May 2020

CYBER SAFETY FOR YOUR BUSINESS DURING CORONAVIRUS

NFU Mutual
BUSINESS INSURANCE

INTRODUCTION

Following the Government restrictions put in place to help stop the spread of Coronavirus, many businesses have had to quickly adapt their ways of working, this has included providing more employees with the ability to work from home.

However, the speed at which many businesses have had to adapt has highlighted several potential data security and IT related issues.

This guide will help you identify some of the key risks and offers some simple, practical steps to help reduce any potential impact to your business.

IT EQUIPMENT AND SUPPORT

To ensure you have the right processes and technology in place to prevent a cyber-attack and to deal with any possible effects, you should consider undertaking a review of your current cyber strategy.

If your business doesn't have one, you could use the Government's Cyber Essentials Scheme. This allows you to obtain an official certificate of compliance to provide assurance to your customers that your online operations are secure and compliant.

Once your strategy is in place it's important to review this regularly, particularly when we are in unprecedented times. Here are some things you need to consider:

Supply company equipment – Wherever possible you should supply staff with equipment to allow them to work from home and avoid asking them to use their own personal equipment, as it increases the risk of an unknown and potentially unsecured device being able to access secure business networks.

Check your security software – If you can provide your staff with equipment, ensure that it is secured against common cyber-attacks before sending to them. This includes the creation of user accounts, licensing and installation of security software, and appropriate instruction for safe use. By doing this you are lessening the risk of your business being exposed to common cyber threats.

Add password authentication measures – Poor password security practices are sadly still commonplace, so by implementing second security checks, you will be providing more barriers for potential hackers to get through.

Control other software used – As your business adapts to new ways of working, you may find that new software is needed to enable your staff to communicate with each other, such as introducing video conferencing services. Often these are cloud based software subscriptions that they can download themselves. Although allowing them to do this will be quicker than going through a procurement process, it could increase the possibility of security concerns being overlooked. Recommend that your employees use the company approved and trusted supplier.

Check your IT support contract – If you use an external IT support company, make sure that the contract you have with them includes cover for security of devices sent out for home working.

Share guidance and advice with suppliers – Don't forget you're not in this alone. Your suppliers are likely to be experiencing similar challenges and therefore may be exposed to the same threats. So, talk to them and share your advice and guidance to help one another.

Manage third party risks – Make sure third parties have appropriate measures in place and that they're not likely to cause a risk to the way in which your business operates. This is especially important if you have a dependency on a supply chain. You might wish to review current processes and conduct additional checks to see how they're protecting their data.

WORKING FROM HOME

For some of your staff this may be the first time that they have had to work from home and been entrusted with company property outside of the office environment. They therefore may need advice and guidance on best practice for doing this - here are some tips on the type of guidance they may need:

- Inform them of the dangers of misusing the device for personal purposes, e.g. web-browsing, personal social media usage or downloads, which can increase the risk of exposing the device to malware.
- Make sure they are aware that other members of their household MUST NOT use the device, if they do it could lead to exposure of sensitive business information, or again open up the risk of exposing the device to malware.
- Highlight the dangers of poor safety practices, for example leaving the device on a table overnight, visible from a window. This may make the device attractive to opportunistic burglars.
- Reinforce the dangers of printing, or making copies of sensitive business information to their own personal media and encourage them not to use external devices such as a USB flash drive.
- Remind employees of data protection regulations, for example, that sending work emails to personal accounts and printing off confidential information means that the company is at risk of a data breach. Consider adding in additional restrictions and rights in your file structure to stop unauthorised printing.
- Ensure any training relating to your policies and technology is undertaken and keep communication about it frequent to ensure it's kept top of mind.

SOCIAL ENGINEERING SCAMS

Hackers and scammers are taking advantage of the current circumstances that many businesses are having to operate in to commit cyber crimes. Most of the scams make use of email and text messages and often seek to get usernames and passwords, bank account details, or spread malware. However, some will still use the telephone, where they pretend to be from an authority seeking your bank account or payment card details.

Beware of the following scams that are already active:

- HMRC scams: Fake emails pretending to be from HMRC, providing a link to make claims for Government support. These emails entice the user to give up confidential account or bank information. They try to capitalise on business desperation to access working capital.
- Fake offers for equipment: Similar to the above, emails are circulating advising on access to preferential deals on personal protective equipment (PPE). These are often linked to new e-commerce websites that will take your payment, but not deliver any products.
- Fake NHS advice: Emails and text messages are sent claiming to represent the NHS. These often request the creation of an account on a fake NHS website, which allows scammers to capture email addresses and common passwords for use in other scams.
- Unrecognised bank transactions: Everyone is being cautious with their finances. Scammers are sending text messages pretending to be from a bank, claiming you have unauthorised or unrecognised transactions. Such a claim can be alarming, especially during a time of heightened worry. The scammer is hoping your concern will make you click on their link. Often this takes you to a fake website used to collect your login information, account details or security responses.

Be extra cautious with every item of communication you receive in the current environment. Scammers are seeking to capitalise on desperation, concern and worry. These emotions can make us more susceptible to fraud.

THINGS TO CONSIDER

- [ ] Think before you click. Scammers are trying to manipulate you into making decisions quickly. Stop and think. Don't be pressured.
- [ ] If you are seeking information on Coronavirus, ensure you visit only authentic Government websites, such as gov.uk/coronavirus.
- [ ] If it sounds too good to be true - it probably is. This is how scammers lure their prey. If you are being offered cheap stock, or a commercial opportunity, be extra careful when opening any files or clicking any links.
- [ ] If you are unsure on advice you've heard, check with your professional advisers. We must all do our part to stop the spread of fake news and false information. If you see such information, and it is indeed fake, call it out to protect yourself and others.
- [ ] The Government is the definitive resource for all state-offered support. Third party websites are not reliable or may not be up-to-date. If in doubt, contact your accountant to seek verification or advice.
- [ ] Remember that you need to report any personal data breaches to the ICO (Information Commissioner's Office) within 72 hours of becoming aware of them. If your business fails to comply with GDPR regulations there are large financial penalties.
- [ ] For additional advice to help protect your business against possible impacts during the majority of cyber attacks, The National Cyber Security Centre recommends 10 steps. Visit ncsc.gov.uk.

NFU **Mutual**

ART-CYCV-0420