Publication: Die Courier
Title: Keep cyber-criminals at bay
AVE: 7134
Page: 6
Publish Date: 06 August 2021
Author: Unspecified

Keep cyber-criminals at bay

In the past 18 months, we've all become used to working from home.

Some of us have even become pros at pretending that we're not really still wearing our PJs in Zoom meetings. But, for most of us, our online security skills are lacking – and this could expose us and our employers to a range of risks.

That's the warning from King Price Insurance's head of client experience, Wynand van Vuuren, who says the world of WFH has seen a boom in attempted cyber-hacks using remote employees as the entry points into corporate networks.

"The problem is that at home, we often do things that we wouldn't do at the office. We share devices with other family members, or use the same device for both personal and work activities. Cyber-criminals know this, and they're increasingly trying to trick consumers into giving up control of their devices to steal their money or access sensitive company information," said Van Vuuren.

So how do we keep ourselves – and our employers safe?

Keep your corporate anti-virus on and up to date

Research shows many WFH employees aren't installing updates which previously would have happened automatically on the company network.

The best way to prevent malware from compromising your and your employer's safety is to make sure you're running the latest version of anti-virus and your operating system.

"If your employer's IT team asks you to install updates, do it. For your good and theirs," says Van Vuuren.

Pay attention to your wi-fi security

A good way to improve your home office security by protecting your network. There are two main ways to do this: first change your wi-fi password to something other than '12345', or your surname.

According to cybersecurity company Mimecast, even devices like smart TVs and home automation systems that are connected to your home network offer a potential entry point for cybercriminals.

Then change your router's default password, which is usually something like 'Admin111'. Hackers can easily access your devices through the router. Make it as hard as possible for them.

As curious as you are, don't click on it!

One of the most common types of cyberattacks is 'phishing', where emails or encrypted files appear to come from reputable companies – but once you click on a link or open an attachment, you could lose control of your system, and your company could become a victim of a ransomware attack.

A global study by Mimecast found that half of South African respondents admitted to opening emails they considered suspicious. Be careful.

Regard all 'urgent' security alerts, offers or deals as suspicious

If a stranger calls you, claiming to be from your bank, software company or even your IT department, and asks to install software on your PC to protect you – don't. Just don't.

"End the phone call immediately and contact your bank or IT department yourself. The moment they install remote access software on your machine, you're in a world of pain," says Van Vuuren.