Making working from home work for you

This document is for investment professionals only and should not be relied upon by private investors.

Keeping your business safe from cyber attack

The coronavirus pandemic has resulted in many employees working from home. The scale of this change and the fact that this new way of working is likely to continue for some time presents many challenges. One such issue is the heightened threat of cyber crime.

Employees may be communicating in new ways, such as through video conferencing, or need to share files remotely. They may also be using personal devices and portable media where the security may not be as robust as their corporate environment. It is therefore important that firms consider how they protect themselves and clients from the risks posed by cyber criminals. You may therefore find the following guidelines useful – they are largely based on advice from the National Cyber Security Centre (NCSC) and can help reinforce the protection your business already has in place.

FundsNetwork

Fidelity™ INTERNATIONAL

Keeping your business safe from cyber attack

Controlling access to corporate systems and data

To enable staff working from home to securely send and receive emails, exchange files and access your firm's IT systems, firms should ensure that a Virtual Private Network (VPN) is in place. A VPN creates an encrypted connection across the internet, and encrypts data exchanged between the remote user and your systems. If you have already established a VPN, make sure it is fully patched and receives regular updates. You may also need to arrange additional licenses and capacity if your firm normally only has a limited number of staff working from home.

In addition, it is highly recommended that all corporate data is stored on the corporate network rather than the employee's mobile device. The ability to copy data out, or print files, should also be carefully controlled.

Advice on choosing, deploying and configuring a VPN can be found on the NCSC's website.

Staff using their own devices

The rapid move to extensive home working may have meant that some staff have had to use their own desktop PCs, tablets, laptops and smartphones to access work systems and data. While this may have been unavoidable, this does present a number of risks. There is an increased likelihood of data loss – work data may be automatically backed up to the individual's private data storage facilities, for example, and other household members may have unrestricted access to confidential information. Staff may also be using out-of-date devices that are particularly vulnerable to cyber attack.

Where employees have been permitted to use their own devices for work purposes, it is important to issue guidance and policies on how they may be used. This may include restricting their use to certain tasks and requiring your firm to have some control over an employee's device. More advice on implementing policies and procedures in this area can be found on the NCSC's website.

Email hacking and the risk this poses to advice firms

While your firm may have introduced robust security measures for your systems and electronic communications, it is very important to be aware that clients may have been targeted by fraudsters. Email is a favoured channel for thieves and email hacking – the taking over of someone's account without their knowledge – is becoming much more prevalent. It is now a common feature of financial fraud and significant sums have been lost to criminals in this way.

In many cases of email-related fraud, advice firms have been held responsible because, among other factors, all communications between the firm and the client were through unsecured email. Commonly, no attempt was made to double check the client's instructions through another established form of communication.

Our factsheet highlights examples of this type of fraud.

Working from home securely – tips and best practice

- ☑ Ensure you work from a secure location, such as your main residence, using a trusted device and wi-fi connection.
- ☑ Always protect your firm's data – be aware of data leakage; work from a separate room isolated from family, friends, flatmates, etc.
- ☑ Keep your devices patched and up to date.
- ☑ Ensure your screen is only visible to yourself and no one else. Avoid sitting with your back to the window where someone can see your screen.
- ☑ Always lock your screen with a password protected screen saver when you leave your computer to ensure data remains protected.
- ☑ Make sure you cannot be overheard when conducting business voice or conference calls.
- ☑ Avoid taking printed corporate documents home. If you do, ensure you keep them secure and never leave the documentation unattended or visible to others. After use ensure the documentation is securely disposed of using a shredder.
- ☑ If your device is lost or stolen report it to the appropriate person within your firm as soon as possible.

Preparing and setting up remote access

It may be that some staff will be working from home for the first time. If this is the case, it is likely you will need to set up new accounts or access permissions for these team members. All user accounts should have robust passwords and the NCSC strongly recommends that you implement two-factor authentication (2FA) if possible. This requires staff to 'prove' their identity in two different ways before they access your firm's systems. This is generally a password plus one other method, such as a unique code that is sent to their smartphone that must be entered in addition to the password.

It could also be possible that employees may need to use different software (or use applications in a different way) while working at home. Initially, a certain amount of familiarisation may be required and you may wish to consider issuing explanatory notes or guides to help team members.

Malware prevention

Any electronic exchange of information, including email, web browsing and removable media, carries with it the risk that malware (malicious software) might be introduced into your systems. Working from home exacerbates this threat. To help reduce this risk, you should consider developing and implementing anti-malware policies and standards. These should include scanning all data for malicious content at the network perimeter, installing firewalls, deploying antivirus and malicious code checking solutions and blocking access to known malicious websites. You should also encourage team members to keep their devices updated with the latest security patches.

Managing user privileges

A privilege is the right of a user to perform a particular system-related operation. Staff working from home may well require access to your systems but these privileges and rights should be at a reasonable – but minimal – level to enable them to perform their role. Granting employees unnecessary system privileges or superfluous data access rights can increase the risk of security/data breaches.

Keeping devices and data safe

Devices used for home working are more vulnerable to theft and loss. Staff should therefore understand the risks of leaving them unattended, especially if taken outside of the home. When not in use, employees should keep their equipment somewhere safe. The NCSC strongly recommends that data is encrypted – most modern devices have encryption built in, but this may need to be switched on and configured. Tools are available that can be used to remotely lock access to an employee's device, erase the data stored on it, or retrieve a backup of this data.

It is particularly important to make sure employees know what to do if a device is lost or stolen. They should be aware of who to report the incident to and appreciate that this should be done as soon as possible. The early reporting of such losses may help minimise the risk to confidential data.

Removeable media controls

Removable media, such as memory sticks, discs and USB flash drives, provide a common route for the loss of sensitive data and the introduction of malware. You may therefore wish to encourage staff working from home to transfer files using alternative means (such as using a corporate storage solution).

Where removeable media is used, your firm should apply appropriate security controls, such as automatically scanning for malware. Other recommended procedures include restricting their use to only necessary functions, encrypting the data held on them and actively managing their reuse and disposal.

Coronavirus phishing scams

Cyber criminals are using the coronavirus pandemic to their advantage – there has been a surge in phishing scams using the outbreak as a hook. They are using phishing emails to steal personal information, gain access to corporate systems and download malicious software. It is therefore recommended that you advise your staff to be vigilant when viewing emails, text messages and electronic communications. Links and attachments within emails should be treated with the utmost caution, especially on mobile devices. Employees should be particularly wary of requests for personal or client information.

For more insights on how to make a success of working from home, visit fundsnetwork.co.uk/homeworkingkit

FundsNetwork

Fidelity INTERNATIONAL

UKM0820/30145/SSO/0821