Working from home? Keep your assets secure, scam-free and insured

If you're allowing your staff to work from home as a preventative measure against the coronavirus pandemic, make sure you're prepared for the increased cybersecurity risks associated with the move.

Wynand van Vuuren, head of customer experience at King Price

This includes taking steps to not only ensure the physical security of company devices that may contain sensitive data but also to secure all access to company networks, says Wynand van Vuuren, head of customer experience at King Price.

“Remote working right now makes a lot of sense, but there are risks attached to this. When accessing corporate networks remotely, there’s a far higher risk of unauthorised access and data leakage. People might engage in behaviour they wouldn’t do at the office, like sharing a device with other family members, using the same device for both personal and work activities, or even connecting to public Wifi spots,” said Van Vuuren.

According to the South African Banking Risk Information Centre (SABRIC), there’s been a sharp rise in cases of cybercriminals are exploiting the spread of Covid-19 by using coronavirus-based scams to trick people into clicking on links in emails or SMSs appearing to offer medical supplies and vaccines.

These emails appear to come from reputable companies – but once people click on links or provide personal information, the cybercriminals can either access their computer systems or bank accounts.

What are the risks?

- If unauthorised people access your system and steal client information, the company may be held legally liable.
- You could become the victim of a ransomware attack, where your systems are blocked by cyber criminals until you pay a ransom.
- Employees working on their own systems can infect the company's systems with viruses – or even worse, other companies' systems, if a virus were emailed to a client, for example.

So what can you do?

There are a number of proactive security measures that you can put in place, says Van Vuuren.

- Implement the best security you can afford: firewalls, security software, malware scanning.
- Train your employees on the basics of security, to avoid issues like phishing.
- Insist that your employees use VPNs on all work-related devices and avoid connecting to public Wifi spots.
- Never click on any links in emails or SMSs, even if they look legitimate. Check with your IT team or your bank if you're not sure.
- Check that you're on a genuine website before entering any personal information.
- Regard all 'urgent' security alerts, offers or deals as warning signs of a hacking attempt.

Add a cyber insurance policy

Make no mistake, cyber insurance can't save your business from attacks – but it's an important way to protect you from the after-effects of a breach by covering expenses for:

- Data breach, including hiring legal and forensic IT professionals to help you recover your data.
- Damage to computer systems and data.
- Disruption following a cyberattack that brings your business to a halt and results in loss of income.
- Insured incidents, like specialist support to check if a cyber threat is real.
- Financial loss and proving fraud, including financial losses resulting from fraudulent inputs into insured computer systems which have led to dishonest transactions.

"The best insurance policy is always one you never have to use. But by combining a proactive, holistic security approach with a strong cyber insurance policy, you should be well on the way to keeping your business healthy while your people are working off-site," says Van Vuuren.