BEWICA

Published 07/04/2020

Cyber risks and covid-19

One virus is enough. Don’t let hackers give you another

As the Coronavirus pandemic continues to force many businesses into difficult financial positions, the threat of cyber security is often pushed to the back of owners’ and employee’s minds.

However, with so many employees now working from home, the threat to businesses from cyber attacks and cyber criminals is on average far higher than it might have been previously.

In this article we explain some of the key risks to businesses that have increased due to the Coronavirus and some of the steps employees and business owners can take to minimise their impact.

Phishing emails are on the rise

Phishing attacks are all about social engineering, and the spread of coronavirus is the perfect opportunity for hackers to impersonate government bodies or healthcare institutions and exploit people’s fears and concerns about the development of this virus.

Some of the consequences of falling for one of these phishing scams are stolen passwords, compromised business emails and the downloading of malicious files onto devices which might lead to a ransomware attack.

During this time of uncertainty, hackers know that people are looking for advice and health information on the spreading of the virus. By impersonating sources that people trust, hackers know that the likelihood of someone clicking on an email is high.

Attacks to your home Wi-Fi

Home networks generally have a wide variety of devices connected to them. In an office environment, the only devices you would likely have connected are smartphones, printers and laptops or computers. In a home environment, additional devices could include video-games consoles, security cameras, smart TV's and IoT devices such as light bulbs and thermostats.

The more devices that are connected to a network, the higher risk of one of these devices having a vulnerability which allows hackers to gain access to your network. With such access, hackers could monitor your internet traffic and gain admittance to anything un-encrypted such as company emails and communication, and potentially even bank account details and login credentials.

What can you do to protect yourself and your business?

1 Be on the lookout for any suspicious emails

If you think you have received a phishing email, it is important not to reply or click on any links. You should always confirm the identity of the person through another method of communication such as phone or company instant messaging.

Never transfer funds using bank details provided over email without verifying them with the recipient over the phone.

2 Use strong passwords

Passwords are the key to accessing all your data, therefore the use of strong and secure passwords is essential to ensuring your information remains confidential and safe.

The National Institute of Standards and Technology (NIST) has proposed the following technique to create easy to remember, strong passwords:

Use passphrases instead of words. For example, memorise 3 words that are easy for you to remember, replacing some letters for numbers and adding special characters, which as a result will generate a hard-to-guess, but easy to remember password.

3 Enable 2-Factor Authentication (2FA)

Using 2FA on all your critical applications (email, messaging, banking etc) will help prevent your accounts from being hacked.

To find out if the applications or web services you use support 2FA, we recommend searching for them on https://twofactorauth.org/.

4 Use Antivirus

If you use Windows 10, you should make sure to turn Windows Defender on to be protected against malware in your computer.

Alternatively, you can use another reputed antivirus. Here is one source that tests the performance of different antivirus programs across operating systems: https://www.av-test.org/en/.

5 Strengthen your Wi-fi security

Change the default name of your home Wi-Fi, change the default password to a unique and strong password and enable your Wi-Fi encryption (WPA2).

6 Use a VPN to connect to your business resources

A VPN works like a tunnel, so every time you log in to an application your information will be encrypted.

See more recommendations regarding VPN's on the NCSC website: https://www.ncsc.gov.uk/collection/mobile-device-guidance/virtual-private-networks

Bewica cyber insurance and Covid-19

Over the last couple of weeks Bewica has received a number of questions from clients about how Coronavirus impacts cyber insurance coverage.

Below are some of the most frequent questions and our answers to them:

Does Bewica cyber insurance cover working from home?

Yes, provided that the security requirements you agreed to upon purchasing the policy continue to be met such as antivirus being in-place on company devices.

Is there any impact on claims service?

While our 24/7 breach response hotline call centre is presently operating, this may change in the current unprecedented situation. We ask that you use the email address; cyber@ctplc.com to report any new cyber incidents.

This email is monitored 24 hours a day, 7 days a week by a distributed team of incident managers who will call you back to provide assistance within 2 hours of your email, although often it is within 15 minutes.

Is Bewica providing any additional help to businesses to reduce risk during this time?

All our policies include access to our cyber risk platform which offers tools such as phishing training, addressing one of the key risks that have increased during the Covid outbreak.

To get access to the cyber risk platform, please visit our sign up page and simply enter your policy number to start setup. Else if you prefer you can send us an email to contact@bewica.com or ask your broker to help you get access.

BEWICA

Crown House, 27 Old Gloucester Street
London, WC1N 3AX

contact@bewica.com
020 3026 5840