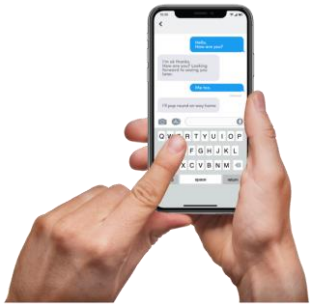
How to recover an infected device

 Prepared by Disability Equality Scotland

1. Confirm your device is infected

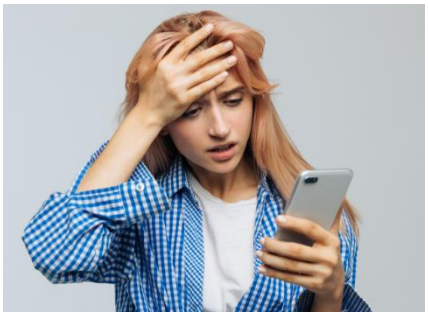


This document has some links in it.

They are in blue text and are underlined like this one: Action Fraud.

A blue link will take you to a website with more information:

- if you click on it if you are using a computer
- if you tap it with your finger if you are using a smartphone



Infected means your device has a **virus**.

A **virus** is a type of bad code or program written to change how a computer works.

A **device** is a is a piece of electronic equipment that can connect to the internet like:

- a smartphone
- a tablet
- a laptop computer

If your device has antivirus protection it will tell you it has found an infection.

Your device may be showing **ransomware**.

Ransomware is a type of bad software designed to block access to your device until a sum of money is paid.

The easiest way to check if your computer or laptop is infected is to run an antivirus scan and see if it finds anything.

If you do not have antivirus, signs of infection include:

- your device is:
    - running slowly
    - rebooting by itself
    - often shuts down programs or **apps** you are using
    - opens programs or apps you are not using

An **app** is a type of software that can be installed and run on your device.

The square symbols on the main screen of your phone are all apps.

- you have pop-up boxes from programs or apps you do not recognise, asking you to do unexpected things

- someone you know tells you that they have got unexpected emails from you, advertising unlikely products, or asking for money

- some apps on mobile devices try to check if your device has been **rooted** or **jailbroken**

Both these terms mean a criminal is trying to unlock your phone and get into its information.

- you get a phone call telling you your device is infected and you need their help to clear it up

This is a common scam.

The caller may say they are from a trusted company like Microsoft, or your internet service provider.

Stop the call straightaway and report it online to Action Fraud or call them on 0300 123 2040.

If you paid money to a scam caller:

- report the call to Action Fraud
- tell your bank or credit card provider

2. Try and fix the infection

If you are on a phone or tablet

These cannot usually be fixed by an antivirus product.

The safest thing to do is a factory reset.

You can usually find this option in the settings section of your device.

The exact name of the feature will depend on which type of device you have.

The National Cyber Security Centre has published advice where you can learn more about erasing the data on your device.

If this does not fix the problem, you will need expert help.

If you are using a computer or laptop:

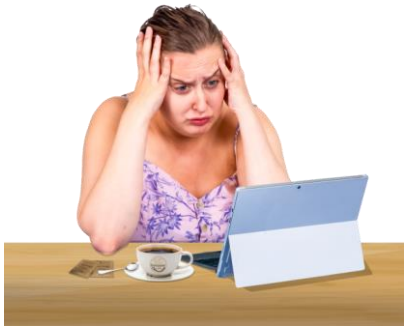
- update your device and programs
- open your antivirus product and run a scan, then follow the instructions

If your antivirus cannot clean your device up you will have to wipe it entirely and re-install everything, starting with your operating system.

You may need to get expert help to do this.

- if you cannot download and install an antivirus product because your **web browser** is infected, you will need to get expert help

Your **web browser** is the way you access the internet, for example Chrome or Edge.



- restore your backed-up data from the last known good back-up

You will lose any data that was not backed up.

If you try to rescue data while your device is still infected, the infection can be carried through after wiping and installing again.

3. After you have fixed the infection

- follow our advice for setting up your devices securely and keeping them safe
- keep your device, and programs and apps up to date
- back up your data
- make sure your PC or laptop has antivirus and that it updates regularly

 Prepared by Disability Equality Scotland