BUSINESS IN THE COMMUNITY

The Responsible Business Network
Northern Ireland

Helping your employees stay well

WORKING FROM HOME: STAYING SAFE ONLINE

An unprecedented number of employees are working from home to reduce the transmission rate and the impact of COVID-19. Cyber criminals are opportunistic and quick to exploit people's anxieties and vulnerabilities in their cyber security to try and steal valuable company data such as customer details. Here are 5 top tips to keep you and your company safer online when working from home.

We strongly recommend all employees complete the National Cyber Security Centre's (NCSC) free cyber security e-learning. If you are a small business owner or IT Manager see the NCSC's new Home Working Guidance. and Small Business Guide for more information.

Use passwords to protect your data

Make sure you switch on password protection on all devices you use for work purposes at home: PC, laptop, tablet and mobile phone. Avoid using default or predictable passwords, we suggest using three random words like 'wombatcheesebog'.

Consider using a Password Manager to reduce password overload.

Look out for phishing attacks

Check for obvious signs of phishing: spelling errors or poor grammar, email addresses that don't match the sender, generic greetings, urgent requests, and offers that seem to be too good to be true or are related to a new 'high risk' event such as covid-19. See examples of COVID-19 scams

Let your company know if you receive or click on any malicious links so they can report it to Action Fraud and in the case of a data breach the Information Commissioner's Office.

Using your own devices

Keep your devices and apps up to date this is known as 'patching' – where possible enable auto updates.

Do not use personal email accounts to send or receive company information.

Ensure lost or stolen devices (iOS and Android) can be tracked, remotely locked or wiped and if your device is lost or stolen report it immediately to your company.

Review your home set up

Change the default password of your routerv and ensure your home network is encrypted with at least WPA2. Check your settings on your iOS and Android device to make sure your firewall is switched on and check your devices are as secure as possible.

Install and switch on antivirus software – check your broadband package as antivirus software is often included for free, you just need to turn it on by checking a box.

Data back up and storage

Do not just save items locally on your device, make sure you regularly back up files using a cloud storage provider.

Close down applications and all your open webpages at the end of each day and switch off your device. This will limit hacker opportunity to access your data.

Store unwanted documents securely until you can take them back to the office for secure shredding.