Smart devices: new law helps citizens to choose secure products

Download the NCSC's point-of-sale leaflet explaining how new PSTI regulation affects consumers and retailers.

Carla V

From 29 April 2024, manufacturers of consumer 'smart' devices must comply with new UK law.

The law, known as the Product Security and Telecommunications Infrastructure act (or PSTI act), will help consumers to choose smart devices that have been designed to provide ongoing protection against cyber attacks.

The law means manufacturers must ensure that all their smart devices meet basic cyber security requirements. Specifically:

1. The manufacturer must **not** supply devices that use default passwords, which can be easily discovered online, and shared. If the default password is used, a criminal could log into a smart device and use it to access a local network, or conduct cyber attacks.
2. The manufacturer must provide a point of contact for the reporting of security issues which – if ignored – could make devices exploitable by cyber criminals.
3. The manufacturer must state the minimum 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 designed.

> **Note:**
> Most smart devices are manufactured outside the UK, but the PSTI act also applies to all organisations **importing** or **retailing** products for the UK market. Failure to comply with the act is a criminal offence, with fines up to £10 million or 4% of qualifying worldwide revenue (whichever is higher).

What smart products are affected by the new law?

The law applies to any 'consumer smart device' that connects either to the internet, or to a home network (for example by wifi). This may include:

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

How is the NCSC helping retailers and consumers?

The NCSC has produced a 'point of sale' (POS) leaflet for retailers to distribute in-store to their customers. It explains how the PSTI regulation affects consumers, and why it's important to choose smart products that protect against the most common cyber attacks.

We'd encourage all retailers to download and print the POS leaflet from the link below. This can be distributed free of charge.

We've already worked alongside major retailers to produce co-branded versions of these materials. If you'd like to add your own organisation's name or logo to the leaflet, please contact us directly on citizensteam@ncsc.gov.uk.

The reverse side of the leaflet explains the important steps consumers should follow **before** they start using their smart devices. These steps are summarised below. For more detailed instructions, please refer to the NCSC's guidance 'Smart devices: using them safely in your home'.

How can consumers make sure their smart devices are secure?

Unlike conventional electrical items, consumers can't simply switch on a smart device and start using it immediately. Here are the two most important things to do.

1. **Check the default settings**
   Some smart devices might not be secure when first switched on, so consumers should check the following:
   - If the device comes with a default password (either to control the device itself, or to access an 'app' for the device), they should change it.
   - Criminals know all the obvious passwords (like '1234'), so consumers should create a secure password, for example by combining three random words.
   - If the device or app offers **two-step verification** (2SV), consumers should turn it on. 2SV (which is sometimes called multi-factor authentication or MFA) makes it much harder for criminals to access devices, even if they know the password.

2. **Install the latest software and app updates**
   Applying updates promptly will protect smart devices from criminals and also adds new features, keeping devices working as they should.
   - If consumers receive a prompt to update a device (or app), they should **not** ignore it.
   - Consumers should turn on the 'automatic updates' option if available (so they don't need to remember to apply future updates).
   - For detailed instructions about updating a specific device, consumers should refer to the **support** area within the manufacturer's website.

Download the POS leaflet

The following leaflet is available as a PDF file. Please contact us if you'd like to receive this in a different file format, or if you'd like to produce a version that

contains your own branding.

Carla V
Citizen Resilience Officer, NCSC

WRITTEN BY

Carla V
Citizen Resilience Officer, NCSC

PUBLISHED

29 April 2024

WRITTEN FOR

Large organisations

Small & medium sized organisations

You & your family

PART OF BLOG

NCSC publications