Corona Virus & Homeworking IT implications

Many organisations will be encouraging more of their staff to work from home as result of the Corona Virus.

As a result of the need to keep the business afloat, this presents additional cyber security challenges that may, especially for smaller companies, be overlooked. Essentially, when your staff access IT systems and your data and/or databases remotely, then risk increases. Proper processes and procedures need to be put in place.

In addition, cyber criminals are already sending 'phishing' emails that try and trick users into clicking on a link to scam websites in an attempt to download malware onto your computer, corrupt your systems or steal your passwords.

Helping staff to look after devices

Here are some general recommendations to support secure home working.

- Prepare home workers with some basic security advice and suggest that IT support check the home workers router to ensure passwords are strong and have been changed from the default.
- Ensure that any home workers device (PC / Laptop / tablet) is secure. So has the device got an up to date virus / threat protection package, and a properly configured Firewall. Also ensure that the device is updated with the latest versions of security and application updates.
- If the homeworker requires access to the company's internal network (rather than a cloud application), ensure they are set-up with a secure VPN and remote desktop connection using strong passwords.
- IT support should ensure that the home worker does not store or save company information on the local device wherever possible.
- Users new to home working may need to use different software (or use familiar software in a different way). These new access routes should be tested and documented guides or "How To's" produced where relevant, for instance 'How to log into and use XX/YY".
- Advise staff not to open emails from unknown sources, don't download apps / software unless advised / approved by IT Support.
- Make use of the latest encryption. Staff are more likely to have their devices stolen (or lose them) when they are out of the office. Most modern devices have encryption built in, but it may still need to be configured and implemented.
- These days mobile device management software includes 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. Ensure these features are set up and applied.
- Manufacturers and software providers are often sending out updates, so ensure staff understand the importance of keeping software (and the devices themselves) up to date, and that they know how to do this. Again, written "How To's" might be useful
- Avoid the use of USB sticks. It may be easy but the risk increase
- More basically, ensure staff know how to report any problems and who to report problems to. 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.

Finally, we are social animals

Tech is going to play a huge part of us minimising the impact of the virus, but we are social animals and many go to work to be with and to help others and many are being driven to work at home and may not want to. The grim truth is that some of your people are going to get lonely, others will get sick.

The more you can accommodate the social aspects of work the better morale is likely to remain. Microsoft Teams, Google Hangouts, Facetime, Zoom and other collaborative apps are likely to become increasingly important to preserving mental health, particularly for anyone enduring quarantine. Encourage your people to talk with each other, even if it is just over the phone.

We have heard of one group of people working remotely who are using a home exercise app to exercise together at the start of the day!

People are the only source of creativity and innovation, they are likely to be under a great deal of personal stress, look after them.

For further information and help with IT Security generally or with the Cyber Essentials programme or the internationally recognised ISO 27001 the Information Security standard please contact mwoods@statius.co.uk or call him on 07976 426 286.