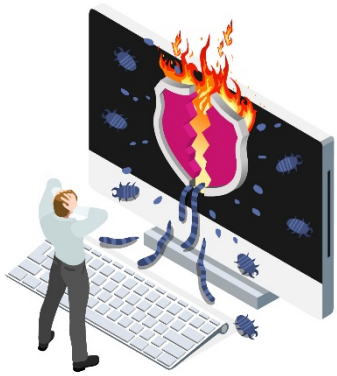
Malware. It's out to get you.



In this guide, we focus on Malware. Read on to find out what it is, what is does, where it comes from, and how to protect yourself.

What is malware and what does it do?

Malware is malicious software designed to cause harm to computers, servers and other devices, or to generate profit by nefarious means.

Viruses, worms, spyware, adware, Trojans and ransomware are all types of malware.

Once installed, malware could damage your device in any number of ways, including:

- Spy on your online activity or access your webcam
- Steal your passwords or files
- Send phishing emails from your account
- Use your device's processing power to mine crypto currency
- Use your device to attack other individuals or networks
- Encrypt the data on your device and demand a ransom for the decryption key

And it's not only Windows PCs that are affected. **Every device is at risk from malware**, be it a MacBook, Samsung Smart phone, LG Smart TV, USB, or even your car.

Where does it come from and how does it get onto your device?

Malware is created by a wide range of threat actors – from lone wolf "script kiddies" with limited resources to highly organised criminal enterprises whose goal is to separate you from your data or cash. Security specialists have even uncovered malware funded by nation-state governments.

These criminals may exploit vulnerabilities in your device's operating system or use social engineering in order to install malware.

Socially engineered attacks use different methods to trick you into downloading and installing malicious software. For example:

- Asking you to click malicious links or attachments in phishing emails, often purporting to be from a trusted organisation or someone you know.

- Providing a seemingly useful piece of software or smartphone app that runs malicious code in the background (trojan).
- Deliberately leaving an infected USB stick in a public area, e.g. a staff car park, in the hope it will be plugged into a corporate device (road apple attack).

So how can you protect against malware?

University devices

All University devices are centrally protected, patched and managed by IT Services. This is one of the reasons we need to schedule server downtime and why you are prompted to restart your computer from time to time.

Personal devices

- Install a trusted antivirus tool – and keep it up to date!
- Make sure you apply software updates and patches as quickly as possible.
- Only download apps from trusted sources, e.g. Play Store for Android or App Store for iOS.
- Never plug in a USB device you have found or don't recognise.
- Regularly back up your system files.
- Enable a firewall.
- Use device encryption tools.
- Ensure you protect your device with a password or PIN.
- Beware unsolicited or unexpected emails, particularly if they urge you to act quickly.
- Where possible, don't use an administrator account on your device. This helps limit access to potential malware.

Remember – malware can affect anyone, on any device. Follow these simple tips to help keep your data, and the University's data, safe.

Still unsure?

If you're still unsure, or if you would like advice, contact the Service Desk – servicedesk@abdn.ac.uk or https://myit.abdn.ac.uk.