Unsplash @Philipp Katzenberger

Cyber attacks proving challenging for businesses in 2020

The coronavirus pandemic continues to cause mayhem for businesses around the world, but this ongoing catastrophe has also created an environment where fraudsters and online criminals thrive.

In April 2020 the World Health Organisation (WHO) reported five times more cyberattacks against their staff and systems than the same period in 2019. Businesses were specifically targeted following the launch of the government's Coronavirus Job Retention Scheme (CJRS) So 2020 is clearly an exceptional year in many ways and has already tested the resilience of even the most experienced business owners.

Businesses targeted due to coronavirus

The attack on businesses immediately after CJRS became 'live' was a sustained attempt by cybercriminals to steal a business' bank details with a view to intercepting government payments or directing businesses to transfer money to rogue operators.

So how can you protect your business from an increasing risk of cyber attacks in a world where the global health pandemic is causing widespread uncertainty and apprehension?

What is a cybersecurity threat and how can you safeguard your business?

Online scammers and fraudsters thrive in situations of fear and chaos, taking advantage of their targets' lack of focus. The measures put in place to protect staff and the economy from coronavirus include extensive home working, but systems may be less secure as a result, and employees have limited IT support.

This, in turn, has created the perfect environment for cybercriminals to breach security by attacking businesses with phishing emails and ransomware.

Phishing attacks

The aim of a phishing attack is to obtain sensitive information about an individual or business. This could include an email address, or in the case of the job retention scheme, business bank details.

The attacker sends an email that appears to have originated from a trusted or official source, such as HMRC, typically in relation to a current event or for a plausible reason. The email generally contains an attachment or link to a malicious website that looks legitimate.

Ransomware

Connecting to a corporate network from home can create cybersecurity gaps where fraudsters take advantage of a more complex connection process, which could potentially lead to a ransomware attack. Essentially, ransomware is malicious software that causes an entire computer system to freeze.

The fraudsters' aim is to collect a ransom to release the system, leading to an extremely challenging dilemma for the business involved. Hiring specialists to deal with the problem is likely to be very expensive, possibly too costly for many businesses, but if the ransom is paid there's no guarantee the fraudsters will do as they say.

So how can this situation be avoided?

Improving cybersecurity in 2020

Understanding how cybercriminals operate and how they might attack business is the first step in safeguarding sensitive and critical information. It's important to keep up-to-date with the latest cyber-attack methods and pass this information on to employees.

Installing antivirus and anti-malware software on all devices including tablets and smartphones used for work is one of the first steps to take, and making sure the firewall is switched on also protects the network.

As far as phishing attacks are concerned, business owners/employees should:

- Assume that any email could be a phishing attack
- Hover their mouse over any links in emails to check the destination URL, without actually clicking on the links
- Send out reminders to staff about phishing emails, how they might appear, and what to do if emails seem suspicious
- Run software updates regularly to 'patch' any known issues

Anyone running a business faces unprecedented challenges in 2020. The effects of this global health emergency are far-reaching and it's crucial not only to consider the high risk of a cyber attack taking place but to keep pace with new developments in cybersecurity as a whole.

Keith Tully is a partner at Real Business Rescue, a business recovery and restructuring specialist for company directors in distress. He's specialised in financing a company, business recovery options, business exiting strategies, director support and COVID-19 support for businesses.

Read also

11 startups tackling cybersecurity in the UK

Article by KEITH TULLY