



# LOCKDOWN REMOTE WORKING GUIDANCE

**HOME WORKING** As we once again move into lockdown and remote working becoming more prevalent across the business sector we wanted to reiterate the following guidance to ensure a safer cyber secure working environment.

We recommend you read the NCSC guidance to prepare your staff for remote working which is available on the following link. <https://www.ncsc.gov.uk/guidance/home-working>

This covers the essential recommendations for business to protect their information. A useful infographic is available here <https://www.ncsc.gov.uk/files/home%20working%20v1.pdf>

**Home working: Managing the cyber risks**

**1. Setting up user accounts & accesses**  
Set strong passwords for user accounts, use NCSC guidance on passwords and review your password policy. Implement two-factor authentication (2FA) where available.

**2. Preparing for home working**  
Think about whether you need new services, or just extend existing services so teams can still collaborate. NCSC guidance on security can help you choose and roll out a range of popular services. In addition:  
• Consider whether you need new services, or just extend existing services so teams can still collaborate.  
• Check devices are ready to be joined (or used) when home working. Ensure devices encrypt data whilst at rest. Most modern devices have encryption built in, but may need to be turned on and configured.  
• Use mobile device management (MDM) software to set up devices with a standard configuration in case the device needs to be remotely locked, or have data erased from it.  
• Make sure staff know how to report any problems, or raise support calls. This is especially important for security issues.  
• Don't testing more expensive to update research when home working should work through the NCSC's Top 100 Best Remote Working Practices.

**3. Controlling access to corporate systems**  
Virtual Private Networks (VPNs) allow home workers to securely access your organisation's IT resources (such as email). If you've not used one before, refer to the NCSC's VPN guidance, which covers everything from choosing a VPN to the advice you give to staff.  
If you already use a VPN, make sure it's fully patched. You may need extra licenses, capacity or bandwidth if you're supporting more home workers.

**4. Helping staff to look after devices**  
Whether using their own (or the organisation's), ensure staff understand the risks of using them outside the office. When not in use, staff should keep devices in a secure place.  
Make sure they know what to do (and who to call) if devices are lost or stolen. Encourage users to report any losses as soon as they can.  
Ensure staff understand how to keep software and devices up-to-date, and that they apply updates promptly.

**5. Using removable media safely**  
USB drives may contain sensitive data, are easily lost, and can introduce malware into your systems. To reduce the likelihood of infection you can:  
• install removable media using local settings  
• use antivirus tools where appropriate  
• only permit the use of sanctioned products  
• protect data at rest (encrypt on removable media)  
• encourage alternative means of file transfer (such as online tools).

**USING PERSONAL DEVICES FOR WORK** If staff are using their own devices to connect to your network please ensure you are conversant with the NCSC guidance at the following <https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device>

**Phishing attacks: Dealing with suspicious emails**

**Make yourself a harder target**  
Information from your website or social media accounts has been a valuable asset for criminals. You can make yourself less likely to be phished by doing the following:  
• Criminals use public profiles to make their phishing emails appear convincing. Review your social profiles, and clean up what you post.  
• Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you.  
• If you have received an email which appears to be from a trusted contact, check the sender's email address. The NCSC's Suspicious Email Reporting Service (SERS) reports suspicious emails to the police.  
**What to do if you've already clicked?**  
The most important thing to do is not to panic. There are a number of practical things you can do:  
• Open your antivirus (AV) software, and run a scan now. Remove any malware that has been detected.  
• If you've been tricked into providing your personal or financial information, you should report it to your other accounts.  
• If you have lost money, you need to report it as soon as possible to your bank. This can be done by calling your bank's fraud department.

**Tell tale signs of phishing**  
Spotting phishing emails is becoming increasingly difficult, and even the most careful user can be tricked. Here are some tell tale signs that could indicate a phishing attempt:  
• Is the email addressed to you by name, or does it refer to you as "customer" or "member"?  
• Do you know the sender's name, and is it a name you would expect to receive an email from?  
• Do you know the sender's email address, and is it a name you would expect to receive an email from?  
• Do you know the sender's phone number, and is it a number you would expect to receive a call from?  
• Do you know the sender's social media profile, and is it a profile you would expect to see from them?  
• Do you know the sender's physical address, and is it an address you would expect to see from them?  
• Do you know the sender's IP address, and is it an IP address you would expect to see from them?

**PHISHING EMAILS** During the previous lockdown there was an increase in online cyber related crime. We recommend your staff are aware of the signs of Phishing emails and have the knowledge to recognise and report such emails. Guidance is available at <https://www.ncsc.gov.uk/guidance/suspicious-email-actions>

**STAFF TRAINING** It is important that staff understand their roles and responsibilities in regards to Cybercrime prevention and it may be prudent to reaffirm staff training and update security protocols during this period. You can access free staff training and ensure updates are enacted promptly on all devices. The wellbeing of staff is also important at this time and it is incumbent on managers to support staff during the period and ensure any Cyber related concerns are addressed timeously with privileged access levels to confidential information being reviewed as required. Free online staff training is available from the NCSC at the following link;

[https://www.ncsc.gov.uk/training/StaySafeOnline\\_web/index.html#/menu/5f215cc1006d2436a3b6c5e2](https://www.ncsc.gov.uk/training/StaySafeOnline_web/index.html#/menu/5f215cc1006d2436a3b6c5e2)

**Business email compromise**  
Dealing with targeted phishing emails

This alert helps you to spot the more obvious signs of targeted phishing emails. These alerts, also known as business email compromise, are typically sent to executives or budget holders with larger opportunities to trick staff into transferring funds, or revealing sensitive information.

