Message Sent By
Sian Rivers (Police, Communications Officer, HQ)

Protect Your Online Security Throughout the Coronavirus Pandemic

We have already seen an increase in cyber attacks emerging at a national level against a variety of targets since the beginning of the coronavirus (COVID-19) pandemic in the UK.

We encourage companies and individuals to consider amplified security measures at this unprecedented time and adhere to the following advice:

Ransomware attacks in particular are on the rise. Ransomware is a malicious form of malware that encrypts your files and prevents you from accessing your computer, data or systems. It can spread throughout a network, potentially having a huge impact on an organisation.

Victims are often then asked to make a payment in order to gain access to files again. There is no guarantee paying will get access back, therefore it's important to regularly back up your business critical files and data, meaning you can recover your data without having to pay a ransom.

For more information on protecting your business from Ransomware see the guidance from the National Cyber Security Centre here: https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Home working

Due to the advancement of the coronavirus and subsequent advice from the Government, employees are increasingly encouraged to work from home or remotely, where possible. While this won't be new to some, companies will likely have an increased number of employees working from home than normal and for a longer period of time.

Follow our tips to stay secure whilst working remotely:

- Change default passwords on you home Wi-Fi router to prevent hackers accessing your network.
- Use strong and unique passwords on every account and device. Consider using two-factor authentication (2FA) which is a second piece of evidence you provide to prove it's definitely you logging in.
- Software updates contain vital security patches - keep all devices, apps and operating systems up to date.
- If you're working in a more public place use a privacy screen and tether using a 3G/4G connection instead of an untrusted Wi-Fi hotspot.
- Only use software your company would typically use to share files. Refrain from using your personal email or 3rd party services unless reliably informed otherwise.

Find out more about working from home here: https://www.ncsc.gov.uk/news/home-working-increases-in-response-to-covid-19

Phishing

Cyber criminals are exploiting the coronavirus as an opportunity to send phishing emails claiming to have important updates or encouraging donations, impersonating otherwise trustworthy organisations.

Ensure you and your staff remain vigilant and informed on spotting suspicious emails. Don't click on links if you're in any doubt, or contact the sender directly to verify.

Guidance on phishing emails can be found here: https://www.ncsc.gov.uk/guidance/suspicious-email-actions

If you have been a victim of a cyber crime, please report it to Action Fraud on 0300 123 2040, or via their website at https://www.actionfraud.police.uk