Government advances plans to boost security of smart products

- Includes further information on powers granted to enforcement body and scope of rules
- Shoppers urged to look at security update periods when buying a smart product

The government has today published proposals for a new law that will help protect millions of smart device users from cyber criminals.

The proposals, drawn up by the Department for Digital, Culture, Media and Sport (DCMS) and supported by the technical expertise of the National Cyber Security Centre (NCSC), detail the government's plans to raise the security standard for all consumer smart products sold in the UK.

As a first step the standard will make sure they adhere to three important requirements, which may be expanded on over time in consultation with stakeholders. The three requirements 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;
- Information stating the minimum length of time for which the device will receive security updates must be provided to customers.

This latest move by government is a significant step towards bringing robust security requirements for consumer smart products, such as smart speakers, kitchen appliances or cameras, into law as part of its ambition to make the UK the safest place to be online.

Research suggests there are now 20 billion smart devices – known as the Internet of Things (IoT) – in use around the world. But with only around 13 per cent of manufacturers embedding even the most basic approaches to cyber security in their products, people's privacy and security is at risk.

The government is already taking world-leading steps to tackle the problem and published a code of practice for consumer IoT security for manufacturers in 2018. Last month DCMS and the NCSC also played a vital role collaborating with global standards body European Telecommunications Standards Institute (ETSI) to develop the first major international standard for the security of smart devices, which will help protect consumers around the world from falling victim to cyber hacks through security vulnerabilities in devices bought on the global market.

Digital Infrastructure Minister Matt Warman said:

> This is a significant step forward in our plans to help make sure

> smart products are secure and people’s privacy is protected.
>
> I urge organisations to respond to these proposals so we can make the UK the safest place to be online with pro-innovation regulation that inspires consumer confidence in our tech products.
>
> People should continue to change default passwords on their smart devices and regularly update software to help protect themselves from cyber criminals.

The call for views also sets out the scope of the rules, what industry will need to do to comply with the new laws and an overview of industry guidance to be produced, as well as information on potential powers granted to the enforcement body. These could include powers to:

- Temporarily ban the supply or sale of the product while tests are undertaken;
- Permanently ban insecure products, if a breach of the regulations is identified;
- Serve a recall notice, compelling manufacturers or retailers to take steps to organise the return of the insecure product from consumers;
- Apply to the court for an order for the confiscation or destruction of a dangerous product; Issue a penalty notice imposing a fine directly on a business.

The proposals will also aim to future proof legislation in an age of rapid technological change and innovation, and the government will be looking for industry, academics and consumer groups to feed back on the plans.

Groups providing feedback to the [Call for Views}(https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views) will help shape the final enforcement approach, which will help determine the body best placed to administer the measures.

Consumer smart products can be the weak points of entry for hackers looking to breach someone’s home network and owners are often unaware that the default passwords or outdated software which can come as standard on a new device can lead to a range of harms, including the invasion of privacy, fraud or even physical harm.

Insecure smart devices also enable more widespread and destabilising cyber attacks on infrastructure and services. In the 2016 Mirai botnet attack, hackers gained access to thousands of IoT products through common default passwords to launch an attack that overwhelmed servers leaving much of the internet inaccessible on the US east coast.

Shoppers are urged to look at information on the duration of security update periods when choosing a smart product and people are still encouraged to follow NCSC guidance and change default passwords as well as regularly update apps and software to help protect their devices from cyber criminals.

National Cyber Security Centre Technical Director Dr Ian Levy said:

> People are at risk because fundamental security flaws in their connected devices are often not fixed – and manufacturers need to take this seriously.
>
> We would encourage all consumer device manufacturers to make their views heard and help us ensure the technology people bring into their homes is as safe and secure as possible.

British Retail Consortium Assistant Director Graham Wynn said:

> Internet of Things products are quickly growing in popularity but most people still do not realise the dangers to personal data from smart products that are insecure. We welcome practical proposals from the government based on the three rigorous requirements to ensure that consumers' safety and privacy are protected.

techUK CEO Julian David said:

> Consumer IoT devices are increasingly delivering on their potential to improve consumers' lives, with smart speakers, activity trackers and smart kitchen appliances a few notable examples. Poor security practices have consistently slowed the adoption of these devices, acting as a barrier to UK citizens reaping the benefits of the latest innovations and products.
>
> techUK has continually supported government's efforts to ensure IoT products are secured at the design stage, starting in 2018 with the Secure-by-Design Code of Practice and now through this legislation. This important step will help ensure consumers are sufficiently protected, building trust and driving wider adoption across this growing sector which can ultimately improve the lives of UK citizens.