NCSC joins industry to offer unprecedented protection for public from scams

Data sharing collaboration will allow ISPs to instantly block access to fraudulent sites.

- National Cyber Security Centre develops capability with industry partners which protects UK citizens from scam websites
- Fraudulent sites will be blocked at scale and in real-time as a result of move
- New capability builds on the success of NCSC's takedown service, which has removed over 2.7 million scams in the past year

CITIZENS across the UK are set to benefit from a landmark partnership between government and industry which will see access to scam websites instantly blocked.

A new data sharing capability developed by the National Cyber Security Centre (NCSC) – a part of GCHQ – in collaboration with industry partners will present Internet Service Providers (ISPs) with real-time threat data that enables them to instantly block access to known fraudulent sites.

The new capability is being made available to all ISPs operating in the UK and will significantly bolster the nation's ability to protect citizens from cyber criminals. In due course, even more defenders will be invited to join, including browser and manager service providers.

The NCSC has previously highlighted the problem of scam websites, including fake news pages where celebrities such as Ed Sheeran and Sir Richard Branson appear to be endorsing investment schemes that seek to trick people into parting with their money.

Announced on day two of the government's flagship cyber security conference, CYBERUK 2022, the new capability will complement the work of the NCSC's Takedown Service, which removed more than 2.7 million scams from the internet last year alone.

Sarah Lyons, NCSC Deputy Director for Economy and Society, said:

"Cyber criminals continuously seek to deploy devious methods to trick us into sharing personal or financial details and it's vital we stay ahead of them.

"This landmark partnership with internet service providers means that scams can be blocked from ever reaching our screens and reinforces the UK's armour in protecting the public from online harms."

BT, which works with the NCSC on a number of initiatives, welcomed today's announcement.

Kevin Brown, Managing Director of BT Security, said:

"Online scams continue to cause massive harm, from the financial losses suffered by individuals and businesses, through to the continued erosion of our trust in the internet and the communications we receive.

"To tackle this, organisations across the public and private sector have to collate resources and openly share intelligence and best practice, even with their peers and competitors.

"We're proud to have worked closely with the NCSC to develop this initiative, which will significantly increase the speed at which we share data and block scams."

If people do encounter a suspicious website, the NCSC's website reporting tool allows anyone to send URLs to be analysed and, if found to be malicious, a notice will be issued to the host requesting that the site be removed.

People who receive suspicious emails should forward them to report@phishing.gov.uk and suspicious texts to 7726 where they will be analysed by the NCSC and removed if found to be fraudulent.

PUBLISHED

11 May 2022

WRITTEN FOR

Cyber security professionals Large organisations Public sector Self employed & sole traders Small & medium sized organisations You & your family

NEWS TYPE

General news