Press release: Leading tech companies support code to strengthen security of internet-connected devices

- Tech companies HP Inc. and Centrica Hive Ltd are the first companies to sign up to commit to the code.
- The code will ensure that businesses continue to strengthen the cyber security of their products at the design stage.
- The UK is leading global efforts to strengthen the security of smart devices and products.

In a world first, government has published new measures to help manufacturers boost the security of internet-connected devices such as home alarm systems, fridges and toys.

There are expected to be more than 420 million internet connected devices in use across the UK within the next three years and poorly secured devices such as virtual assistants, toys and smartwatches can leave people exposed to security issues and even large scale cyber attacks.

To combat this, the Department for Digital, Culture, Media and Sport (DCMS) and the National Cyber Security Centre (NCSC) set out plans in a 'Secure by Design' review to embed security in the design process of new technology rather than bolt it on as an afterthought.

As a result, a new Code of Practice has been developed with industry to improve the cyber security of devices, encourage innovation in new technologies and keep consumers safe.

Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office, David Lidington said:

> Our National Cyber Security Strategy sets out our ambitious proposals to defend our people, deter our adversaries and develop our capabilities to ensure the UK remains the safest place to live and do business online.
>
> Tech companies like HP Inc. and Centrica Hive Ltd are helping us put in place the building blocks we need to transform the UK's cyber security.
>
> I am proud to say the UK is leading the way internationally with our new Code of Practice, to deliver consumer devices and associated services that are Secure by Design.

Minister for Digital, Margot James, said:

> From smartwatches to children's toys, internet-connected devices have positively impacted our lives but it is crucial they have the best possible security to keep us safe from invasions of privacy or cyber attacks.
>
> The UK is taking the lead globally on product safety and shifting the burden away from consumers having to secure their devices.
>
> The pledges by HP Inc. and Centrica Hive Ltd are a welcome first step but it is vital other manufacturers follow their lead to ensure strong security measures are built into everyday technology from the moment it is designed.

Poorly secured devices can threaten individuals' privacy, compromise their network security, their personal safety and could be exploited as part of large-scale cyber attacks. Recent high-profile breaches putting people's data and security at risk include attacks on smart watches, CCTV cameras and childrens' toys.

To make sure consumers are protected when using internet-connected devices and while manufacturers implement stronger security measures, Government and NCSC have worked closely with consumer groups and industry to develop guidance on smart devices in the home.

The new Code of Practice outlines thirteen guidelines that manufacturers of consumer devices should implement into their product's design to keep consumers safe.

This includes secure storage of personal data, regular software updates to make sure devices are protected against emerging security threats, no default passwords and making it easier for users to delete their personal data off the product.

Dr Ian Levy, the NCSC's Technical Director, said:

> With the amount of connected devices we all use expanding, this world-leading Code of Practice couldn't come at a more important time.
>
> The NCSC is committed to empowering consumers to make informed decisions about security whether they're buying a smartwatch, kettle or doll. We want retailers to only stock internet-connected devices that meet these principles, so that UK consumers can trust that the technology they bring into their homes will be properly supported throughout its lifetime.

The Government has also published a mapping document to make it easier for other manufacturers to follow in HP Inc.'s and Centrica Hive's footsteps.

Further work is underway to develop regulation that will strengthen the security of internet-connected consumer products.

Implementing the Code of Practice can help organisations make sure that smart devices that process personal data are compliant with the stronger data protection laws which came into force in May. Failure to comply with the General Data Protection Regulations (GDPR) means firms could risk fines of up to £17 million or 4 percent of global turnover, for the most serious data breaches.

Seb Chakraborty, Centrica Hive's Chief Technology Officer, said:

> Meeting the privacy and data protection expectations of our valued customers is a priority.
>
> We invest heavily in the security of our products and we are delighted to support Government in this global step forward, building strong security measures into devices at the point of design.

