Quick Guide: Cleaning viruses with Sophos Anti-Virus

This quick guide describes how to clean viruses and other malware from your PC using Sophos Anti-Virus

What is a virus?

A virus is a computer program that can spread across computers and networks by making copies of itself, usually without the user’s knowledge. In recent years they have been more of a criminal intent than malicious, aiming at stealing your banking details or personal information.

All PCs managed by IT Services have Sophos Anti-Virus installed. This is available for free to all departments, and may also be used on the home PCs of staff and students as part of our site licence.

If you find a virus on your PC, or suspect that there is one, you should act on it by following the instructions in this guide.

Checking your PC for viruses

1. First of all, check that Sophos is fully up to date by right-clicking on the shield and selecting Update now. The shield will pulse as it updates and then return to blue. If a cross appears then the update has failed (see over).

2. If you use USB storage devices, ensure that they are plugged in and recognised by the PC.

3. For Windows PCs, right-click on “My Computer” (Windows XP and earlier) or “Computer” (Vista and later) and select Scan with Sophos Anti-Virus. For Macs, click on your Sophos shield icon and select Scan This Mac.

4. A virus scan will now begin. This will take a while so leave it to finish.

5. When the scan is complete you will see a summary screen. Any detected items will be placed in your Quarantine manager. Click on the blue Quarantine text to see them.

Removing Viruses

Within Quarantine manager, you will see one detected item per line with a list of available actions for this item which may include:

a) Clean up – disinfect the files, if possible (this will be your most likely choice). This will leave the files intact but will remove the virus from them.
b) Move – move the infected files to a specified location (e.g. a USB stick to give a sample to ITS).

c) Delete – delete all infected files (not recommended if system files are infected or your PC may not turn on again).

d) Authorize – allow the quarantined files to run (not recommended unless you are absolutely positive that this is a false detection).

To select an available action, tick the box next to the item and then at the bottom right press the Perform action button. Make your choice from there.

Sometimes there is not an option to Clean up. This means that Sophos didn’t find all infected files on its first attempt and you should run a second full scan of your computer. If a second scan still doesn’t allow you to Clean up, this means that Sophos doesn’t know how to clean it up yet and you should try again the next day when new updates are available.

What should I do if my updates fail?

If you check for updates and a cross appears on your shield, first of all check that your network connection is active by browsing to the University home page (for example) and then clicking on your browser’s refresh/reload button. If you cannot display a web page then it’s likely that Sophos can’t update because there is no network connection.

If you can connect to web pages but Sophos still won’t update, run a full scan as described elsewhere in this document and attempt to clean up any detected viruses. Then reboot your PC and try to update again.

Sophos has detected items which aren’t viruses

Sophos Anti-Virus now also detects other malware which it categorises as follows:

- **Adware** – software whose aim is to extract money from you somehow, usually by convincing you to buy software you didn’t need or want. It is extremely rare for adware to be useful to you so it should often be uninstalled or deleted.

- **PUAs (“potentially unwanted applications”)** – software whose aim is to piggyback a legitimate software installation in order to get installed themselves. These can be applications you intended to install, but Sophos has decided it’s worthless as a precaution.

- **Suspicious behaviour** – software which acts like a virus but may not be, for example by having a badly behaved installer. If it’s something you specifically installed then you should Authorize it, otherwise uninstall it.

For these categories of malware it is up to you to decide if it’s unwanted, and you should either uninstall it if you don’t want it or Authorize it from within Sophos quarantine if you do. Whereas viruses are always bad, some software is merely annoying but not necessarily annoying to you.

For further information, please contact:

**IT Services**

Email: its-help@reading.ac.uk