National Cyber Security Centre
a part of GCHQ

New security law for smart devices

Your rights as a consumer

From 29 April 2024, manufacturers of consumer 'smart' devices (like the one you've just bought) must comply with new UK law.

The law will help consumers to choose smart devices that provide **ongoing protection against cyber attacks**.

This card explains **why** this new law is required, and **how** it affects you - as a consumer.

To find out more, please scan this QR code:

What products are affected by the new law?

Consumer smart devices that connect to the internet (or your home network). This may include:

- smart speakers, smart TVs and streaming devices
- smart doorbells, baby monitors and security cameras
- cellular tablets and smartphones
- wearable fitness trackers (including smart watches)
- smart domestic appliances (such as light bulbs, kettles, thermostats, fridges and washing machines)

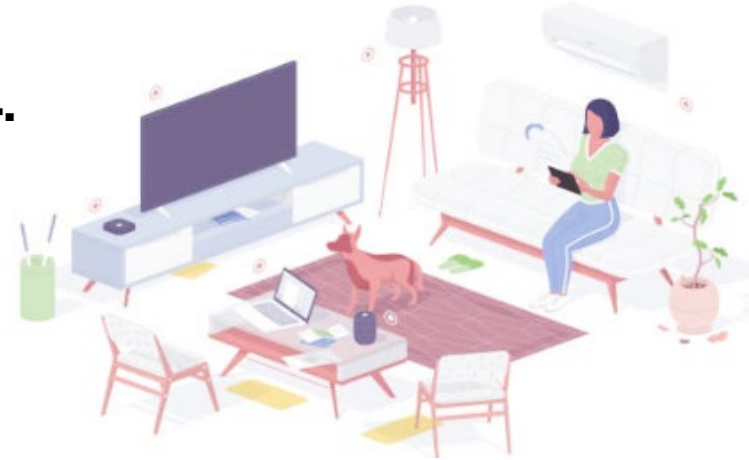
What will the new law mean for you, as a consumer?

Manufacturers must ensure that all smart devices meet basic cyber security requirements:

1. They must provide a point of contact for the reporting of security issues which - if ignored - could make devices vulnerable.
2. They must **not** ship devices that use default passwords (which can be easily found out and shared online). Knowing the password, a criminal could log into your device and use it to access your network, or to conduct cyber attacks.
3. They must state the length of time for which the device will receive important security updates. When updates are no longer provided, devices are easier to hack, or may stop working as expected.

The new law takes effect on 29 April 2024. What can you do in the meantime?

There's lots you can do to make sure that your smart devices are working securely. Please visit ncsc.gov.uk/smart, or turn over to find out how to make sure your devices are secure.



National Cyber Security Centre
a part of GCHQ

Getting started with your smart device

Following this advice will ensure your smart device is secure, and is protected from cyber attacks throughout its lifetime.

For more information, please visit the Cyber Aware website.

www.cyberaware.gov.uk

The Cyber Aware programme, from the UK's National Cyber Security Centre, helps you stay secure online, whether at work or at home.

Cyber Aware

1. Check the default settings

Some devices might not be secure when first switched on, so you should check the following:

- You'll need to create a password during setup. If the device (or app) comes with a **default password**, change it.
- Criminals know all the obvious passwords (like '1234'), so make sure you create a secure one, for example by combining **three random words**.
- If the device or app offers **two-step verification** (2SV), turn it on. 2SV (which is sometimes called multi-factor authentication or MFA), makes it much harder for criminals to access your devices, even if they know your password.

2. Install the latest software and app updates

Applying updates promptly will protect your device from criminals, adds new features, and keeps it working as it should.

- If you receive a prompt to **update your device** (or app), don't ignore it.
- Turn on the '**automatic updates**' option if available, so you don't need to remember to apply updates.
- For detailed instructions about updating a specific device, refer to the **support** area within the manufacturer's website.

For more tips on using smart devices securely, visit **ncsc.gov.uk/smart**, or scan the adjacent QR code.