Crime prevention advice for

Malware and Ransomware

What is malware?

Malware is malicious software, which - if able to run - can cause harm in many ways, including:

- causing a device to become locked or unusable
- stealing, deleting or encrypting data
- taking control of your devices to attack other organisations
- obtaining credentials which allow access to your organisation's systems or services that you use
- 'mining' cryptocurrency
- using services that may cost you money (e.g. premium rate phone calls).

What is ransomware?

Ransomware is a type of malware that prevents you from accessing your computer (or the data that is stored on it). The computer itself may become locked, or the data on it might be stolen, deleted or encrypted. Some ransomware will also try to spread to other machines on the network, such as the Wannacry malware that impacted the NHS in May 2017.

Normally you're asked to make a payment (often demanded in a cryptocurrency such as Bitcoin), in order to unlock your computer (or to access your data). However, even if you pay the ransom, there is no guarantee that you will get access to your computer, or your files. Occasionally malware is presented as ransomware, but after the ransom is paid the files are not decrypted. This is known as wiper malware. **For these reasons, it's essential that you always have a recent offline backup of your most important files and data**.

Should I pay the ransom?

The National Cyber Security Centre (NCSC) supports the National Crime Agency (NCA) recommendations. The NCA generally advise **not** to pay the ransom, as there is no guarantee that you will get access to your device (or data).

Warwickshire County Council

Warwickshire POLICE

Philip Seccombe Police and Crime Commissioner for Warwickshire

What can I do to protect myself?

1. Update Windows

WannaCry only affects computers running Microsoft Windows operating systems that don't have the latest security patches installed. If you are using a recent version of Windows (Windows 7, Windows 8, Windows 8.1 or Windows 10) **and** have automatic updates turned on, you should already be protected automatically against WannaCry.
To update your version of Windows:

- If you are using a currently supported version (Windows 7, Windows 8, Windows 8.1 or Windows 10), run Windows Update and apply any updates.
- If you are using Windows XP, Windows Vista or older versions of Windows, download the WannaCry security update and install it.

Note: We **strongly recommend** that you do not continue to use unsupported operating systems, but instead upgrade to one which receives regular security updates from the vendor.

2. Run antivirus

- Make sure your antivirus product is turned on and up to date. Windows has a built in malware protection tool (Microsoft Defender) which is suitable for this purpose.
- Run a full scan to make sure your computer is currently free of all known malware.

3. Keep a safe backup of your important files (see our data back up leaflet for more details)

What to do if you have been infected with ransomware

The National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk, as well as this please see our 'Recover an Infected Device' leaflet.