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.

Forum focuses on bolstering UK's future resilience

The UK Resilience Forum (UKRF) met on Tuesday 3 May, bringing together stakeholders from across the private, public and voluntary sectors, as well as our emergency services, to work together on bolstering the UK's resilience.

Chaired by Lead Minister for Resilience and Minister for the Cabinet Office, Rt Hon. Michael Ellis QC MP, the Forum was established in July to strengthen the country's resilience by improving communication and collaboration on risk, emergency preparedness, crisis response and recovery.

Its membership builds on those with duties under the Civil Contingencies Act. It includes national, regional and local government, private and voluntary sectors, emergency services and utilities. There are also representatives who join as voices for communities and people impacted by emergencies, including Citizens Advice, National Emergencies Trust, and the Voluntary and Community Sector Emergencies Partnership.

Members were notified that the Civil Contingencies Act post-implementation Review was published on 1 April, which provides a framework for emergency preparedness in the UK and acts as a critical building block to make the UK as resilient as possible. Also, that the Biological Security Strategy Call

for Evidence had been completed.

Lead Minister for Resilience and Minister for the Cabinet Office, Rt Hon. Michael Ellis QC MP, said:

> Continuing to bolster the UK's resilience from domestic and global threats is vital, and the Forum provides space for a range of crucial organisations and partners to provide insight so we can ensure our emergency preparedness remains effective and aligned.
>
> We continue to identify key challenges on the horizon in order to effectively pivot resources to tackle risks, and to prioritise preparedness accordingly, working collaboratively to protect the UK.

> Effective partnership working across agencies is vital to ensuring that we keep our communities safe. The UK Resilience Forum is therefore a welcome and critical structure, which allows key stakeholders to better plan and prepare. Importantly, provides a way of sharing sector experience and learning with government so we can work together on how best to deliver more effective joint agency responses in the future.

The UKRF will meet every six months.

As part of the Government's ongoing commitment to transparency, a note of each UKRF meeting will be published.

New Ofqual 3-year plan puts students and apprentices at its heart

Ofqual's new 3-year plan announced today (4 May) sets out its ambition for the future of qualifications that are sought after, fair, accessible, valued and world class. The plan details the work Ofqual will do towards this, with the interests of students and apprentices at its heart.

Ofqual has a pivotal role to play in leading, influencing and enabling innovation and transformation in assessment and qualifications. New approaches to assessment, including the use of technology, have the potential to improve quality and fairness for students and apprentices and to strengthen the resilience of how qualifications and assessments are delivered.

Ofqual will work with awarding organisations to harness greater innovation and the use of technology to promote assessments that are valid, efficient and implemented safely in the interests of students.

Ofqual will oversee the reintroduction of exam-based assessment in 2022 across general, vocational and technical qualifications where they were cancelled due to the coronavirus (COVID-19) pandemic and will work to secure trust and confidence in awarding arrangements for 2022 and beyond.

Ofqual will look to the future demand for technical qualifications by working in partnership with Institute for Apprenticeships and Technical Education on technical qualifications, T Levels, higher technical qualifications and apprenticeship end-point assessments. The introduction of new Digital Functional Skills qualifications into the market also signals that the qualification landscape will be changing over the next decade and Ofqual will be developing and consulting on arrangements to secure high-quality qualifications as part of the government's post-16 qualifications review.

Ofqual will regulate to ensure that exams and assessments become more accessible for all students, including students with special educational needs and disabilities and students new to this country for whom English is an additional language.

Ofqual will transform how qualifications can be chosen and compared by building an interactive Register of Regulated Qualifications to make the qualifications market clearer and easier to navigate.

Ofqual will make the qualifications market work better in the interests of students by promoting transparency and by helping all those that take and use qualifications to make informed choices, including on the basis of price. Regulation must support a coherent and navigable qualifications market for students, apprentices and employers.

Ofqual Chair Ian Bauckham said:

> Ofqual's deep assessment expertise, access to expansive data and our convening power afford us a unique role in shaping the future of qualifications and assessment. We are ambitious in that goal. Regulation must enable good innovation that is in the interests of students and apprentices.
>
> The pandemic has, rightly, catalysed questions about not if, but when, and how, greater use of technology and onscreen assessment should be adopted. All proposed changes need to be carefully assessed for their impact on students, including those with special educational needs and disabilities. It is right that we use research and evidence to challenge existing practice so that we continue to improve what we offer for students and apprentices.

Chief Regulator Dr Jo Saxton said:

> I am delighted to be publishing our 2022 to 2025 corporate plan – the first in my tenure as Chief Regulator. At its heart is my personal commitment that the interests of students and apprentices will be the compass that guides us on every decision and action. They will be our true north. I know the power of qualifications from my own personal experience and from my time working on the frontline of schools in some of the most disadvantaged areas in the country. Qualifications open doors. They are a passport to new opportunities and possibilities. To fulfil that role they must be trusted, understood, good quality and fair.
>
> This corporate plan sets out the work that Ofqual will do to make sure that regulated qualifications are just that. I also want to make it easier for students to see a clearer choice of options. We are also looking at the future landscape of qualifications and so will be developing and consulting on arrangements to secure high-quality qualifications as part of the government's post-16 qualifications review.

