNING: NEVER open an unexpected attachment without scanning it first.

You should also check USB pen drives before opening files, especially if they have been used outside of the university on a PC attached to the internet.

To safeguard your work against potential virus damage, backup your files at regular intervals to your H: drive.

Files stored on the H: drive of workarea computers are backed up each night

What antivirus software is available on Windows 10 workstations?

The antivirus software available on the Windows 10 workstations is Microsoft Defender.

Antivirus for Managed Devices - Linux and Macs

Linux - IDG Managed Linux devices are protected by ClamAV

Managed Macs are enrolled in Jamf and have an extra layer of protection from Jamf Protect (in addition to macOS XProtect)

Antivirus for Semi-managed university owned devices

Windows 10 and 11 have Microsoft Defender Anti-Virus already built in
macOS includes built in antivirus technology called XProtect

Linux users are advised to download and install ClamAV

Antivirus for Personally owned devices

Windows 10 and 11 have Microsoft Defender Anti-Virus already built in

macOS includes built in antivirus technology called XProtect

Linux users are advised to download and install ClamAV

What are hoax viruses?

Hoax viruses are email messages containing information about non-existent virus threats. If you receive one of these messages, read it carefully. If it tells you to warn everyone you know, it's almost certainly either a hoax or out of date. It's best to delete these emails as soon as they are received. **Don't forward it to anyone.**

If you receive an email with a short subject line, no body text or just a web link or an attachment, even if it comes from someone you know (unless they have made you aware they are sending it), **delete it as it may contain a virus.**

How will I know if it is a hoax?

A hoax would often contain the following indicators within the email: Message gives an impression of high urgency and desperation (e.g. use of capital letters, excessive exclamation marks etc.).

It tells you to forward the message to as many people as possible.

Provides details on how to remove the threat, often referring to specific system files that exist on your computer.

What is adware, spyware and malware?

If you see popup messages when browsing the internet, or your computer has suddenly become slow, you may have adware, spyware or malware which has not been detected by your antivirus software. This may have been downloaded when browsing websites. Adware may appear as advertising slogans or popup messages. Spyware or malware is a type of program that may have been installed when you download freeware, and may collect information about your browsing habits.

IT Services Help Desk

✉ helpdesk@warwick.ac.uk

🖥 warwick.ac.uk/its