GUIDANCE

Smart devices: using them safely in your home

Many everyday items are now connected to the internet: we explain how to use them safely.

28 November 2019

Smart devices are the everyday items that connect to the internet. This can include both 'hi-tech' items (think smart speakers, fitness trackers and security cameras), and also standard household items (such as fridges, lightbulbs and doorbells). Unlike conventional household items, you can't just switch on a smart device and forget it; you'll need to check a few simple things to protect yourself.
This page explains how to set up and manage your smart devices to keep your home - and your information - safe. Information on your consumer rights can be found on Which? and Citizens Advice.

What is the risk from using Smart Devices?

Just like a smartphone, laptop or PC, smart devices can be hacked to leave your data and privacy at risk. Very rarely, devices have been controlled by somebody else managing the device, often to frighten the victim.

- Children's GPS and fitness trackers (BBC News)
- Security cameras could be hijacked (BBC News)

- Smart home gadgets in domestic abuse warning (BBC News)

The NCSC and DCMS are encouraging manufacturers to make (and keep) their products secure, and have developed a code of practice (PDF) to help keep consumers safe. There's also lots you can do to protect yourself.

Setting up your device

Before you buy, check reviews of the product and the manufacturer. For information about how to set up a **specific device**, refer to the manufacturer's documentation. This may be a printed manual or 'getting started' guide that came with the device, on the manufacturer's website (check the **Support** area first), or within the app itself.
Some smart devices will work without being connected to the internet. Others may need an internet connection, a smartphone app, or for you to create an account. Again, check their website for details.

Check the default settings

Some devices may be insecure when they are first switched on, so you'll need to take some quick steps to protect yourself.

- If the device comes with a password that looks easily guessable (for example **admin** or **00000**), change it.
- Easily guessable passwords can be discovered by cyber criminals, so make sure you choose a secure one.

Managing your account

If the device or app offers two-factor authentication (2FA), **turn it on**. 2FA provides a way of 'double checking' that you really **are** the person you are claiming to be, and makes it much harder for criminals to access your online accounts, even if they know your password.
Some products can be controlled when you're away from your home Wi-Fi, by creating an online account linked to your device. You can also often back up your settings and data, so you can recover them if you need to wipe your device. However, accessing your device like this can make it easier for other people online to access them without your permission, so make sure you have changed default passwords and enabled 2FA if available.

Keeping your device updated

As with your computers and smartphones, installing software updates promptly helps keep your devices secure. For each of your smart devices, you should:

- switch on the option to install automatic updates (if available)
- install any manual updates when prompted
- make sure your device's operating system is up to date

If something goes wrong

If you become aware of an incident that's been reported and you think your device is affected:

- visit the manufacturer's website to see if there's information available on what you should do
- check the National Cyber Security Centre and the Information Commissioner's Office for advice
- if you think someone has malicious control/access of a device in your home, you should perform a factory reset

Getting rid of your device

If you decide to sell, or give your device to someone else, you should first perform a factory reset. This will return the device to its original settings, and should also remove all your personal data from the device. Check your manufacturer's website if you need to find out how to perform a reset.

PUBLISHED
15 February 2019

REVIEWED
15 February 2019

VERSION
1.0

WRITTEN FOR
Individuals & families