
For many of us, today's home is a very convenient and cool place to live, with more and more devices responding to a tap in an app, or the sound of your voice.

**However, every device that's connected to your Wi-Fi is also transmitting data which could be of interest to criminals, including your speakers, voice assistants, cameras, intruder alarms, cameras, door locks and security lighting. Or even your kids' toys.**

Not setting up and maintaining the appropriate security measures for your smart devices, their apps, and your Wi-Fi network could lead to your information being stolen, and even your every movement being observed.

Another consideration is that the data provided by your smart devices – or the information you supply when you set them up – could be used by manufacturers for unwanted purposes, including being sold on to third parties.

**Top tips for your smart devices**

- Consider, that **buying well-known, reputable brands** means that more care has probably been taken in securing the products – for your and your family's security.

· For smart devices for which you need to log in to connect, **replace factory-set passwords** with secure ones you create yourself. This is because default administrator passwords may be common to every device shipped, and potentially insecure. If in doubt, check manufacturers' instructions on how to change passwords.

· **Don't use the same password** for more than one connected device, nor share passwords with those you already use for other online accounts.

· Make sure your **Wi-Fi network is secure.** Read our advice page on *Wireless Networks & Hotspots* at www.getsafeonline.org

· Make sure that all your **computers and mobile devices are protected** with updated internet security software / app, and that access to these devices is safeguarded with a PIN or passcode.

· Check the apps associated with your connected devices and **install updates as soon as prompted.** Also, regularly check manufacturers' websites for updates, as they can be slow to push these out via the app.

· **Limit the amount of information you provide** when setting up an app to what is absolutely necessary.

· Be aware that devices like voice assistants, smart speakers and cameras are always **active and potentially recording** unless you switch off or disable them.

*SOURCE: Get Safe Online*

*Please feel free to share these messages with any vulnerable friends, relatives or neighbours.*