Russian attacks on civilian infrastructure in Ukraine: UK statement to the OSCE

Thank you, Madam Chair, again for convening us today and bringing together panel experts for such a timely discussion that has highlighted the impacts on civilians when critical services are damaged, as well as the role of States in protecting these services in armed conflict.

As has been noted several times today but cannot be overstated, a little over a year ago, Russia joined with others at the UN Security Council to unanimously adopt Resolution 2573. Yet, in a flagrant breach of International Humanitarian Law, Russian bombers have, in recent weeks, repeatedly and remorselessly dropped targeted munitions on civilian infrastructure in Ukraine, including government buildings, hospitals, schools, and transportation.

Today we have heard the numbers of verified attacks on Ukraine's health facilities. Stretched healthcare facilities in the East are having to respond to growing reports of gender-based violence, including Conflict-Related

Sexual Violence. Earlier today, Prime Minister Johnson addressed Ukraine's Parliament, setting out a new package of military aid to enable Ukraine to defend itself as well as specialised civilian protection vehicles, and we will continue to provide humanitarian aid including generators to support vital services to keep running.

The dangers of this war transcend borders. As described by our keynote speaker, the world has witnessed concerning attacks on Ukrainian nuclear facilities, demonstrating Russia's reckless attitude to nuclear safety and security. The UK will continue to support neighbouring countries, including those which are hosting refugees. We continue to provide regional support in the cyber space, including by sharing threat information. For instance, we have recently launched our new programme supporting Georgia to implement its new National Security Strategy, focusing on incident management, information sharing, and the cyber awareness of vulnerable groups.

At times of heightened international tension all critical service providers must be vigilant to the risk of cyber compromises. Earlier this month, the UK joined our international partners to share updated mitigation advice against state-sponsored and criminal cyber threats. Strengthening the relationships between government departments, regulators, and private sector operators is key to ensuring the latest threats, risks and vulnerabilities are understood and mitigated effectively.

States should, where possible, make publicly available their approaches to cyber security and resilience, including how they relate to critical infrastructure protection. The UK routinely publishes this information including guides on how to effectively detect, respond to and resolve cyber incidents, and crucially where organisations can find support from certified Cyber Incident Response companies assessed against clear published standards. Sharing best practice in approaches to critical infrastructure dependences and cooperating across borders are crucial elements of strengthening our international resilience.

Madam chair, we have entered a new world where service protection and resilience measures must not only be prepared to stand up to threats caused by non-state terrorist acts, but direct and targeted missile attack. As we enter the third month of President Putin's illegal and unprovoked war, not only do thousands of civilians remain in Mariupol, Kherson, Donetsk, Luhansk, and other cities, struggling to survive without food, water, warmth, and medical supplies, but the effects continue to mount around the world. The OSCE has a role to play to prevent knock-on crises in crime, trafficking, and terrorism, and the UK stands ready to support the Security Committee to that end.

Thank you.

Embajadas Británicas en México, Guatemala y El Salvador abordan retos para la libertad de prensa

World news story

Para conmemorar el Día Mundial de la Libertad de Prensa 2022, las Embajadas Británicas en México, Guatemala, El Salvador y Honduras organizaron una mesa redonda regional.

En la sesión también se abordaron los impactos de la disminución de los espacios democráticos para un periodismo seguro y abierto. También se discutió cómo la comunidad internacional puede ayudar a apoyar el periodismo independiente.

Jon Benjamin y David Lelliot, embajadores del Reino Unido en México y El Salvador respectivamente brindaron los discursos de apertura y clausura. Ambos destacaron la importancia de la libertad de los medios de comunicación como un componente clave de las comunidades democráticas prósperas:

“El intercambio libre de ideas es el motor del desarrollo, tanto económico como político y social. Esfuerzos dirigidos a reducir o limitar la libertad de medios de comunicación son contraproducentes”, señaló David Lelliott.

“En los últimos 15 días, más de 700 periodistas se han beneficiado de un reciente proyecto de formación impartido por la Oficina de la UNESCO en México, con el apoyo de nuestra embajada, del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y del gobierno federal”, recalcó Jon Benjamin, en relación al trabajo de la Embajada Británica en México para promover la libertad de los medios de comunicación y apoyar a las y los periodistas.

De acuerdo al Comité para la Protección de los Periodistas (CPJ), México es el país más peligroso del mundo para ser periodista fuera de una zona de conflicto. El CPJ informa que, de los 25 periodistas asesinados en todo el mundo en 2022 hasta ahora, siete han sido asesinados en México.

El Reino Unido mantiene su compromiso de promover el periodismo independiente en todo el mundo, esencial para construir sociedades abiertas, prósperas y democráticas. El debate sobre los retos de la libertad de los medios de comunicación a nivel regional ayudará a informar el apoyo del Reino Unido a los periodistas a través de proyectos tanto nacionales como regionales.

Published 3 May 2022