Coronavirus
Staying safe online

COVID-19

#keepbusinessworking

We are all adjusting to the current situation and it is important to make sure that security is still central to the way we are all working, especially if we are not used to working remotely. Here are six questions to ask yourself if you are working from home.

1 Is it a scam?

Beware of scammers and fraudsters claiming to offer working from home kits, treat offers of Government aid or bank-related support with extreme caution. These scams can come from emails that appear to be from legitimate sources, i.e. phishing attacks, or via website adverts, again the website could be legitimate but the advert could be a scam.

2 Is your home WI-FI secure?

Ensure your device does not share data with other devices connected. Consider using a Virtual Private Network (VPN) to provide anonymity by hiding the user and making it hard for anyone to track your information as it goes through the internet.
By default, where possible use multi-factor authentication, where users need a password and a PIN code (usually sent to the phone) in order to access the work network.

Ensure that your home Wi-Fi has not been compromised or is being used by someone outside the household. Check the devices on the network are known to you. If there are unknown devices connected, change your WIFI password immediately. Make sure you are connecting to your home Wi-Fi and not someone else's.

3 Are you using Antivirus?

Devices such as tablets or home laptops may not have secure and up to date antivirus software, so could be open to cyber attacks, thus compromising company data if they are used to work from home. Check that these devices have up to date antivirus software, no matter what operating system they use.

4 Are your documents secure?

Try not to download and work on documents on home devices other than those linked to your work.

If you are not careful this could result in sensitive documents being shared accidentally to family members or outside your household. Monitor where documents are downloaded to and ensure their deletion on additional devices.

5 Are your devices up to date?

Ensure that all updates are applied and refrain from using out-of-support software – patching can repair potential flaws in the software which may be exploited by attackers.

6 Are you revealing sensitive information?

Ensure that other household members don't have access to sensitive information about your customers, staff, or your business. If you have to share a device, consider setting up a separate profile or user account for work purposes.

Want to know more?

The National Cyber Security Centre has top tips for staying safe and or check out the Government guidelines on cyber security

Together we'll keep business working.

With kind thanks to Ian Webb, Ian Webb Consultancy
and Arthur Mainja, KPMG

Please contact us at info@jerseybusiness.je for help and support.

Jersey Business
EXPERTISE. SHARED.