

COVID-19: Keep your team operating securely while working remotely

Welcome to the latest ER blog - keeping you up to date on cybersecurity.

COVID-19 is having a major impact on everyone's life, including changing the way we work resulting in the huge number of us now doing so from home.

Cybercriminals are taking advantage of reduced IT team sizes due to self isolation and lockdown who are having to manage a remote workforce which leads to significant pressure on the IT infrastructure.

The online trade publication and social community for IT professionals, Techrepublic, yesterday reported that the COVID-19 lockdowns are causing a huge spike in data breaches - much worse than anticipated - according to the International Association of IT Asset Managers who said "Too many organisations have left themselves wide open for attack".

In the report, they cite four areas causing breach risks:

- Assets are being purposely left with reduced security - eg removing admin permissions so that employees can complete the task without administrator oversight and working remotely may mean computers are not being kept up to date with the latest security patches.
- The rapid addition of new hardware leaves reduced time for security. The need to quickly purchase and deploy laptops has removed focus on cybersecurity and user training.
- Computers on home networks may be less secure. Connection should be via a properly configured VPN rather than just over the internet.
- Due to the rush to equip people to work from home securely after lockdown, unprepared/untrained users are more prone to making mistakes and falling victim to phishing attempts such as appeals for money, disinformation campaigns or new information about COVID-19. This gives cybercriminals the opportunity to gain login credentials and install malicious software.

This increased risk of breach is dangerous for businesses who leave themselves wide open to loss of data, reputation, income and potentially huge fines.

There are things business leaders can do to help them protect themselves and reduce the risks significantly:

- Turn your employees from being a potential vulnerability to a cybersecurity asset: provide online training to help them understand their responsibilities under GDPR, how they can spot and avoid the risks and turn them into a human firewall.
- Set up a VPN or other secure means to ensure employee access to the company network is done safely.
- Ensure advanced cybersecurity solutions are in place to help protect and secure each computer.

Data security is a joint effort between IT teams and users. User training and good computer security is the only way to ensure businesses get through COVID-19 intact and stop them from becoming yet another security statistic.

Contact us today to find out how EnterpriseRed can help your company stay safe and secure during the COVID-19 pandemic - for no cost, no contract and no commitment, for up to 6 months. [Click here for more information.](#)

Tel: 0203 371 9178

Email: support@enterprised.com