# Remote workers, SMMEs, health sector more at risk of cyber threats

The Covid-19 pandemic and lockdown has created new vulnerabilities that fraudsters and cyber criminals have been quick to exploit, IITPSA experts have warned.

Photo by Josue Verdejo© from Pexels

Speaking at an IITPSA Western Cape chapter webinar on how to become cyber resilient and more aware during Covid-19, Terence Govender, director of IT Advisory at Mazars South Africa, said: “Our research has found that top targets for fraud and cybercrime at the moment include home users, SMMEs and the health sector.”

Govender said home users were particularly vulnerable because remote working users were seemingly more relaxed at home than they were at the office, following the notion that cyber attacks only happen at the office. In addition, they did not always have antivirus software, personal firewalls or Virtual Private Network (VPN) software installed.

SMMEs were also an easy target because they did not always have the budget for sophisticated security software, or might not have a CISO or IT professional. And the health industry was a target because of the extensive data in its records, regarded as personal or highly confidential information This sector was also used as a means to commit fraud, amid people’s concerns about Covid-19 and their health.

Noting that cybercrime increasingly pitted computer against computer, he said: “Covid-19 has brought a trend for hackers to launch more phishing and malware attacks using Covid-19 messaging, and to capitalise on less secure corporate networks.”

While webinar participant polls revealed that 88% were using secure VPNs for home workers and only 38% had experienced phishing or other attacks related to Covid-19, Govender said that many industries other than the IT sector were experiencing a dramatic increase in Covid-19 themed phishing attacks. Govender went on to mention that Google blocked over 240 million Covid-19 related spam emails between March and April 2020 alone.

“The move from corporate to home is where the exploitation has become vast. We see up to 75 records stolen every second by hackers, and 24% of data breaches as a result of human error through phishing or business process errors. 30,000 websites are now being hacked daily.

The motive for these attacks was largely for financial gain,” Govender said.

Govender said: “The average cost of a stolen record on the black market is around R4,000, with health records ($408), financial records ($206) and services records ($181) the most valuable. The reason these records are so valuable is because they contain so much personal information that can be exploited.”

To reduce risk, Govender advised organisations to ensure that laptops were up to date with anti-virus software, that relevant VPN software was enabled, to use hard disk encryption with maximum password requirements, and ensure that remote work policies were the same as when working on the network at the office. In addition, home users should ensure that personal computers also have Anti-virus software and personal firewalls for protection.