12 tips to help any remote worker

Like many of us in the UK, you may now find yourself working from home for an unknown period. Whether you're a remote working veteran or you've only ever been office-based, today's circumstances are new to us all. To help you navigate the world of remote working and with the support of your IT team, we've compiled our top 12 tips for keeping safe and secure when working from home.

They'll make your life easier and help you do your job with peace of mind. Check them out below and get in touch with IT if you're unsure what your company has in place.

1 Check out home working policies

If it didn't already, the company you work for will almost certainly have a home working policy in place now. Contact HR or IT for guidelines or to set up a brief video training session. Look out for points such as WiFi use, security, incident reporting and permissions.

2 Secure your home WiFi router

Settling into home working means depending on domestic WiFi. To ensure your home router doesn't compromise the business network you need to: change your router password, ensure firmware updates are installed, and encryption is set to WPA2 or WPA3. Ask the IT team to help you check these tasks off.

3 Use a VPN to access networks

A VPN (virtual private network) blocks criminals from seeing internet traffic and therefore helps protect sensitive data, apps and communications from being stolen, hacked or compromised. A VPN must be intentionally installed, so drop IT a message about setting one up on any and all work devices.

4 Install enterprise security software

If you're using a company device at home, seek clarification that essential cybersecurity such as antivirus, firewalls and email filtering is installed. If using a personal device, don't take built-in security software for granted – ask IT to remotely install enterprise-grade solutions fit for business activity .

5 Check your password hygiene

Working from home makes it more important than ever to ensure that accounts are protected with strong passwords. Create unique passwords for each account that comprise a long string of upper and lower case letters, numbers and special characters. Also check where and how passwords are secured, encrypting files if possible.

6 Review data storage practices

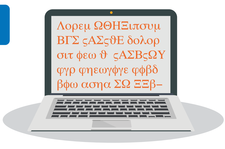
Storing files directly to devices should be kept to a bare minimum, and only done so if it's essential to business. Work and store documents on the corporate network via a VPN, and encrypt data stored on devices. Schedule a screen sharing session with IT, who will demonstrate the best storage practice for your company.

7 Backup to a private cloud

Data can be lost to cyberattack, network outages, hardware damage or even human error. When working from home, it's most convenient and reliable (for yourself and the IT team) to backup to the cloud. Avoid using personal accounts – contact IT who will configure your device to automatically backup in regular cycles to an approved, central cloud location.

8 Use encrypted comms if necessary

Remain diligent about GDPR and data protection when working at home, especially because remote devices are considered easier targets for hackers. If you need to communicate sensitive information with colleagues or customers, your company can provide you with software or apps that encrypt communications end-to-end.



9 Be wary of COVID-19 scams

Since the end of February 2020, phishing emails related to COVID-19 have increased by a shocking 667%. Scam texts (smishing) capitalising on the uncertainty are also on the rise. To ensure you'll be able to intercept and prevent an attack, ask for a remote training session.

10 Update systems, software and patches

Updates always seem to come at the most inconvenient times, don't they? However, operating system, app and patch updates are critically important and help to protect your device and the network it's connected to from cyberthreats such as viruses. Set updates to run automatically out of working hours to avoid downtime.

11 Refrain from shadow IT

Shadow IT is the result of colleagues undertaking tasks that change a company's IT estate, such as altering settings or installing software. You might long for your favourite app on your office PC or have seen a programme that could transform your day. But, resist the urge to go DIY and drop IT a message instead. They're really busy right now, so be patient.

12 Don't mix work and personal devices

Under usual circumstances, you wouldn't use your work mobile to WhatsApp friends, or your personal laptop to Skype a client. So, avoid falling into the trap of mixing devices – it's bad for security, data protection and your own well-being. Oh, and always lock your devices when you're finished working.

Follow these practical tips and you'll soon be working safely, securely and with a lot less weight on your shoulders. And remember, if you're feeling overwhelmed about the change, be thankful that you didn't turn yourself into a potato (yes, a potato) on Teams and go viral like this unfortunate lady! Check it out if you need a laugh – you're welcome.

k3 cloud, hosted and managed services

t: 0844 579 0800 w: www.k3msp.com e: enquries@k3btg.com