timico®

Keeping your business secure during the Coronavirus outbreak

In these uncertain times, it’s more important than ever that we all take sensible precautions to ensure we remain safe. But with a growing number of organisations implementing remote working practices, there are other viruses beyond COVID-19 that businesses and their employees need to be aware of.

The BBC reports an alarming spike in email scams linked to Coronavirus targeting individuals and businesses alike. Cyber-criminals are sending a variety of phishing emails preying on fears of the pandemic, in attempts to infect computers with malware and steal critical information.

While the increased frequency of these types of scams is concerning, if businesses and their employees remain vigilant and follow best practice advice, the chances of systems becoming infected are significantly reduced.

National Cyber Security Centre (NCSC) guidance explains how organisations can defend themselves against malware and ransomware attacks. In this article, we have outlined the NCSC’s four key tips to help your business thwart cyber-criminals and protect your IT infrastructure.

TIP 1: Make regular backups

Unfortunately, it’s not possible to completely eliminate the threat of malware infection, and at some point, it’s likely your system will become infected. So, if you fall foul of a ransomware scam, it’s vital that you’ve backed up your most critical data.

Every organisation will have different priorities, but you should identify the most important files for your business and ensure you have up-to-date backups.

TIP 2: Prevent malware from being delivered to devices

Make it harder for viruses and malicious content to reach your network by filtering to permit file types you would expect to receive, blocking known malicious websites and inspecting content actively.

This can be done by network services rather than users’ devices.

TIP 3: Prevent malware from running on devices

With malware infection inevitable at some point, the NCSC recommends adopting a ‘defence-in-depth’ strategy, using layers of defence with mitigations at each stage to help you identify malware and prevent it from causing significant damage to your organisation.

For instance, utilising device-level security features you can centrally manage which applications are permitted to run on devices connected to your network. Other best practice recommendations include using antivirus and anti-malware products, and ensuring devices have the latest security updates.

TIP 4: Limit the impact of infection and enable rapid response

There are several steps you can take to ensure your business recovers from an infection quickly. These include, but aren't limited to:

1. Preventing lateral movement so attackers can't gain further access into your network
2. Using two-factor authentication
3. Removing obsolete platforms from the rest of your network
4. Reviewing and removing user permissions on a regular basis
5. Developing an effective incident response plan

The NCSC's guidance also includes advice on what to do if your organisation has already been infected, as well as providing more detailed information on the steps outlined above.

We would recommend sharing the guidance with stakeholders in your business as well as the wider NCSC website, which is full of best practice advice on combating cyber- criminals and keeping businesses and individuals safe.

DID YOU KNOW FINANCIAL SUPPORT FROM THE GOVERNMENT IS AVAILABLE?

The Government has announced a series of measures to help businesses during these challenging times.

To find out more about available business support, visit:
www.gov.uk/government/publications/guidance-to-employers-and-businesses-about-covid-19/covid-19-support-for-businesses