George Brasher, HP Inc. UK managing director, said:

> Cyber-crime has become an industry and IoT 'endpoint' devices increasingly constitute the frontline of cybersecurity. At HP, we are reinventing the state of the art in device security to address modern threats.
>
> Today we design our commercial products with security built-in not bolted on, not only designed to protect, but also to detect and self-heal from cyber-attacks. We are delighted to be joining forces with the UK Government in our shared ambition to raise the bar broadly in consumer IoT device security, starting with the connected printers we are all used to at home.

Alex Neill, Which? Managing Director of Home Products and Services, said:

> Which? tests many internet-connected products and has already improved security on devices in more than 1 million UK homes including TVs, voice-activated assistants, smart thermostats, and wireless routers.
>
> We welcome the Government taking a lead in tackling the growing issue of security in internet-connected products. Manufacturers of these smart devices must now show they are taking security seriously and sign up to the Code to better protect consumers who use their products every day.

Teg Dosanjh, Director of IOT, MDE & SmartThings, SAMSUNG, said:

> As a global leader in connected technology, Samsung understands that privacy and security are of great importance to consumer trust in connected devices. We build market-leading cyber security into all our products and warmly welcome the Government's desire to make connected devices as safe and secure as possible. We will continue to work with Government to develop these proposals and ensure the transformative potential of the Internet of Things is delivered safely for everyone.

This initiative is a key part of the Government's five-year, £1.9 billion National Cyber Security Strategy which is making the UK the most secure place in the world to live and do business online.

Notes to editors

The Code of Practice for Consumer IoT Security was developed by DCMS in conjunction with the National Cyber Security Centre and with support from other Government departments, industry and academic partners. The project has been informed by an expert advisory group which included subject matter experts from industry, consumer organisations and academia.

The Government's Digital Strategy includes the aspiration for the UK to remain an international leader in the development and uptake of IoT. The Government's actions include the funding of research and innovation in IoT, including through three-year £30 million IoT UK Programme.

The Government's Digital Charter is a rolling programme of work to agree norms and rules for the online world and put them into practice. In some cases this will be through shifting expectations of behaviour; in some we will need to agree new standards; and in others we may need to update our laws and regulations. Our starting point will be that we will have the same rights and expect the same behaviour online as we do offline.

Domestically, Her Majesty's Government Procurement, via Crown Commercial Service, will be adjusted to ensure future negotiations with suppliers of IoT products used by government departments will employ the Code to ensure the safety of such devices

HP Inc. creates technology that makes life better for everyone, everywhere. Through our portfolio of printers, PCs, mobile devices, solutions, and services, we engineer experiences that amaze. More information about HP Inc. is available at http://www.hp.com/UK.

Centrica Hive commits to ensure that all new devices, those designed and manufactured from 1st January 2021, will adhere to the 13 guidelines set out in the Code of Practice for Security in Consumer IoT Products.

Centrica Hive began back in 2013 with their customers telling them they wanted comfort and convenience, and a thermostat they could control that was easy and simple to use. Today, with £500 million investment from parent company Centrica plc, the Hive range of connected products has grown its

range and geographical market, into North America, Canada, UK, Ireland and most recently Italy, with more opportunities for global expansion.

Hive focuses on making everyday life a little easier, freeing people up to spend time doing the things they love. The range of Hive products and services now incorporates a suite of products (including motion sensors, plugs, light bulbs and cameras) all controlled from a central home hub that Hive call their ecosystem. Designed to work together, to offer affordable, easy to use solutions and make a difference in people's lives. The total number of Hive connected home customers has reached one million worldwide with over two million products sold.

Code of Practice

To make sure consumers are protected when using internet-connected devices and while manufacturers implement stronger security measures, Government and NCSC have worked closely with Information Commissioner's Office, Get Safe Online, consumer groups, the British Retail Consortium and industry experts to develop consumer guidance on smart devices in the home. This work supports efforts by Action Fraud who highlight that consumers can report fraud or cyber crime to their organisation.

The guidance Centrica Hive currently provides, advises consumers on how they can correctly set-up and configure their devices securely.