How can I make my connected home more secure?

What is the Internet of Things?

The Internet of Things, often referred to as IoT, are everyday objects that connect to the internet.

These connected devices can be activated using voice commands, or controlled by downloading and using an app or via a Bluetooth connection. Examples of the Internet of Things include:

- Smart speakers,
- smart meters (for home electricity and heating),
- wearables such as fitness trackers.

What is the Internet of Toys?

The Internet of Toys are toys that connect to the internet.

Similar to the Internet of Things, these toys can be controlled using a smartphone app, voice commands or using a Bluetooth connection.

Connected toys are different from other toys because they collect, use, and share data via the internet. Examples of the Internet of Toys include:

- Connected action figures and dolls,
- robotic toys such as drones,
- learning development toys that aim to teach children a new skill.

What are the risks associated with the Internet of Things?

Although connected devices and toys provide children with opportunities for learning and interactive play, there are risks associated with the Internet of Things. For example:

Concerns have been raised about whether these devices are collecting too much personal information from children.

Some children (either accidentally or on purpose) are able to search for and access age-inappropriate material via a connected device such as a smart speaker.

Children may make 'in-app purchases' and spend money, which is often taken from their parents' bank account without their knowledge or consent.

Some of these devices may be more vulnerable to hacking and monitoring, as there are currently no security standards in place for connected devices.

Luckily, there are things you can do to minimise these risks.

There things you can do to help make your connected home safer for your child:

1. Do your research: Research different products online and read reviews. This is a great way to find out more about a product including age restrictions and credibility, as well as hearing directly from other parents.

2. Read the manual: Read the manual provided by the manufacturers. Information should be given about the privacy of the device, how it connects to the internet, and information about any app which may need to be downloaded in order to use the device.

J.A. Franklin, CEOP Ambassador

3. Set up parental controls: Make use of the parental controls available on your home broadband and any internet enabled device in your home. You can find out more about how to use parental controls by visiting your broadband provider's website, or see weblinks below

4. Use safe search: Enable the 'Safe Search' function on your connected device and web search engines. This will allow you to limit the material your child can see when online. It is important to understand that no parental control or 'Safe Search' function is 100% effective. This cannot be used alone to protect your child from accessing age-inappropriate material.

5. Change the default password: When you buy a connected device or toy, change the default password. Use a strong password that cannot easily be guessed and do not share this with others.

6. Set your Bluetooth to 'undiscoverable': Many connected devices are Bluetooth enabled. This means they are able to connect to nearby devices without having to connect to the internet. If the device has Bluetooth, set this to 'undiscoverable' so your child doesn't share data or pair with an unknown device.

7. Review and/or delete audio files: Some connected devices or toys work by listening to your child's voice commands, so these devices usually record and keep these audio files to work properly. Refer to the manual and find out how to review and/or delete audio files. If there's a microphone on your child's connected device, you can turn on the 'mute' button. This will stop the device from recording and storing audio files.

8. Talk to your child: Include connected devices in your online safety conversations, reinforcing the message that if your child sees or hears anything that makes them feel worried, they can speak to you or another adult they trust. Read further information on starting the conversation about online safety.

9. Supervise your child: If your child is primary school aged, supervise them when they are online or using a connected device. You should keep the connected devices your child uses in communal areas of the home such as in the kitchen or living room.

Extra support

For help setting up parental controls or reviewing the privacy settings of a connected device or toy, you can get advice by calling the NSPCC/O2 Helpline on 08088005002.

NSPCC download-set up kids tech devices

https://www.internetmatters.org/resources/e-safety-checklist-getting-your-kids-tech-devices-set-up-safe/

Internet matters

https://www.internetmatters.org/parental-controls/

CEOP / Think you know Parental controls

https://www.thinkuknow.co.uk/parents/articles/Parental-controls/

CEOP / Think you know: Tips for Starting a conversation with your child

https://www.thinkuknow.co.uk/parents/articles/having-a-conversation-with-your-child/

J.A. Franklin, CEOP Ambassador

J.A. Franklin, CEOP Ambassador