Smart devices promise to make our lives easier. In many cases - they do, however these new technologies present risks too. Whether you're using a digital assistant to record your shopping list or you're controlling your lights through a smart system, many smart functions can be 'hacked' and controlled by someone outside your home. This guide will help you identify some of the ways you can stay alert and protect yourself.

1 KNOW THE RISKS

The success of any smart device relies on it communicating with other devices using the Internet. It's an unavoidable part of using smart devices, but it does expose you to numerous risks. Attackers could use the Internet connection to steal your data for identify fraud or to make unauthorised purchases through your devices. There is even potential for more sinister exploitation, such as child grooming or cyber-bullying.

2 WHAT IS THE INTERNET OF THINGS?

This is the term given to all the devices connected to the Internet in your home. It includes a new digital doorbell connected to your smartphone, your kettle that boils when you tell it to on your tablet or your heating that comes on when you swipe on your smart watch. The Internet of Things (IoT) is designed to make life easier, but it also opens up your home network to potential cyber-attacks. It doesn't mean you can't enjoy the benefits, but it does mean being aware of the potential negatives.

3 CHECK ENCRYPTION SETTINGS

Whenever data is sent over the Internet, it is 'encrypted'. This makes it harder to read if it's intercepted. You should look to use a strong encryption setting, such as WPA2, rather than WPA or WEP. You can check your router manual on how to do this.

4 KEEP YOUR SOFTWARE UP TO DATE

Manufacturers constantly update and improve software used in smart devices. Some will automatically alert you to an update, but not all do. To be on the safe side, it's a good idea to set reminders in your calendar. Check the manufacturer's website for any updates and run them if necessary.

5 RENAME THE 'GATEWAY' TO YOUR HOME

Your Internet router is the virtual gateway to your home network. It needs protecting. To do this, you should change the default name (the SSID) and password. You can usually find steps to do this in the instruction manual. Don't use your family name. Choose something more obscure. Make the password complicated too, using upper and lower-case letters, numbers and symbols. Do this for your router and any other smart devices connected to the Internet.

12 Top Tips To Get Smart About The DEVICES In Your Home

National Online Safety®

6 USE A SEPARATE NETWORK FOR GUESTS

If your router has a feature that allows you to set up a separate network for guests, you should use it. That way, when guests use your Wi-Fi, they won't have access to your devices.

7 SAY GOODBYE TO SIRI AND ALEXA

It's a good idea to change the activation words on your smart devices so they are unique to you and your family. This makes it that much harder for people to break into your smart devices.

8 DEACTIVATE ANY UNNECESSARY FEATURES

Though it's a fun idea, you probably don't need to control your kettle from outside the house. In fact, there are often many unnecessary features included on smart devices. Where possible, you should look to disable these. Doing so reduces the ability for people to hack your devices. When someone sees you've actively taken steps to increase security, they're less inclined to try to compromise them.

9 TRUST YOUR INSTINCTS

If you ever feel something is wrong or your network is being exploited, visit the manufacturer's website or ring their technical support department. It's better to be safe than sorry.

10 BUILD A WALL

You could also purchase a dedicated 'firewall' device. This is something that plugs into your network and stops cyber threats reaching your router. Some routers do have a firewall element included, but they are no replacement for the real thing. A firewall device thoroughly analyses information coming in and out of your network and helps stop malicious attacks. A security device is strongly recommended to anyone who works from home or deals with sensitive information.

11 SECURE YOUR SMARTPHONE

If you do use apps on your smartphone to control devices in your home, make sure your smartphone is secure. At the very least makes sure the pin function is enabled, as well as any biometric authentication you have. Where possible, it's also a good idea to download some anti-virus software for your smartphone too.

12 REGULARLY AUDIT YOUR DEVICES AND CONSOLES

Every now and then you should check through all of your smart devices (including games consoles connected to the Internet). Turn them off at the mains and disconnect them from the Internet. In fact, it's good practice to disconnect any devices that aren't in use. It's a small thing but really does help. Even when you think a device might be in sleep mode, if it's connected to the Internet it could still be listening or streaming data.

Meet our expert

Emma was a secondary school Computer Science teacher for more than decade. Since leaving education, she has been working in a cyber security firm delivering cyber awareness training to businesses and carrying out network testing. She is a mother of a five-year-old and has vast experience of controlling and managing how children access online services and use apps.

SOURCES: https://www.ncsc.gov.uk, https://www.getsafeonline.org

Users of this guide do so at their own discretion. No liability is entered into. Current as of the date of release: 10.04.2019