Information Security: Windows Defender on PCs

The University of Aberdeen uses **Windows Defender** to protect servers and networked Windows PCs against viruses, spyware and other malicious software.

Malicious software can try to install itself on your computer any time you connect to the Internet, or when you install a program using a USB drive, or other removable media. Once installed, it may not be immediately apparent as it can be programmed to run at unexpected times.

Windows Defender prevent malicious software from infecting your computer via:

- **Real-time protection**
  By default, Defender is configured to monitor your computer all the time and will alert you when a virus or other malicious software attempts to install or run on your computer.
- **Automatic scan**
  A full system scan is scheduled to run automatically within the maintenance window on all University computers.
- **Manual scan**
  You can also manually set Defender to scan your whole PC or specific drives, files or folders for potential threats that might put your computer at risk.

Common symptoms of an infection

The presence of malware on your computer may not always be immediately obvious, so it's important to run regular scans; however, some of the more common symptoms are listed below.

- New toolbars, links, or favourites that you did not intentionally add to your web browser.
- Your home page, mouse pointer, or search program changes unexpectedly.
- You type the address for a specific site, such as a search engine, but you are taken to a different website without notice.
- Files are automatically deleted from your computer.
- Your computer is used to attack other computers.
- You see pop-up ads, even if you are not on the Internet.
- Your computer suddenly starts running more slowly than usual.

Status icon

The Windows Defender status icon is located at the right-hand side of the Windows taskbar. It changes appearance according to the state of the software and whether it has detected any potential threats.

Icon	Status
	Defender is up to date. It is unlikely that harmful or unwanted software is present. This should be the normal working status of Windows Defender.
	This indicates that Defender has stopped working either due to: – An infection by malware with a high severity rating. – It has not been updated for an extended period.

If a virus or other malicious software is detected

Notification message

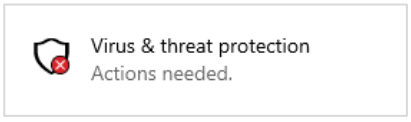
As soon as real-time protection detects a virus or other malicious software, a notification message appears in the bottom right-hand corner of your computer screen.

For example:

Windows Defender status icon change

The Windows Defender icon on the taskbar changes from  to 

If you click on that icon you will see:



Automatic cleaning

Windows Defender will automatically clean your computer and display a green status icon once the threat has been removed.

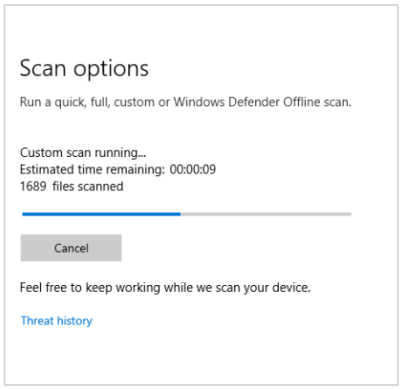
Note: If you connect a USB drive to University classroom or Lecture Theatre PC, any virus-infected file on your USB drive that is identified by the University's anti-virus software as being high risk will be automatically deleted from your device.

Manual scan of a custom location

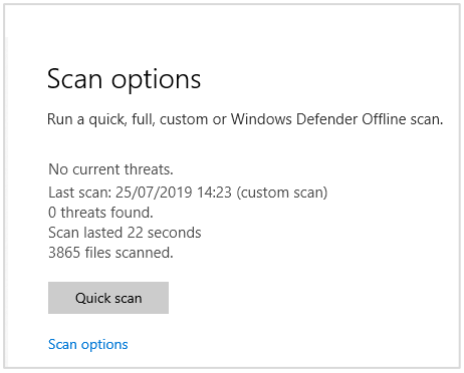
If you are concerned that one of your files or folders or USB drives may be infected, you can run a Manual scan.

1. From **This PC** or **File Explorer**, browse to the location of the file, folder or drive to be scanned.
2. **Right-click** on the file or folder or drive.
3. Select **Scan with Windows Defender** from the pop-up menu.
4. Scanning will begin.
5. You may see an indication of the progress of the scan.

Note: if it you choose a small file or folder the scan can appear to happen instantly.



6. Once the scan is complete a summary of the scan findings will appear.

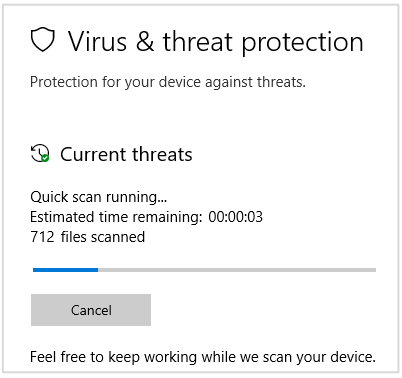


Quick or Full scan of PC

Windows Defender is set to automatically scan for threats and you should not have to take any action.

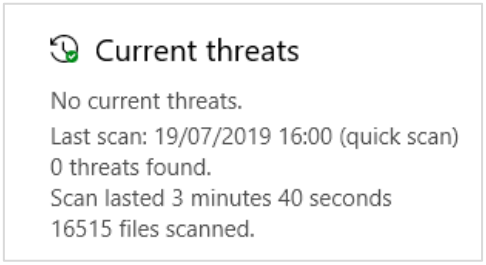
However, if you are concerned and want to run a Quick or Full scan on your PC.

1. Click on the **Windows Defender** status icon in your task bar.
2. Click **Virus & threat protection**
3. Click **Quick scan**
4. The scan will start immediately. You will see the progress bar and note of number of files momentarily on the screen as Windows Defender scans each of the files on your PC in turn.
5. To abandon the scan, click **Cancel**.



If a Quick scan does not detect any problems but you still suspect that there is a virus infection on your PC:

1. Select **Scan options**
2. Choose **Full scan**
3. Click the **Scan now** button.
4. Once a scan is complete, the Home screen will appear with a summary of the scan.



Further information and help

If a virus or threat does not seem to have been automatically cleaned by Windows Defender or you have any concerns about the security of your PC contact servicedesk@abdn.ac.uk for advice.

Alternatively use MyIT to report an issue to the IT Service Desk: https://myit.abdn.ac.uk