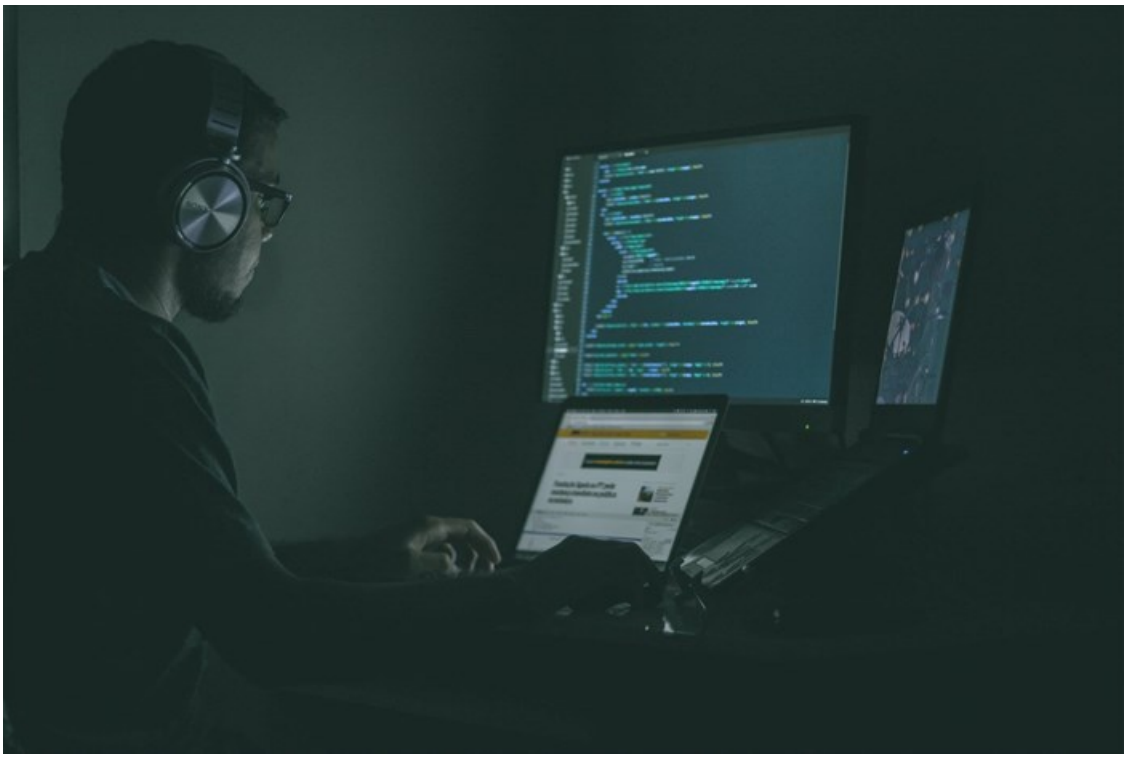
BIZCOMMUNITY

Cybersecurity for your SME: All you need to know

By Siyabonga Mabuza

7 Oct 2022

Effective cybersecurity is as important to the success of any business as capital funding, skills mix, innovation and good management in today's world. This is especially true since the widespread move to remote and hybrid working over the past two years, which has made both individuals and organisations more vulnerable to cyberattacks. And not only are users on open networks more vulnerable to these attacks, cybercrime is becoming more sophisticated every day.



Source: Unsplash

Large companies have the benefit of firewalls, dedicated IT departments and advanced security protocols, but even they're vulnerable to cybercrime, so SMMEs have to be alert to the threat it poses to both business information and continuity.

Yet many don't know where to start when it comes to preventing cyber intrusions, data theft and malicious attacks.

Forewarned is forearmed

The first line of defence against cybercrime is awareness and vigilance – and there's good reason to be vigilant. In 2021 alone, there were 230 million cyberthreat detections in South Africa, with phishing attempts being the most common.

Around 96% of businesses and organisations in the country were targeted by this form of attack during the course of the year, with the number targeted by data and business email attacks not far behind.

And these are no longer simple end-point attacks. Criminal syndicates have developed complex, multi-stage operations that are designed to compromise computer networks through their most vulnerable points; usually their people.

All it takes is a careless click on a suspicious link in an email and the damage is done. This is how most cyber criminals gain access to sensitive information and bank accounts or deliver malicious software, like ransomware.

Ransomware, which is designed to block access to a computer system until a ransom is paid, has become a widespread threat, with 75% of known ransomware having been used to initiate attacks on three out of four organisations worldwide.

What's the solution?

In SMMEs, where entrepreneurs and their staff often perform multiple functions, protecting individual and networked computers from an attack can seem like an overwhelming task.

There are, of course, some important steps that everyone who uses a computer should take.

For starters, it's important not to use the same password on multiple platforms as this makes it more difficult for hackers who've discovered a password to gain access to all of our online accounts. You should also be vigilant of suspicious links in an unexpected email, even one that looks as if it could come from a known service provider.

South African data breach costs reach an all-time high, report finds

28 Jul 2022

Cybercriminals imitate to mirror the mails sent out by trusted organisations, hoping to catch users unaware. In fact, it's a good discipline never to click on a hyperlink in an email. Make it a practice to copy hyperlinks and open them separately in your browser instead. And always remember the golden rule: think before you click.

The importance of training

Ideally, all members of staff who make use of computers, whether standalone or networked, should attend a cybersecurity training course conducted by an established and reputable provider so that they can learn to understand cyber criminals and the way they operate.

As much as individuals and businesses benefit from new technologies, so do hackers. Many make use of AI tools such as machine learning to mine for data that may make computers or networks vulnerable – and many even use bots to maximise the reach of their phishing attacks.

YouTube comments become new tool for scammers

6 Jul 2022

Cybersecurity skills are as important to a business as functional, financial and managerial skills – and training helps

entrepreneurs and their staff to understand more than just the basics. Formal training will, for example, help them to recognise and strengthen vulnerable points in the business's IT and data systems.

They'll also learn more about how AI works, about the metaverse and about blockchain technology – and about how using these technologies can create system vulnerabilities. Most importantly, they'll learn all about ways to protect the business's technology and data systems.

The bottom line is that data is one of the most valuable assets in any business today and, with so much sensitive information now online, nothing can be left to chance.

ABOUT THE AUTHOR

Siyabonga Mabuza is head of cybersecurity for 4th Industrial Revolution Incubator (4IRI).