Tougher consumer protections against malicious apps

- Proposals include a world-first code of practice to set minimum security and privacy requirements for app store operators and developers

- New report published today reveals malicious apps downloaded by hundreds of thousands of users put people's data and money at risk

- People downloading apps to smartphones, games consoles and TVs will be better protected from hackers under new government plans to boost security standards.

Millions of people use apps every day to shop, bank and make video calls and the UK app market is worth £18.6 billion. But there are few rules governing the security of the technology or the online stores where they are sold.

A new report on the threats in app stores published today by the National Cyber Security Centre (NCSC) shows people's data and money are at risk because of fraudulent apps containing malicious malware created by cyber criminals or poorly developed apps which can be compromised by hackers exploiting weaknesses in software.

To provide better protection for consumers, the government is launching a call for views from the tech industry on enhanced security and privacy requirements for firms running app stores and developers making apps.

Under new proposals, app stores for smartphones, game consoles, TVs and other smart devices could be asked to commit to a new code of practice setting out baseline security and privacy requirements. This would be the first such measure in the world.

Developers and store operators making apps available to UK users would be covered. This includes Apple, Google, Amazon, Huawei, Microsoft and Samsung.

The proposed code would require stores to have a vulnerability reporting process for each app so flaws can be found and fixed quicker. They would need to share more security and privacy information in an accessible way including why an app needs access to users' contacts and location.

Cyber Security Minister Julia Lopez said:

> Apps on our smartphones and tablets have improved our lives immensely – making it easier to bank and shop online and stay connected with friends.

> But no app should put our money and data at risk. That's why the Government is taking action to ensure app stores and developers raise their security standards and better protect UK consumers in the digital age.

The NCSC report found all types of app stores face similar cyber threats and the most prominent problem is malware: corrupted software which can steal data and money and mislead users.

For example, last year some Android phone users downloaded apps which contained the Triada and Escobar malware on various third-party app stores. This resulted in cyber criminals remotely taking control of people's phones and stealing their data and money by signing them up for premium subscription services without the individual's knowledge.

The NCSC report concludes the government's proposed code of practice will have a positive impact and reduce the chances of malicious apps reaching consumers across different devices.

NCSC Technical Director Ian Levy said:

> Our devices and the apps that make them useful are increasingly essential to people and businesses and app stores have a responsibility to protect users and maintain their trust.
>
> Our threat report shows there is more for app stores to do, with cyber criminals currently using weaknesses in app stores on all types of connected devices to cause harm.
>
> I support the proposed Code of Practice, which demonstrates the UK's continued intent to fix systemic cybersecurity issues.

The code follows a government review of app stores launched in December 2020 which found some developers are not following best practice in developing apps, while well-known app stores do not share clear security requirements with developers.

The app stores call for views is part of the government's £2.6 billion National Cyber Strategy to ensure UK citizens are more secure online and is alongside other tough UK safeguards for people using internet-connected devices.

It is also part of the government's work leading international efforts to raise awareness on the need for security and privacy requirements for apps to protect users.

There are already tough data protection laws in the UK to protect people's data and these are enforced by the Information Commissioner's Office.

A new product security law making its way through parliament will place new

requirements on manufacturers, importers and distributors of consumer tech. They will have to ban easy-to-guess default passwords in devices and make manufacturers transparent about the length of time products will receive security updates alongside providing a vulnerability disclosure policy.

People should also follow the National Cyber Security Centre guidance to help secure smart devices.

Ends

Notes to Editors:

The eight-week call for views will run until 29 June 2022. App developers, app store operators and security and privacy experts are encouraged to provide feedback to inform the government's work in this area.

Following the call for views, we will review the feedback provided and will publish a response later this year. The review complements the government's upcoming digital markets pro-competition regime, including the Competition and Market Authority's market study into mobile ecosystems, which will create a more vibrant and innovative digital economy across the UK.