Press release: New measures to boost cyber security in millions of internet-connected devices

BOSSES behind ‘smart’ devices such as televisions, toys and speakers found in millions of homes will be expected to build-in tough new security measures that last the lifetime of the product, as part of plans to keep the nation safe from the increasing cyber threat.

Estimates show every household in the UK owns at least 10 internet connected devices and this is expected to increase to 15 devices by 2020, meaning there may be more than 420 million in use across the country within three years.

Poorly secured devices threaten individuals’ online security, privacy, 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 children’s dolls.

Developed in collaboration with manufacturers, retailers and the National Cyber Security Centre, the Government’s Secure by Design review review lays out plans to embed security in the design process rather than bolt them on as an afterthought.

The Government will work with industry to implement a rigorous new Code Of Practice to improve the cyber security of consumer internet-connected devices and associated services while continuing to encourage innovation in new technologies.

Speaking ahead of a launch event at consumer champion Which? headquarters, Margot James, Minister for Digital and the Creative Industries, said:

> We want everyone to benefit from the huge potential of internet-connected devices and it is important they are safe and have a positive impact on people’s lives. We have worked alongside industry to develop a tough new set of rules so strong security measures are built into everyday technology from the moment it is developed.
>
> This will help ensure that we have the right rules and frameworks in place to protect individuals and that the UK continues to be a world-leading, innovation-friendly digital economy.

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

> The NCSC is committed to ensuring the UK has the best security it can, and stop people being expected to make impossible safety judgements with no useful information.

> We are pleased to have worked with DCMS on this vital review, and hope its legacy will be a government ‘kitemark’ clearly explaining the security promises and effective lifespan of products.

> Shoppers should be given high quality information to make choices at the counter. We manage it with fat content of food and this is the start of doing the same for the cyber security of technology products.

The Secure by Design report outlines practical steps for manufacturers, service providers and developers. This will encourage firms to make sure:

- All passwords on new devices and products are unique and not resettable to a factory default, such as ‘admin’;
- They have a vulnerability policy and public point of contact so security researchers and others can report issues immediately and they are quickly acted upon;
- Sensitive data which is transmitted over apps or products is encrypted;
- Software is automatically updated and there is clear guidance on updates to customers;
- It is easy for consumers to delete personal data on devices and products;
- Installation and maintenance of devices is easy.

Alongside these measures for ‘Internet of Things’ manufacturers, the report proposes developing a product labelling scheme so consumers are aware of a product’s security features at the point of purchase. The Government will work closely with retailers and consumer organisations to provide advice and support.

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

> With connected devices becoming increasingly popular, it’s vital that consumers are not exposed to the risk of cyber-attacks through products that are left vulnerable through manufacturers’ poor design and production.

> Companies must ensure that the safety of their customers is the absolute priority when ‘smart’ products are designed. If strong security standards are not already in place when these products hit the shelves, then they should not be sold.

Julian David, CEO of TechUK said:

> The opportunities created by the Internet of Things are now becoming clear. It offers consumers and citizens greater empowerment and control over their lifestyles, from managing energy consumption at home to having peace of mind that a frail relative is going about their normal routine.
>
> However, these opportunities also bring risk and it is important that the IoT market now matures in a sensible and productive way, with security embedded at the design stage. This project is the start of that maturity. Industry has been keen to engage in the review and demonstrate what is best practice. It is important that companies throughout the supply chain now adopt and build on this Code of Practice to build the trust required to drive widespread take-up of the IoT.

Mark Hughes, CEO, BT Security:

> BT shares the Government's ambition to make the UK the safest place to work and do business online. We are proud to have played a key advisory role in the development of the draft Code of Practice, having shared our technical insight with the Government in our capacity as a global network operator, UK broadband provider and as a global provider of cyber security and IoT services.
>
> From the development of the world's first Cleanfeed filter to block child abuse images, free parental controls for broadband products and devices, to warning or blocking our customers from known malware and phishing sites, BT has been at the forefront of keeping consumers and families safe online for many years. BT is actively involved in driving standards, interoperability and security across the IoT market and will continue to provide guidance to the Government and industry around best practice for securing internet connected devices.

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 Secure by Design report 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 report can be found at Secure by Design report.

Stakeholders have an opportunity to send feedback on the report's draft proposals via securebydesign@culture.gov.uk from the 7th March until the 25th April.

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.

Consumer tips for IoT device security:

- Research the security of a product before buying
- Check your home router does not have a default password/username
- Change any default passwords and usernames found in devices
- Check all the available security settings
- Check the manufacturers' website to see if there are any updates available
- If there's a two-step identification option – use it

Further guidance on security for consumer IoT / devices can be found ICO's website.

Associated services: This primarily refers to applications that manage internet-connected devices. Such applications usually run on phones and connect to cloud-based services.

Draft Code of Practice:

- All IoT device passwords must be unique and not resettable to any universal factory default value.
- Companies that provide internet-connected devices and services must have a vulnerability disclosure policy and point of contact.
- Software must be kept updated. This includes the need for updates to be timely and not impact on the functioning of the device
- Any credentials must be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable
- Security-sensitive data, including any remote management and control, should be encrypted when transiting the internet, appropriate to the properties of the technology and usage. All keys should be managed securely
- Ensure software integrity: Software on IoT devices must be verified

using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function
- Ensure that personal data is protected in accordance with data protection law
- Make systems resilient to outages. Resilience must be built into IoT services where required by the usage or other relying systems, so that the IoT services remain operating and functional
- Monitor system telemetry data. If collected, all telemetry such as usage and measurement data from IoT devices and services should be monitored for security anomalies within it
- Make it easy for consumers to delete personal data on devices and products.
- Make installation and maintenance of devices easy
- Validate input data: Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices must be validated

The Government will be conducting more work in 2018 to further develop these recommendations. This will involve considering how following the Data Protection Bill, the Government can further embed guidelines in the Code of Practice within regulations.

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.