

BUILDING A SECURE REMOTE WORKING ORGANISATION

With one third of IT decision-makers admitting that their organisations had suffered a data breach as a result of remote working¹, how do you ensure that your company data stays protected during this time of business as unusual?

01.

Secure your remote working policy

A home office network is **3.5x more likely** to be infected by malware than a corporate network²

Cyber criminals **know** if you're a home user or a business user working at home

02.

Be extra wary of phishing attacks

Covid-19 related phishing emails now represent the largest theme of **attacks**³

Scams increased over **400%** in the UK alone across February and March⁴, with victims collectively losing over £1.6million⁵

Make sure your employees know to **check who sent an email before opening it**. They should also think twice before clicking on unknown links

03.

Don't forget about home device security

Your team will be using whatever printer or scanner they have available at home

These devices probably **don't have the standard security** features provided by your corporate network equipment

With more than **25%** of all devices having one or more services exposed on the internet⁶, they are more vulnerable to attack

To safeguard your business critical data, give your employees support in ensuring that their network is private and can only be accessed with a **secure**, non-default password

04.

And confidential paperwork

Ensure your remote workers are treating company paperwork with the same care as their own bank statements, making sure they **shred or safely store** anything confidential until they're able to return to the office

05.

The best policy is to have one

Working from home **doesn't mean** company policies can be relaxed

Remind your team to only use applications, networks and cloud locations **provided by the business**

Any free cloud collaboration and storage tools they might be tempted to use **may not be secure** if they've not been vetted by you

If any of your team is working remotely, you need to make sure that they have a clear understanding of how to maintain the same standard of business security awareness, whether they're in the four walls of the office or sat on their sofa.

Click here to learn how you can not only survive, but thrive in these times of business as unusual.

Canon

See the bigger picture

¹ <https://www.raconteur.net/technology/covid-19-cybersecurity>

² <https://threatpost.com/malware-risks-triple-for-remote-workers/154735/>

³ <https://www.cbi.org.uk/articles/phishing-coronavirus-and-working-from-home/>

⁴ <https://www.actionfraud.police.uk/alert/coronavirus-related-fraud-reports-increase-by-400-in-march>

⁵ <https://www.thebusinessdesk.com/westmidlands/news/2040001-the-perils-of-remote-working-the-next-normal-in-data-protection>

⁶ <https://www.bitsight.com/blog/identifying-unique-risks-of-work-from-home-remote-office-networks>