Government to strengthen security of internet-connected products

A new law will protect millions of users of internet-connected household items from the threat of cyber hacks, Digital Minister Matt Warman announced today.

The plans, drawn up by the Department for Digital, Culture, Media and Sport (DCMS), will make sure all consumer smart devices sold in the UK adhere to the three rigorous security requirements for the Internet of Things (IoT).

These are:

- All consumer internet-connected device passwords must be unique and not resettable to any universal factory setting
- Manufacturers of consumer IoT devices must provide a public point of contact so anyone can report a vulnerability and it will be acted on in a timely manner
- Manufacturers of consumer IoT devices must explicitly state the minimum length of time for which the device will receive security updates at the point of sale, either in store or online

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 want to make the UK the safest place to be online with pro-innovation regulation that breeds confidence in modern technology.
>
> Our new law will hold firms manufacturing and selling internet-connected devices to account and stop hackers threatening people's privacy and safety.
>
> It will mean robust security standards are built in from the design stage and not bolted on as an afterthought.

The measures were developed in conjunction with the business industry and the National Cyber Security Centre and set a new standard for best practice requirements for companies that manufacture and sell consumer smart devices or products.

Following on from the consultation, Government's ambition is to further develop legislation that effectively protects consumers, is implementable by industry and supports the long term growth of the IoT. Government aims to deliver this legislation as soon as possible.

Nicola Hudson, Policy and Communications Director at the NCSC, said:

> Smart technology is increasingly central to the way we live our lives, so the development of this legislation to ensure that we are better protected is hugely welcomed.
>
> It will give shoppers increased peace of mind that the technology they are bringing into their homes is safe, and that issues such as pre-set passwords and sudden discontinuation of security updates are a thing of the past.

This follows the government's voluntary Secure by Design Code of Practice for consumer IoT security launched in 2018. The Code advocates for stronger cyber security measures to be built into smart products at the design stage, and has already been backed by Centrica Hive, HP Inc Geo and more recently Panasonic.

The Government is working with international partners to ensure that the guidelines drive a consistent, global approach to IoT security. This includes a partnership with standards bodies. In February 2019 the European Standards organisation published the first globally-applicable industry standard on consumer IoT security, which is based on the UK Government's Code of Practice.

Matthew Evans, director of markets, techUK said:

> Consumer IoT devices can deliver real benefits to individuals and society but techUK's research shows that concerns over poor security practices act as a significant barrier to their take-up. techUK is therefore supportive of the Government's commitment to legislate for cyber security to be built into consumer IoT products from the design stage.
>
> techUK has been working on these three principles for the past four years. We support the work to ensure that they are consistent and are influencing international standards.
>
> We look forward to working closely with Government and industry to

> ensure the implementation of the legislation provides protection for consumers whilst continuing to promote innovation within the IoT sector.

John Moor, Managing Director, IoT Security Foundation said:

> Over the past five years, there has been a great deal of concern expressed toward vulnerable consumers and inadequate cybersecurity protection. Understanding the complex nature of IoT security and determining the minimum requirements has been a challenge, yet, after a thorough and robust consultation, those baseline requirements have now been universally agreed.
>
> The IoT Security Foundation welcomes the results of the consultation as it not only provides clarity for industry, it is great news for consumers and bad news for hackers.