**What is business email compromise?**  
Business email compromise (or BEC) is a form of phishing attack where a criminal attempts to trick a senior executive (or budget holder) into transferring funds, or revealing sensitive information. The criminals behind BEC send convincing looking emails that might request financial payments, or contain links to 'fake' websites. Some criminals may create websites designed as harmless attachments, which are activated when opened. Unlike standard phishing emails that are sent out indiscriminately to millions of people, BEC is specifically targeted at senior members of all sizes and across all sectors, including from small organisations and government.

**Make yourself a harder target**  
Information about you that's easily viewed on your work and private websites (including social media accounts) can be used by criminals to make their phishing emails appear more convincing. Review your privacy settings, and think about what you post across your social and professional accounts. Be aware what your friends, family and colleagues say about you online, as this can also reveal information that can be used to target you. If you spot a suspicious email, flag it as spam/junk in your email inbox. Tell your IT department that you've identified it as potentially unsafe.

**Tell tale signs of phishing**  
Spotting a phishing email is becoming increasingly difficult and will trick even the most careful user. Having the confidence to ask 'is this genuine?' can be the difference between staying safe, or a costly mistake. Think about your usual working practices around financial transactions. If you get an email from an organisation you don't do business with, treat it with suspicion. Look out for emails that appear to come from a high-ranking person within your organisation, requesting a payment to a particular account. Look at the sender's name and email address. Does it sound legitimate, or is it trying to mimic someone you know? Ensure that all important email requests are verified using another method (such as an account, a phone call, logging in or in-person). Does the email contain a veiled threat that asks you to act urgently? The suspicious of words like 'urgent' or 'you have been a victim of crime, click here immediately'. Some emails will try and create official-looking emails by including logos and graphics. Is the design (and quality) what you'd expect?

**What to do if you've already clicked?**  
The most important thing is to not panic. Your IT department will have steps in place to help staff who think they've been phished. If you think you've been a victim of a phishing attack, tell your IT department as soon as you can. The sooner you tell them, the more likely they'll be able to help.

© Crown Copyright 2020

**BUSINESS EMAIL COMPROMISE (BEC)** is a form of phishing attack, typically a cybercriminal will send a fake invoice or request for payment information to be updated. Another tactic is sending an email posing as a manager or CEO within a company. Always be sceptical of urgent and hurried requests to transfer/pay invoices. Verify these requests using known contacts. The

National Cyber Security Centre have produced an infographic that outlines this security threat and actions to take to avoid BEC: <https://www.ncsc.gov.uk/files/Business-email-compromise-infographic.pdf>

**VIDEO CONFRENCING** As businesses move to a more Cyber resilient footing video conferencing will become more prevalent in everyday work. Guidance on Video Conferencing is available at <https://www.ncsc.gov.uk/guidance/video-conferencing-services-security-guidance-organisations>

**Video conferencing**  
Using services securely

The COVID-19 lockdown means many of us are now using video calls to stay in touch with family, friends and work colleagues. If you're new to video conferencing, the top holder will help you to get started. Even if you're familiar with video conferencing, you should take a moment to review how you're using it.

**1. Downloading video conferencing software**

- If using standalone video conferencing software, only download it from trusted sources (such as Apple's App Store or Google Play), or from the service provider's official website.
- Use tech websites and other trusted sources to research what app is right for you. The 'free' version of a video conferencing service will provide good enough security for personal use, provided you've set it up correctly.
- Check the privacy settings. You should make sure that you understand what (if any) data the service will access during operation. You may have the option to opt out of sharing data.

**2. Setting up video conferencing services**

- Make sure that the password for your video conferencing account (or for the device or app you are using for video conferencing) is different to all your other passwords, and difficult for someone to guess. If available, set up two-factor authentication (2FA) for the account (and for your device and other apps, if available).
- Test the service before making (or joining) your first call. Check that your microphone and camera work and that your internet connection is fast enough. Learn how to mute your microphone and how to turn off the camera.
- Many services allow you to record the meeting, share files, or show what is on somebody's screen. Find out how to tell if the call is being recorded.

**3. Hosting and joining calls**

- Do not make calls public. Connect directly to the people you want to call using your contacts/address book, or provide private links to the individual contacts. If possible set up the call so that a password is required to join.
- Consider using the lobby feature to ensure you know who has arrived. Make sure people are who they say they are before they join the call, the password function described above can help with this.
- Think about what your camera shows when you're on a call. Would you expect to share that information with strangers? Consider blurring or changing your background, you'll find instructions on how to do this on the support website for your video conferencing service.

**4. Keep all devices and applications up to date**

- Make sure that all your devices and applications (not just the video conferencing software) are kept up to date. Applying software updates is one of the most important things you can do to protect yourself online.
- Update all the apps (and your device's operating system) whenever you're prompted. It will add new features and immediately improve your security.

© Crown Copyright 2020

If you have been a victim of crime, and it is not an ongoing emergency, you can report this to Police Scotland on 101. For all emergency calls, dial 999.

This alert was sent out for your information by Police Scotland  
Cybercrime Harm Prevention Unit - [PPCW@CyberHarmPrevention@Scotland.pnn.police.uk](mailto:PPCW@CyberHarmPrevention@Scotland.pnn.police.uk)  
All information was correct at time of distribution. 07/01/2021.