BitCo

23 July 2018

Cybersecurity: 5 things SMEs should be doing

Chances are you're tired of hearing about security breaches, but with more and more unprepared businesses ending up on the firing line, it's time to start implementing reliable security solutions if your business doesn't already have them in place. Naivety and ignorance are no longer valid excuses, and owners of small and medium-sized organisations in every sector are under even more pressure to comply with data protection requirements as well as safeguard their operations. If big fish like Liberty can be hacked, how vulnerable are local SMEs to cybercrime? You do the maths.

Despite the obvious danger, about 87% of small business owners don't consider themselves at risk of falling prey to cyber-predators. This misconception highlights why it is so important to take real action and ensure that your security measures can adapt to risks before they materialise. Here are five easy-to-implement defence mechanisms for your business:

1. **Strengthen password protection**

   Possibly the easiest security procedure to execute, there's no reason to still use your birthday as your desktop password. Increase password difficulty and uniqueness with a mix of lower- and uppercase letters, numbers and special symbols, and utilise reminders that prompt you to update passwords regularly. Two-factor authentication (which you're probably familiar with in terms of banking app transactions) is also valuable as an additional layer of security for sign-in processes. A further good idea is to limit employee access to passwords according to their role at the company – not everyone needs access to everything on the system as this creates additional avenues for cyber-attackers to exploit.

2. **Educate employees**

   The most advanced cybersecurity system means very little when your staff don't know how to use it properly. Introduce security protocols for keeping employee, vendor and client information safe, as well as damage-control procedures staff can follow should a breach occurs. Train employees to follow best cybersecurity practices at all times. This applies particularly to identifying fake emails and unsecured websites – the typical source of malware infection.

3. **Update devices**

   Regular software, operating system and web browser updates are crucial to shield desktops, laptops, tablets and cellphones against the latest, ever-evolving security threats. Cloud software should be automatically updated by the provider but ensure you and your staff make a point of manually checking for new versions of all other software anyway, especially your antivirus protection. If your employees use personal devices for work – in line with the growing BYOD (Bring Your Own Device) trend, consider having a network administrator install monitoring software and promote automatic security updates on these pieces of hardware. Such cautionary moves help to ensure an uncompromised company network.

4. **Create backups regularly**

   Schedule routine backups (daily, or at least weekly) of all important information stored on company computers and keep a copy of these backup files in the cloud, as well as on an offline hard drive to be extra-safe. Both copies should be encrypted.

Data backups form part of a broader cyber resilience strategy to help your business resume normal operations in the event of a cybercrime incident.

5. **Install an on-premise managed firewall**

   For around-the-clock, all-inclusive and enterprise-grade protection, your best bet is an on-site firewall. A service provider will install, manage, monitor and maintain the hardware, removing any guesswork and offering you peace of mind that your systems and all the precious data they contain are safe from illicit access attempts.

Given that cyberattacks are so prevalent, and increasing, it's best for businesses of all sizes to prepare for the worst. Implementing the above security measures, and having a holistic cybersecurity strategy in place, will help to prevent unauthorised network entry and reputation-damaging data loss.

-ENDS-

About BitCo
BitCo Telecoms, a National Telecommunications Service Provider has been revolutionising business connectivity for over a decade. BitCo builds, maintains and manages their private Fibre Optic and Wireless Last Mile Network which spans South Africa.

Complete control combined with Quality of Service (QoS) guarantees operational uptime and a network to optimally service the broad Business Market.

Not only does BitCo Telecoms offer services directly to companies, they enable any level of the ICT Channel to maximise their business by leveraging off a carrier-grade Fibre and Wireless network.

BitCo's robust network core is housed in one of South Africa's foremost data centres. Here, they peer directly with the other major operators as well as NAP Africa, JINX, CINX and DINX. They have international breakout in Johannesburg, KwaZulu-Natal and Cape Town. This lowers latency, call costs and aids millisecond failover options.

bitco.co.za. Connectivity is Everything.

For more information, contact:

Company:	BitCo Telecoms
Contact:	Communications
Tel:	087 135 0000
Email:	communications@bitco.co.za