App security and privacy interventions - BCS Briefing

June 2022
This document
This is the BCS briefing to the DCMS consultation on ‘App security and privacy interventions’.

1 App security and privacy interventions
The UK government conducted a review into the app store ecosystem from December 2020 to March 2022, which found malicious and poorly developed apps continue to be accessible to users. The review concluded some developers are not following best practice when creating apps. The review also found

- All app stores share a common threat profile with malware contained within apps the most prevalent risk.
- Prominent app store operators are not adequately signposting app requirements to developers and providing detailed feedback if an app or update is rejected.

As a result of the review government is conducting a consultation on introducing a voluntary Code of Practice for all app store operators and developers. See the next section for further details of the proposed code of practice. Deadline for responses is June 29, 2022.

Government plan to introduce the Code on a voluntary basis. Depending on stakeholder feedback once the Code is introduced,

- the government will explore the challenges and opportunities of placing the principles of the Code on a regulatory footing.

2 Proposed Code of Practice
Stakeholders that would be affected by the proposed code of practice are:

- App Store Operators: The persons or organisations responsible for operating the app store.
- Developers: Persons or organisations which create or maintain apps on the app store.
- Platform Developers: Individual(s) responsible for producing the operating system, default functionality and the interface that enables third parties to implement additional functionality, such as through apps.

The code of practice covers the following key principles (each of these are expanded on in the consultation document here)
1. Ensure only legitimate apps that meet security and privacy best practice are allowed on the app store
2. Implement vulnerability disclosure processes
3. Keep apps updated to protect users
4. Provide important security and privacy information to users in an accessible way
5. Enterprise app stores shall be secured where provided
6. Promote security and privacy best practice to developers
7. Provide upfront and clear feedback to developers by app stores

3 Accompanying interventions

If the code is implemented government will also look at
- working closely with app store operators and consumer groups to ensure that any additional information provided for users as a result of the principles is clear and accessible
- how the ICO should explore the development of further tools and guidance to explain the concepts of data protection by design and default
- exploring the challenges and opportunities of placing the principles of the Code on a regulatory footing

Who we are

BCS is the UK’s Chartered Institute for Information Technology. The purpose of BCS as defined by its Royal Charter is to promote and advance the education and practice of computing for the benefit of the public.

We bring together industry, academics, practitioners and government to share knowledge, promote new thinking, inform the design of new curricula, shape public policy and inform the public.

As the professional membership and accreditation body for IT, we serve over 60,000 members including practitioners, businesses, academics and students, in the UK and internationally.

We also accredit the computing degree courses in over ninety universities around the UK. As a leading information technology qualification body, we offer a range of widely recognised professional and end-user qualifications.