Contact: Brent McDonald – Inspire Insurance
Phone: 02476 998924
Email: communications@inspireinsurance.co.uk

Keeping Remote Staff Cyber-Secure During the Pandemic

COVENTRY, 14th April 2020 – The coronavirus disease 2019 (COVID-19) pandemic has resulted in unprecedented workplace changes for organisations across industry lines. While the government is enforcing a UK lockdown, requiring individuals to practise self-isolation and social distancing, employers like you must make necessary adjustments to allow your staff to work from home. However, implementing a teleworking programme carries a wide range of cyber-risks. Specifically, having your employees work from home can increase their vulnerability to cyber-attacks—which could result in costly consequences for your organisation.

In fact, recent research from cyber-experts revealed that hackers across the globe have been taking advantage of remote workers in the midst of the COVID-19 pandemic by utilising a variety of phishing scams. These scams, which typically appear as fraudulent emails from trusted organisations such as Public Health England or the World Health Organisation, trick victims into clicking on malicious links—thus allowing hackers to infiltrate their devices and access sensitive data. These attacks have already resulted in losses totalling nearly £1 million, and they aren't stopping anytime soon.

Now more than ever, it's vital to ensure your teleworking programme is secure by providing employees with adequate cyber-security resources. Review the following guidance for best practices on how to keep remote employees (and in turn, your overall organisation) protected from cyber-attacks during these unprecedented times.

Prepare Your Technology

First, it's important to assess your workplace technology to ensure it possesses proper cyber-security features to combat teleworking risks. At a glance, your organisation's software should have these key characteristics:

A virtual private network (VPN)

Having a VPN allows your employees to utilise a private, protected network connection. VPNs provide numerous cyber-security features, such as hiding users' IP addresses, encrypting data transfers and masking users' locations. If you don't already have a VPN, you are missing a crucial step in implementing a secure teleworking programme. If you do already possess a VPN, make sure it is fully patched. Further, keep in mind that additional licences, capacity or bandwidth may be required if your organisation normally has a limited number of remote employees. For more VPN guidance, click here.

Restricted access controls

Be sure that all remote work technology possesses the same account access restrictions as that of your on-site software. Only allow competent, qualified and trusted staff to have access to sensitive company data.

Encryption capabilities

Apart from having a VPN, make sure that your remote work technology has additional encryption capabilities to keep sensitive data protected in the event that an employee's device becomes lost, stolen or compromised.

Antivirus and malware protection

Lastly, require all remote work technology to be bolstered with the latest antivirus, malware and firewall protection software.

Prepare Your Employees

After you have prepared your technology, it's time to provide employees with robust resources and training to ensure a cyber-secure teleworking programme. This is especially important for employees who haven't worked from home in the past or lack advanced digital skills. Consider providing staff training on the following topics:

Conducting key operations

Be sure to educate your staff on how to conduct common teleworking practices, such as video teleconferencing and document sharing. Create written instructions for employees who need additional support.

Taking care of technology

Encourage employees to log out of their devices when they are finished working for the day and store all workplace technology in a secure, protected location.

Creating strong passwords

Require all employees to create strong passwords for their company accounts and devices. These passwords should be an appropriate length (at least 10 characters), difficult to guess and contain a variety of special characters (eg capital letters and punctuation marks). Employees should update their passwords on a routine basis.

Using removable media

Using removable media (eg USB drives) can carry a variety of cyber-security risks, seeing as they often contain sensitive information and are easy to misplace. With this mind, cyber-experts recommend prohibiting your employees from using removable media for work purposes. However, if you must use removable media, be sure to educate staff on safe use and storage practices. For additional removable media guidance, click here.

Utilising personal devices

If you allow employees to utilise personal devices for work purposes, make sure you implement and enforce a bring your own device policy. Only allow competent, qualified and trusted employees to use their own devices.

Conducting regular updates

Be sure employees know how to conduct regular software updates on all workplace technology. If you allow staff to use personal devices for work purposes, ensure they know how to conduct software updates on this technology as well.

Detecting signs of phishing

Educate your employees on the following common signs of phishing scams:

- The email requests the recipient to share sensitive personal information or account credentials.
- The email claims to be from a trusted contact but isn't from the correct email address.
- The email contains glaring errors, such as typos, poor grammar, false information or false imagery (eg an incorrect company logo).
- The email does not address the recipient by name or has been sent to a long list of other recipients.
- The email is from an unknown sender or a contact that your organisation rarely communicates with.
- The email contains links that direct you to the wrong website or asks you to log in to an account.
- The email claims to be urgent, comes across as demanding or is threatening.

Reporting cyber-concerns

Finally, make sure that all employees know how to report any cyber-concerns that they might experience while teleworking. Staff should report these problems to their direct supervisors and your IT department, if needed. If

an employee needs to report a serious concern, such as a cyber-attack, they should also know how to contact Action Fraud.

For additional teleworking training guidance from the government, click here.

Have a Cyber-incident Response Plan

In addition to preparing your technology and your staff, make sure your organisation has a cyber-incident response plan in place to help limit the potential consequences in the event of a cyber-attack. Educate all employees on this plan and test it regularly for effectiveness. Make updates to your plan as necessary.

Purchase Robust Cyber-insurance

As cyber-attack trends continue to evolve during these unprecedented times, so should your cyber-insurance policy. Be sure to regularly review and update your policy to avoid the ruinous ramifications of a cyber-attack.

For more information and cyber-insurance solutions, contact us today.

###

Inspire Insurance is specialist commercial insurance broker specialising in niche and bespoke insurance for firms including Cyber Insurance, Professional Indemnity, Motor Fleet, Liabilities and Construction Bonds. Our Professional Risks team have recently developed a Cyber Risk Exposure Tool to help businesses analyse their cyber exposure quickly and for free, for more details visit https://inspireinsurance.co.uk/cyber_risk_exposure_test.aspx.