New plans to boost security of consumer smart devices

- Pot of £400k to support market of industry-led assurance schemes for rapidly growing Internet of Things sector

- Comes as smart device owners urged to change default passwords and regularly update apps and software

The government has launched a £400,000 funding pot for innovators to design schemes to boost the security of internet-connected products, Digital Infrastructure Minister Matt Warman announced today.

The [programme](#) aims to support the development of the market of assurance schemes for consumer smart products, known as the Internet of Things (IoT).

Assurance schemes demonstrate that a device has undergone independent testing or a robust and accredited self-assessment process. These schemes are vital in enabling consumers to make security-conscious purchasing decisions.

The move will mean manufacturers can choose from a variety of schemes to demonstrate their product has undergone independent testing or a robust self-assessment process in line with the government's [Code of Practice](#) for Consumer IoT Security. It will also allow retailers to ensure they are stocking secure internet-connected devices, and could enable shoppers to make better informed decisions when buying new smart products.

The sale of connected devices is on the rise. Research suggests there will be 75 billion internet connected devices, such as televisions, cameras, home assistants and their associated services, in homes around the world by the end of 2025.

Digital Minister Matt Warman said:

> We are committed to making the UK the safest place to be online and are developing laws to make sure robust security standards for consumer internet-connected products are built in from the start.
>
> This new funding will allow shoppers to be sure the products they are buying have better cyber security and help retailers be confident they are stocking secure smart products.
>
> People should continue to change default passwords on their smart devices and regularly update software to help protect themselves from cyber criminals.

The move, led by the Department for Digital, Culture, Media and Sport (DCMS), comes as the government is progressing legislation to bring into law minimum security requirements for smart devices.

The laws announced earlier this year will make sure all consumer smart devices sold in the UK adhere to the three rigorous security requirements. These are:

- Device passwords must be unique and not resettable to any universal factory setting
- Manufacturers must provide a public point of contact so anyone can report a vulnerability
- Manufacturers must state the minimum length of time for which the device will receive security updates.

In a further move to boost the country's cyber resilience at a time when the public increasingly relies on technology to stay connected, the government last month launched the new ['Cyber Aware'](#) campaign which offers advice for people to protect passwords, accounts and devices.

The government continues to work in partnership with other governments and global standards bodies, such as ETSI, to drive a consistent, global approach to the cybersecurity of smart devices.

Owners of smart products are still encouraged to follow the National Cyber Security Centre [guidance](#) and change default passwords and regularly update apps and software to help protect their devices from cyber criminals.

[NCSC Guidance on 'Smart Devices: Using them safely in your home" is available here](#)