GUIDANCE

Home working: preparing your organisation and staff

How to make sure your organisation is prepared for an increase in home working, and advice on spotting coronavirus (COVID-19) scam emails.

As part of managing the coronavirus (COVID-19) situation, many organisations will be encouraging more of their staff to work from home. This presents new cyber security challenges that must be managed.

In addition, cyber criminals are preying on fears of the coronavirus and sending 'phishing' emails that try and trick users into clicking on a link to a bad website (which could download malware onto their computer or steal passwords).

This guidance:

- recommends steps to take if your organisation is introducing (or scaling up the amount of) home working
- provides some tips on how individuals can spot the typical signs of phishing emails

Note: For official information about coronavirus, please refer to trusted resources such as the Public Health England or NHS websites.

Asking your staff to work from home

Whilst working from home will not be new to many organisations and employees, the coronavirus is forcing organisations to consider home working on a greater scale, and for a longer period of time. You may have more people working from home than usual, and some of these may not have done it before.

Setting up new accounts and accesses

If you need to set up new accounts or accesses so your staff can work from home, you should set strong passwords for user accounts. Please refer to the NCSC guidance for system owners responsible for determining password policy. The NCSC strongly recommend you implement two-factor authentication (2FA) if available.

Preparing for home working

Working from home can be daunting for people who haven't done it before, especially if it's a sudden decision. There are also practical considerations; staff who are used to sharing an office space will now be remote. Think about the new services that you may need to provide so they can continue to collaborate such as chat rooms, video teleconferencing (VTC) and document sharing. The NCSC guidance on implementing Software as a Service (SaaS) applications can help you

choose and roll out a range of popular services. If you are already providing such services, you'll need to plan for a potentially large increase in users.

Here are some general recommendations to support secure home working.

- Remote users may need to use different software (or use familiar applications in a different way) compared to what they do when in the office. You should produce written guides for these features, and test that the software works as described.
- Depending on the experience of your staff (and the applications you provide), you should consider producing a series of 'How do I?' guides. For example, you might produce a 'How to log into and use an online collaboration tool'.
- Staff are more likely to have their devices stolen (or lose them) when they are away from the office or home. Make sure devices encrypt data whilst at rest, which will protect data on the device if it is lost or stolen. Most modern devices have encryption built in, but encryption may still need to be turned on and configured.
- Fortunately, the majority of devices include tools that can be used to remotely lock access to the device, erase the data stored on it, or retrieve a backup of this data. You can use mobile device management software to set up devices with a standard configuration.
- Make sure staff know how to report any problems. This is especially important for security issues (see looking after devices below).
- Your staff might feel more exposed to cyber threats when working outside the office environment, so now is a great time for them to work through the NCSC's Top Tips for Staff e-learning package.

Controlling access to corporate systems

Virtual Private Networks (VPNs) allow remote users to securely access your organisation's IT resources, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and your services.

If you are already using a VPN, make sure it is fully patched. Additional licenses, capacity or bandwidth may be required if your organisation normally has a limited number of remote users.
If you've not used one before, please refer to the NCSC's VPN Guidance, which covers everything from choosing a VPN to the advice you give to your staff.

Helping staff to look after devices

Devices used for working outside an office environment are more vulnerable to theft and loss. Whether using their own device or the organisations, ensure staff understand the risks of leaving them unattended, especially in public places. When the device is not being used, encourage staff to keep it somewhere safe.

Make sure that staff know what to do if their device is lost or stolen, such as who to report it to. Encourage users (in a positive, blame-free manner) to report any losses as soon as possible. The early reporting of such losses may help minimise the risk to the data, and staff who fear reprisals are less likely to report promptly.

Ensure staff understand the importance of keeping software (and the devices themselves) up to date, and that they know how to do this.

Removable media

USB drives can contain lots of sensitive information, are easily misplaced, and when inserted into your IT systems can introduce malware. When USB drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them. You can reduce the likelihood of infection by:

- disabling removable media using MDM settings
- using antivirus tools where appropriate
- only allowing products supplied by the organisation to be used
- protecting data at rest (encrypt) on removable media

You can also ask staff to transfer files using alternative means (such as by using corporate storage or collaboration tools), rather than via USB. For more information, refer to the NCSC's Removable media guidance.

Using personal rather than work devices

If you are permitting people to use their own devices to work remotely, please refer to the NCSC's Bring Your Own Device (BYOD) guidance.

Spotting email scams linked to the coronavirus

Cyber criminals are preying on fears of the coronavirus and sending 'phishing' emails that try and trick users into clicking on a bad link. Once clicked, the user is sent to a dodgy website which could download malware onto your computer, or steal passwords. The scams may claim to have a 'cure' for the virus, offer a financial reward, or be encouraging you to donate.

Like many phishing scams, these emails are preying on real-world concerns to try and trick people into doing the wrong thing. Please refer to our guidance on dealing with suspicious emails to learn more about spotting and dealing with phishing emails.

For genuine information about the virus, please use trusted resources such as the Public Health England or NHS websites.

What to do if you have already clicked?

The most important thing to do is not to panic. There are number of practical steps you can take:

- Open your antivirus (AV) software if installed, and run a full scan. Follow any instructions given.
- If you've been tricked into providing your password, you should change your passwords on all your other accounts.
- If you're using a work device, contact your IT department and let them know.
- If you have lost money, you need to report it as a crime to Action Fraud. You can do this by visiting www.actionfraud.police.uk.

PUBLISHED
17 March 2020

REVIEWED

17 March 2020

VERSION

1.0

WRITTEN FOR ⓘ

Small & medium sized organisations

Large organisations

Public sector

Cyber security professionals