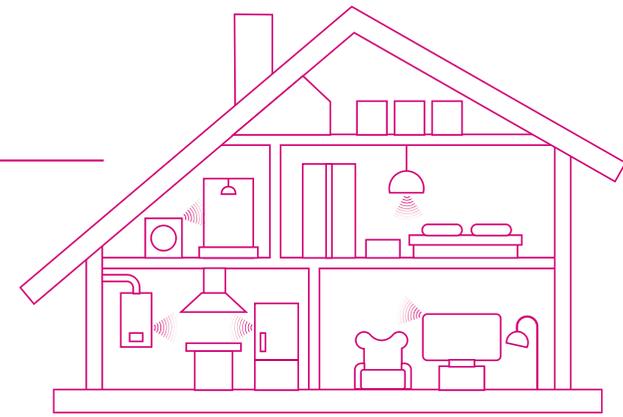


# Consumer Guidance for Smart Devices in the Home

Smart or internet-connected devices, such as smart TVs, music speakers, connected toys or smart kitchen appliances can bring great benefits to your daily life. However, without taking steps to secure all of your internet-connected products, you and your data could be at risk from someone getting unauthorised access to your device or account. Developed by the UK government and industry experts, this guidance will help you manage the security of your devices and help protect your privacy.



## SETTING-UP YOUR DEVICE

- **Read and follow the set-up instructions** for the device. These are often found in an app downloaded onto your smartphone, tablet or from a paper manual and guide that comes with the product.
- **Check device instructions to see if you need to** create an account on the manufacturer's website, or download any other recommended apps.
- If you are prompted to enter a password during the set-up process that is easy to guess, (such as 'admin' or '00000'), **you should change it.** Guidance on creating a strong password can be found on the **Cyber Aware** website.



## MANAGING YOUR ACCOUNT

- To **set-up and manage your device**, you may need to create or use an existing account on the manufacturer's website. This account may allow you to add a new device or link your smartphone to your devices. You should ensure that your account has a **strong password**.
- For added security, if the device or app offers **Two Factor Authentication** which provides a second layer of security, (such as a text message to your phone) you should enable it. This is particularly important if the account contains your **personal data** or **sensitive information** or is linked to something that may impact your or another person's physical safety.
- **Some products allow you to access or control them** when you are away from your home's Wi-Fi network; such as, to view security camera footage. Consider whether you need to make use of this feature, as products may allow you to disable it either in the app settings or within your account.



## KEEP UPDATING YOUR SOFTWARE AND APPS

Much like your laptop and smartphone, software and app updates help keep your devices secure. You should:

- **Check whether you can set-up and enable automatic updates** (on the app or on your online account).
- **Install the latest software and app updates.** These updates should download and install automatically on your device. If not, then you should install them straight away so you have the latest security protections. You should be prompted when a new update is ready to install, usually via a pop-up message or in the settings menu in the app or device menu.



## IF YOU BECOME AWARE OF AN INCIDENT AND THINK IT AFFECTS YOUR DEVICE

- **Visit the manufacturer's website** to see if there is information available on what you should do next.
- Check the **National Cyber Security Centre** and the **Information Commissioner's Office** websites to see any published guidance.
- Further advice on your consumer rights can be found on the **Which?** and **Citizens Advice** websites.

