smart home week

29th May - 4th June 2017

Top Tips for Keeping Your Smart Home Safe

May 2017

Introduction

More and more of us are using smart technology to make our daily lives comfortable and convenient, whether this means checking the baby monitor on your smartphone or remotely controlling the thermostat on your way back from work.

However, as we introduce these internet-connected devices to our homes it's important we remember to keep them as secure as possible.

Criminals and hackers are always looking for ways to exploit new technology, so we've put together these five tips for keeping your smart home safe.

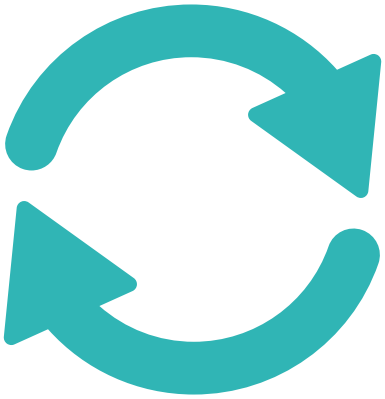
1. Stay Up To Date

As criminals become more and more sophisticated in their attacks, manufacturers and security companies have to upgrade their own technology and techniques.

One of the most important ways they do this is by releasing updates that beef up the security of your devices.

Some devices download these updates automatically, while others will require you to manually check to see if there's anything new. In either case, it's vital that you install the latest update.

The user manual that comes with your equipment will often include information on where to find updates, and suppliers often allow you to sign up for email notifications when they're released.



2. Change The Default Settings

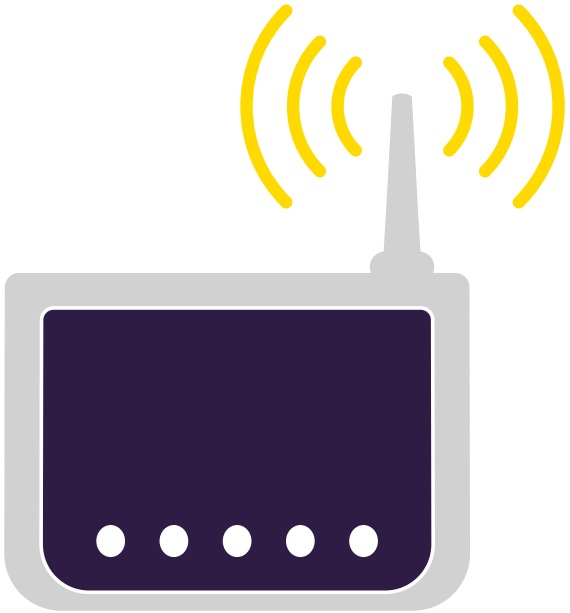
This one may sound a little obvious, but all of us are probably guilty of leaving some device set with its default password or login for the sake of convenience.

The devices we buy are often set with default login information when we get them home from the shop. These are usually easy to remember and have the advantage of being written down somewhere in the manual, but that doesn't mean we should keep them.

It's relatively simple for hackers to get access to the default passwords of devices, and if you haven't changed yours they can log in and start making changes with barely any effort. Once you have set a new password, it's important to remember to regularly update this.
You should also use different passwords for different devices, otherwise if hackers get their hands on it they could use it to access everything.

As well as passwords and usernames, many devices that connect to the internet have a default name or ID that can be seen by anyone with access to the network. While this won't allow them easy access, it still gives them information about what kind of equipment your using. Changing these names to something only you will understand helps to make life a little harder for a would-be hacker.

Always follow best practices around connected devices, such as installing a firewall on your home network. You might also consider one of the new devices designed to protect connected devices, such as the Bitdefender Box or the Norton Core.



3. Make Sure You Use Encrypted Signals

Many smart devices use wireless signals to communicate with each other. For example, the control panel of your security system may send out a signal telling one of the sensors around the house to turn itself on or off.

If a hacker gets close enough to your house, they may be able to use specialist devices to pick up these messages and record them.

As worrying as this may sound, it usually isn't a problem as most reputable systems ensure these signals are encrypted before they're sent, and are virtually useless to anybody listening in. Some less reliable systems, however, don't bother to scramble the signal before sending it, allowing anybody with the right equipment to analyse and then replicate it.

Over time, this can give them complete control of the system. In order to avoid this, make sure you invest in a reputable, reliable system that offers encryption and only used approved partners. If you have any doubts, check out reviews online and talk with your supplier.

4. Minimise Real World Tampering Risks

Sometimes it can be easy to forget that the smart devices we use, whether they're doorbells or printers, also need to be kept secure in the real world.

Many devices have buttons or control panels on them that can be used to view information useful to hackers. For the most part, this isn't too much of a worry – we tend to keep the devices in our homes and if criminals get their hands on them network security is probably the least of our worries – but wireless doorbells or security cameras are often left outside and are much easier to access.

The best way to counter this is to make sure you invest in products that can't easily be moved or detached, especially if you're using them outdoors.

Depending on the device and your confidence in your installation skills, it may also be best to invest in a professional installation and set-up.

5. Smart Devices Need Smart Passwords

You've probably heard this piece of advice before, but that doesn't make it any less important. Strong passwords are a vital part of keeping any internet-connected device secure, whether it's your laptop or your coffee machine.

The common tips for creating a secure password include avoiding common phrases or words – 'password' and '1234' are usually the first things hackers try – as well as personal information such as birthdays or anniversaries.

While these may be easy to remember, intelligent hackers can find out these kinds of things out by looking at things like your social media accounts.

There are plenty of places to find out more information on securing your password, such as this short guide from Google.

For further information please visit

smarthomeweek.co.uk