New cyber security laws to protect smart devices amid pandemic sales surge

- Apple, Samsung, Google and other manufacturers will say when smartphones, smart speakers and other devices will stop getting security updates
- Easy-to-guess default passwords to be banned on virtually all devices under new law
- Rules will make it easier for people to report software bugs that can be exploited by hackers

Makers of smart devices including phones, speakers, and doorbells will need to tell customers upfront how long a product will be guaranteed to receive vital security updates under groundbreaking plans to protect people from cyber attacks.

New figures commissioned by the government show almost half (49%) of UK residents have purchased at least one smart device since the start of the coronavirus pandemic. These everyday products – such as smart watches, TVs and cameras – offer a huge range of benefits, yet many remain vulnerable to cyber attacks.

Just one vulnerable device can put a user's network at risk. In 2017, attackers infamously succeeded in stealing data from a North American casino via an internet-connected fish tank. In extreme cases hostile groups have taken advantage of poor security features to access people's webcams.

To counter this threat, the government is planning a new law to make sure virtually all smart devices meet new requirements:

- Customers must be informed at the point of sale the duration of time for which a smart device will receive security software updates
- A ban on manufacturers using universal default passwords, such as 'password' or 'admin', that are often preset in a device's factory settings and are easily guessable
- Manufacturers will be required to provide a public point of contact to make it simpler for anyone to report a vulnerability.

Smartphones are the latest product to be put in scope of the planned Secure By Design legislation, following a call for views on smart device cyber security the government has responded to today.

It comes after research from consumer group Which? found a third of people kept their last phone for four years, while some brands only offer security updates for a little over two years.

The government continues to urge people to follow NCSC guidance and change default passwords as well as regularly update apps and software to help protect their devices from cyber criminals.

Digital Infrastructure Minister Matt Warman said:

> Our phones and smart devices can be a gold mine for hackers looking to steal data, yet a great number still run older software with holes in their security systems.
>
> We are changing the law to ensure shoppers know how long products are supported with vital security updates before they buy and are making devices harder to break into by banning easily guessable default passwords.
>
> The reforms, backed by tech associations around the world, will torpedo the efforts of online criminals and boost our mission to build back safer from the pandemic.

Security updates are a crucial tool for protecting people against cyber criminals trying to hack devices.

Yet research from University College London found none of the 270 smart products it assessed displayed information setting out the length of time the device would receive security updates at the point of sale or in the accompanying product paperwork.

By forcing tech firms to be upfront about when devices will no longer be supported, the law will help prevent users from unwittingly leaving themselves open to cyber threats by using an older device whose security could be outdated.

Just one in five global manufacturers have a mechanism in place to allow security researchers – firms and individuals who find security flaws in devices – to report vulnerabilities.

These moves have been supported by important tech associations across the globe including the Internet of Secure Things (IoXT), whose members include some of the world’s biggest tech companies including Google, Amazon and Facebook.

Brad Ree, CTO of the Internet of Secure Things (IoXT) Alliance, said:

> We applaud the UK government for taking this critical step to demand more from IoT device manufacturers and to better protect the consumers and businesses that use them.
>
> Requiring unique passwords, operating a vulnerability disclosure program, and informing consumers on the length of time products will be supported is a minimum that any manufacturer should provide. These are all included in the IoXt compliance programme and have been well received by manufacturers around the world.

The new law builds upon world-leading work the government has already done to boost the security of smart devices, including publishing a code of practice for device manufacturers to boost the security of their products in 2018.

Last month the Digital Secretary Oliver Dowden set out his ten tech priorities which included keeping the UK safe and secure online and the government published its groundbreaking Integrated Review of defence and security.

The government also played a vital role in developing the first major international standard for consumer device cyber security to help manufacturers protect consumers around the world from falling victim to cyber attacks.

This standard has been supported by the Cybersecurity Tech Accord (CTA), an industry association whose members include Arm, Microsoft and Dell, and has also been promoted in Australia, Singapore, Finland and India – demonstrating Britain’s global influence as a cyber power.

Three new voluntary assurance schemes have been launched recently to give shoppers confidence a smart product has been made cyber secure, thanks to a £400,000 government grant.

- The Stockport-based Internet of Toys Assurance Scheme will allow parents to know from the outset whether a smart toy they are buying their children has been tested and meets the minimum security requirements

- The Smart TV Cybersecurity Certification programme will provide third-party testing and give confidence to buyers of smart TV products by allowing approved devices to display a certification logo

- The IASME IoT Security Assured initiative will be open to start-ups and smaller companies to carry out verified cyber security self-assessment of their products to ensure they meet high standards.

National Cyber Security Centre Technical Director Dr Ian Levy said:

> Consumers are increasingly reliant on connected products at work and at home. The Covid-19 pandemic has only accelerated this trend and while manufacturers of these devices are improving security practices gradually, it is not yet good enough.
>
> DCMS’ publication builds on the 2018 Code of Practice and ETSI EN 303 645 to clearly outline the expectations on industry. To protect consumers and build trust across the sector, it is vital that manufacturers take responsibility and pay attention to these proposals now.

> It is also important to support uptake of good practice and provide industry with opportunities to innovate. I’m pleased to see the pilots, funded by DCMS, begin to test ways in which customers will be able to gain confidence in the security of these devices.

Annalaura Gallo, Head of the Cybersecurity Tech Accord secretariat, said:

> Trust in technology is a key issue of our time and security is a fundamental building block to achieve this.
>
> We welcome the leading role played by the UK Government in promoting a national and international focus on this issue in a way which is designed to drive up security without imposing onerous burdens on people creating new technology for consumers.

John Moor, Managing Director of the Internet of Things Security Foundation, said:

> We welcome this announcement as a necessary and considered development to make consumers safer. As an expert body, we welcome the clarity it brings for our manufacturing members both now and moving forwards.
>
> The Internet of Things is constantly evolving and security requirements must continue to keep pace. As such, the importance of vulnerability management and updating security software cannot be understated. In the words of one of our members: ‘remember, if it ain’t secure, it ain’t smart’.

Rocio Concha, Director of Policy and Advocacy at Which?, said:

> New laws to tackle this issue are a crucial step as there are a vast array of connected devices with security flaws, many of which are currently on the market, that put consumers at risk from cyber criminals.
>
> We share the government’s ambition to make the UK one of the safest places in the world for consumers to use smart technology and this must be backed up by strong enforcement, ensuring people can get effective redress when they purchase devices that fail to meet security standards and leave them exposed to data breaches and scams.

The government intends to introduce legislation as soon as parliamentary time allows.

ENDS

Notes to editors

Read the government’s consultation response on proposals for regulating consumer connected product cyber security.

The government commissioned Ipsos MORI to undertake a survey to explore consumer purchasing behaviour of, and attitudes to connected devices published today. It shows the popularity of smart devices is on the rise, with three in five consumers (57 per cent) reporting an increase in their use since the start of the pandemic.

The research also shows nine in 10 consumers (87 per cent) think smart devices should come with privacy and security features as standard, while only one in five (20 per cent) have previously checked to see if a new smart device has a default password which can make devices vulnerable to hacks.

The Integrated Review of defence and security sets the goal of cementing the UK’s position as a responsible and democratic cyber power and announced a commitment to publish a new National Cyber Strategy later this year. The strategy will set out how the UK intends to build a more resilient digital nation and realise the benefits that cyberspace can bring.

Last year DCMS and the NCSC also played an important 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.