# Top Tips to Make Your Home Cyber Safe

The Internet of Things, IoT, is the network of all the devices that can be connected to the Internet. You may automatically think of your laptop or smart TV, but IoT also includes things like gaming consoles, home assistant devices, your house alarm or your baby monitor.

And while these devices can improve how we live and work, remember, anything that's connected to the Internet can be vulnerable to attacks by hackers. Here are some steps you can take to help protect your home.
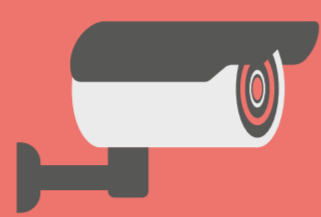
1. Secure all your devices

Ensure all your devices are protected with strong passwords or set up **two-factor authentication (2FA)** which is available on most IoT devices.
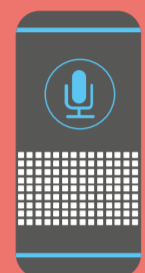
You should also **change the default password** and network name. It's important to remember not to include anything in your network's name that gives any information about your home or family, for example your name or address.

2. Check your apps

Downloading apps directly from the **official application store** (Google Play, Apple App Store etc.) is the safest way to get them. Clicking on a random link to download an app could lead to infecting your device.

Consider carefully what information and **permissions** you give before installing.

Regularly review your apps and remove what is unnecessary.

3. Review the privacy settings on your social media accounts

Go to your account's privacy settings and there you can **choose settings** that you are comfortable with.

Think carefully about what **information to include** in your profile, platforms can ask for information that you do not need to give them.
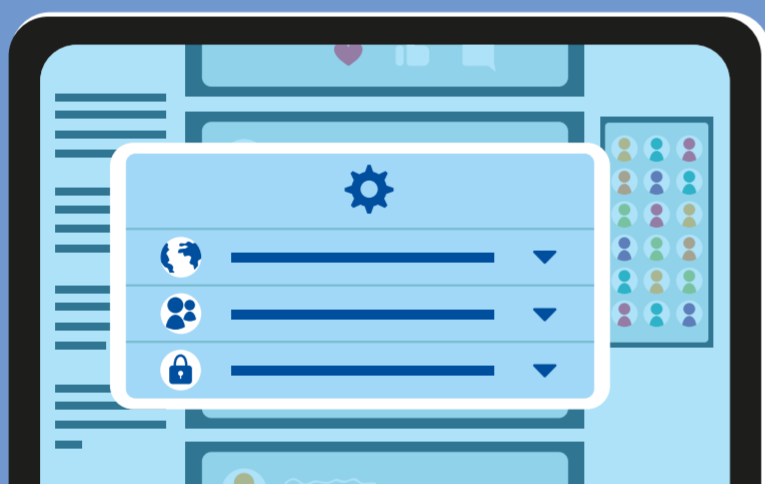
4. Set automatic updates on all devices and back up your data

IoT devices are vulnerable to attacks from hackers so having the **latest updates** is a vital part of keeping your devices secure. Setting up automatic updates means you won't have to remember to do it yourself.

Make sure you have **copies** of what is important to you stored somewhere offline or in the cloud, for example your photos or your contacts.
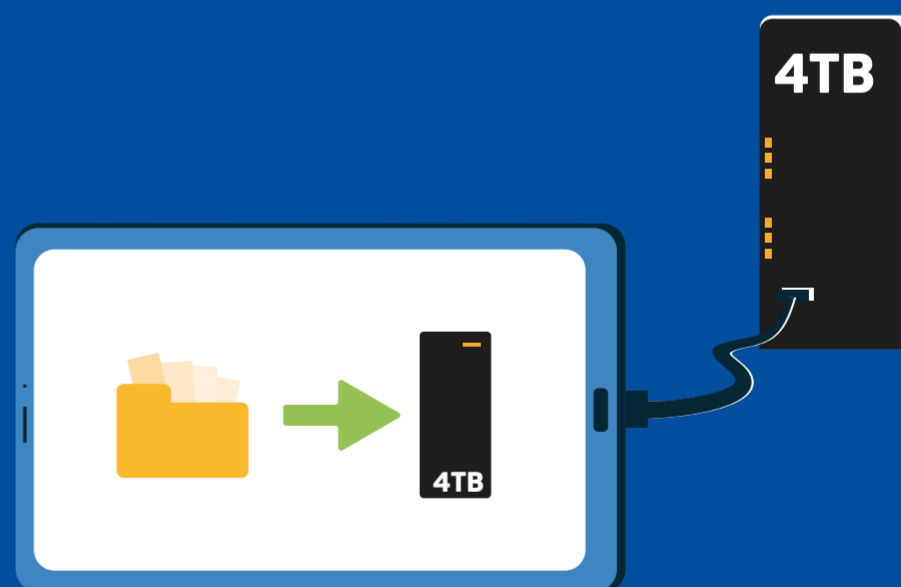
5. Keep your work and home devices separate

We suggest you have **separate devices** for work and home. The device you use for work should be kept for work purposes only, this will help you to minimise losses if your device is compromised.

If you have to share a device, make sure each user has a **separate user profile**.