Lead Scotland

Linking education and disability

Lead Scotland

Using smart devices safely in your home

Easy Read

Easy Read made by Disability Equality Scotland

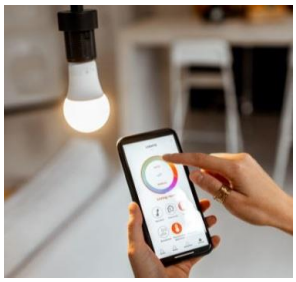
made with photosymbols®

Using smart devices safely in your home

Smart devices are everyday items that connect to the internet.

This can include things like

- smart speakers
- smart watches
- fitness trackers
- security cameras
- household items like
    - fridges
    - lightbulbs
    - doorbells



Do not switch on a smart device and forget about it.

Just like a smartphone or computer, smart devices can be **hacked** and put your information and privacy at risk.

Hacked means that someone else has got into your system without permission.

You need to check a few simple things to keep your home and your information safe.

This document explains how to protect yourself.

Setting up your device

Before you buy something, check **reviews** of it and of the manufacturer.

A **review** says what people think about the produce.

You can do this on websites like Trustpilot or Which?

Check the information from the company that made the product for information about how to set up your device.

This could be

- a printed manual or 'getting started' guide that came with the device

- on the manufacturer's website

Check the ‘Support’ area first.

- in the app

Some smart devices do not have to be connected to the internet.

Others may need

- an internet connection

- a smartphone app

- for you to create an account

Check their website for more information about this.

Check the default settings

Default means the settings that your device already has.

Some devices may not be secure when they are first switched on.

Change the password if the device comes with a password that looks easy to guess like ‘admin’ or ‘00000’.

Cyber Aware has advice about how to make a secure password.

https://www.cyberaware.gov.uk/passwords

Managing your account

If the device or app offers 2 step verification (2SV), turn it on.

It means a person must prove who they are in 2 different ways.

2SV usually works by texting or emailing you a number or code that you enter to prove that it is really you.

It makes it much harder for criminals to get into your online accounts, even if they know your password.

You can control some devices when you are away from your home Wi-Fi.

You use an online account linked to your device to do this.

You can back up your settings and data, so you can recover them if you need to get rid of all your personal information from your device.

Keeping your device updated

For each of your smart devices

- switch on the option to install automatic updates (if it is available)
- install any manual updates when it asks you to
- make sure the operating system is up to date

If something goes wrong

If you think your device is affected

- visit the manufacturer's website to see if it has information about what to do
- check the National Cyber Security Centre and the Information Commissioner's Office for advice

- if you think someone has accessed a device in your home and has control of it, do a factory reset

A **factory reset** means returning the device to its original settings.

It should remove all your personal information from the device.

Getting rid of your device

If you decide to sell or give your device to someone else, you should do a factory reset.

Check the manufacturer's website to find out how to do this.