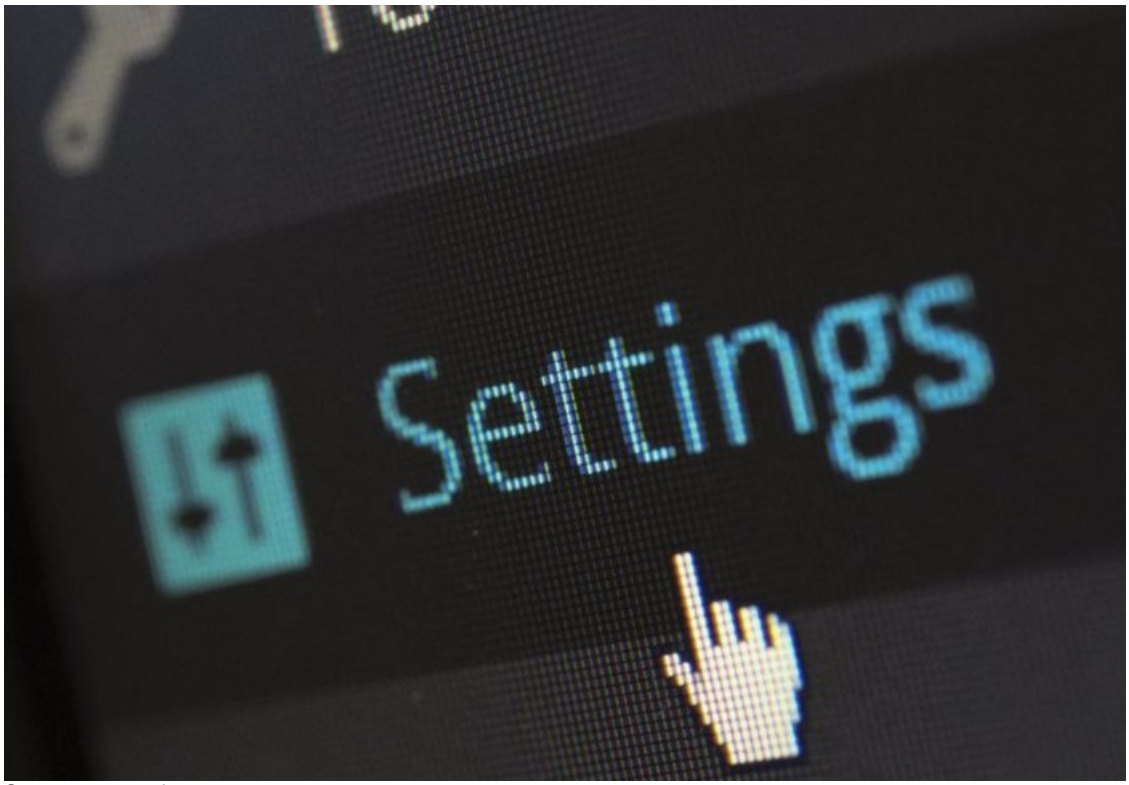
BIZCOMMUNITY

Flattening the cybercrime curve

With millions of office workers now working from home as a result of the Covid-19 pandemic, this has become an opportune time for cybercriminals seeking to exploit the crisis and penetrate corporate defences via unsecured home networks.



Source: www.pexels.com

Unprecedented digital dependency has created unprecedented vulnerability, and an increase in malicious attempts to exploit the mass shift to online platforms for remote working, with South Africa experiencing a ten-fold spike in network attacks when much of the country moved to work from home.

Dr Martin Butler, senior lecturer in digital transformation at the University of Stellenbosch Business School (USB) says companies should ensure that the “digital equivalent of handwashing, face masks, social distancing and decontamination” is being implemented by their now-remote workforce.

Cybersecurity provider Kaspersky reported a spike in South Africa in devices affected by cyberattacks, from the norm of under 30,000 daily to 310,000 on 18 March, and “extremely high levels of cyber exploits since – similar to reports from across the cybersecurity industry and across the world”, he said.

The World Economic Forum (WEF) recently stated that the rise in cybercriminal activity seeking to exploit the Covid-19 crisis made cybersecurity “critical to collective resilience” in the face of the pandemic’s impact on the global economy.

Butler said the risk of “brute force attacks” – in which cybercriminals attempt various password combinations to gain access to corporate systems via individual user accounts – remained high and, with compromised credentials responsible for over 80% of breaches2, businesses need to implement encrypted communication such as Virtual Private Networks (VPNs) now more than ever.

“Ensuring company policies are applied on the corporate laptop that shares a home network with multiple devices such as mobile phones, is not sufficient,” he said.

Trends

Cybersecurity company Cynethas identified two main trends in the coronavirus-linked information security breaches – attacks aimed at stealing remote user credentials, and weaponised email attacks such as phishing and malware that may not be picked up by home email software.

With most work-from-home employees using online collaboration and video conferencing software, Butler warned that some of these systems are not yet integrated into corporate single-sign-on systems or thoroughly tested and embedded in safe remote environments.

“This creates a perfect tsunami for cybercriminals. They can attack devices on unsecured home networks, mostly running outdated software or unsecure hardware, or exploit employees who are using relatively new systems at the extreme of their comfort levels.

“For cybercriminals it is the perfect time to get a malware link to the anxious, and not very tech-savvy, end-user wanting to know the latest Covid-19 news and information. One ill-informed action may be all that is required for ransomware to penetrate corporate defences from remote locations,” he said.

While highly-secure corporate networks should be able to prohibit or at least identify unauthorised activities to ensure that data assets remain protected and services are uninterrupted, home-based WiFi networks and 4G connections don’t have the benefit of corporate security policies and technologies.

“Although it is in principle possible to secure these distributed onramps to the internet that have become central in the work-from-home context, protection of them is now the responsibility of each individual user and not corporate IT – and therein lies the danger,” Butler said.

Security measures

In addition to using encrypted communication such as a VPN, Butler recommended that remote workers take precautions including:

- Using secure and complex passwords; and changing them frequently.
- Not replying to or clicking on links in phishing emails or messages.
- Be on the alert for Covid-19 scam emails.
- Ignore and delete Whatsapp messages with unknown links (especially from unknown senders).
- Take extreme care when connecting to unsecured networks.

Cybersecurity expert and futurist Dr Rianne van Vuuren, a PhD Future Studies graduate from the USB, advised that IT

managers promote cybersecurity by:

- Ensuring that a full-service internet security suite is used by all employees.
- Regular updates of all software, which could save a company from significant future losses if such vulnerabilities are exploited by cyber-criminals.
- Keeping up to date on major cybersecurity breaches in order to proactively ensure that potential vulnerabilities in their networks are secured.
- Developing a risk model as well as a disaster recovery plan with the necessary backups – “this would be a lifesaver in case of catastrophe”.

Butler said where corporate IT policies on using company assets off-site used to focus on physically securing devices, and losing a device was a nuisance – “today, losing control over a device and thus enabling remote access to company systems and data, could be disastrous”.