RailBusinessDaily

GCHQ gives advice to construction businesses

February 24, 2022

Businesses that work in construction are now being offered cyber security guidance from a department in GCHQ.

The world-famous intelligence and security agency is providing first-of-its-kind advice to businesses, many of which help build our rail network.

The Cyber Security for Construction Businesses guide from the National Cyber Security Centre (NCSC) – a part of GCHQ – provides tailored, practical advice for the industry on how to protect their businesses and building projects.

Construction businesses of all sizes continue to be targeted by cyber attackers due to the sensitive data they hold and the high-value payments they handle.

The guidance, launched with the Chartered Institute of Building (CIOB), is aimed at small and medium-sized firms as businesses rely more on digital tools and ways of working, such as using 3D modelling packages, GPS equipment and business management software.

The guide offers practical advice for each stage of construction, from design to handover, and sets out the common cyber threats the industry faces, including from spear-phishing, ransomware and supply chain attacks.

Sarah Lyons, NCSC Deputy Director for Economy and Society Engagement, said: “As construction firms adopt more digital ways of working, it’s vital to put protective measures in place to stay safe online – in the same way you’d wear a hard hat on site.

“That’s why we’ve launched the new Cyber Security for Construction Businesses guide to advise small and medium-sized businesses on how to keep their projects, data and devices secure.

“By following the recommended steps, businesses can significantly reduce their chances of falling victim to a cyber attack and build strong foundations for their overall resilience.”

Construction Minister Lee Rowley MP said: “Data and digital technology is helping to make the construction industry more productive, competitive and sustainable. However, with this new technology comes threats that businesses must be wary of and take action to defend themselves from.

“This guide provides firms with easy to follow, practical advice to improve resilience to online threats, which will help to ensure projects are delivered on time and securely.”

Caroline Gumble, Chief Executive of the Chartered Institute of Building, said:“The consequences of poor cyber security should not be underestimated. They can have a devastating impact on financial margins, the construction programme, business reputation, supply chain relationships, the built asset itself and, worst of all, people’s health and wellbeing. As such, managing data and digital communications channels is more important than ever.

“This guide provides a timely opportunity to focus on the risks presented by cyber crime, something that has been highlighted by CIOB for some time. We’re now delighted to partner with the National Cyber Security Centre (NCSC) and the Centre for the Protection of National Infrastructure (CPNI) to produce another invaluable resource.”

The new guidance is split into two parts: the first aimed at helping business owners and managers understand why cyber security matters, and the second aimed at advising staff responsible for IT equipment and services within construction companies on actions to take.

The advice outlines seven steps for boosting resilience, covering topics including creating strong passwords; backing up devices; how to avoid phishing attacks; collaborating with partners and suppliers; and preparing for and responding to incidents.

The majority of businesses in the construction industry fall under the small and medium-sized categories.

Last year, a survey by the Department for Digital, Culture, Media and Sport of all types of businesses found more than a third of micro (37%) and small businesses (39%) reported falling victim to a cyber security breach or cyber attack in the previous year, with this increasing to 65% for medium-sized businesses.

The NCSC is committed to helping UK organisations of all sizes improve their cyber resilience and has a published a range of guidance on how to defend against online threats on its website.

For smaller construction businesses without dedicated IT staff, the NCSC’s Small Business Guide offers further affordable, practical advice on how to stay secure online, while larger organisations can find guidance in the 10 Steps to Cyber Security collection.