Coronavirus v cybersecurity

Every week, Maddyness curates articles from other outlets on a topic that is driving the headlines. This week, we look at how the coronavirus is a vulnerable time for companies to experience cyberattacks and the need for strengthening cybersecurity.

A public fund to develop tech tackling cyberattacks

The Defence and Security Accelerator (DASA) has announced a £1M fund to develop technology that predicts and counters cyber-attacks, in Phase 2 of the DASA 'Predictive Cyber Analytics' competition. This work will develop, adapt and merge the novel approaches explored in Phase 1 of the competition, to proactively defend deployed UK military systems and networks from the rapidly growing threat of offensive cyber action from aggressive adversaries. Read more on GOV UK

Threat on the UK Governments

177 cybersecurity and privacy experts have signed an open letter to the UK government asking it to ensure the contact tracing app it has deployed to track the spread of coronavirus to be sure that it doesn't get used as a mass-surveillance tool. NHSX, the NHS' digital experimental arm, says the app will be

rolled out in Britain in the next two to three weeks. Read the full story on Business Insider

Threat on online streamers personal finance

BRITONS have been warned to take extra care during the coronavirus lockdown, as criminals move towards online streaming websites to harness more victims. Hundreds of copycat websites have surfaced, imitating popular streaming companies like Netflix, Amazon and Disney. Criminals have created counterfeit websites to harvest personal data from unsuspecting people, acquiring information such as bank details and credit card information. This could leave streaming users seriously out of pocket. Read more on the Express

The National Cyber Security Centre takes down 2,000 online scams

In the last two months, the cyber-specialised agency – which is part of the intelligence organisation GCHQ – has taken down 471 coronavirus-related fraudulent online stores, 555 sites spreading malware and 200 more dedicated to phishing, uncovering 832 frauds in which an initial payment is sought on the promise of the return of a large sum of money. Read more on Civil Service World

Cybersecurity principles for retailers

As the COVID-19 outbreak continues to threaten the global economy, it has also led to some significant threats relating to cybersecurity in the retail industry. The retail industry is the hotbed for customers' personally identifiable information (PII) and is also linked to their payment data needed to complete transactions. Read the story on My Total Retail

Case study: Thales helps NHS Wales to maximise its cybersecurity

Amid the coronavirus, healthcare organisations across the world are being targeted by cyberattacks at a time when they can least afford to be compromised. This has seen the cybersecurity industry unleash a wave of support for healthcare, for NHS Wales support has come from the defence

specialist Thales. Read more on Verdict

Read also

Cyberattacks increase as WFH continues

Read also

Global cybersecurity trends to watch in 2020

Article by MADDYNESS