BIZCOMMUNITY

Stay safe from cybercrime with what's left of 2019

By Simon McCullough

30 Aug 2019

Data breaches and cyberattacks are undeniably on the rise as hackers become increasingly sophisticated. Across the globe, businesses are finding it difficult to grapple with rapidly shifting cybercriminal motivations, tactics and appetites for destruction.

Simon McCullough, Major Channel Account Manager at F5 Networks

To both understand and keep pace with cybercrime, businesses and consumers should both be wary and adopt the tools to fight fire with fire. With edge computing – its data and the application thereof – distributed across multiple locations cybersecurity remains a very critical part of the business.

This is most imperative in the case of South Africa where digital banking is growing and research has shown that South Africans lose more than R2.2bn to internet fraud and phishing attacks annually.

The reality is that both organisations and consumers are affected by cyberattacks and fraudulent activities, making education around cybersecurity more relevant than ever before as the country moves to greater reliance on digital technology.

Here are some key cybersecurity tips for any growing business, and consumers, to avoid any cyber-fraud tricks.

Tips for organisations

- Got an annoying mail to ask if you have logged on to one of your usual platforms from a different device? Don't ignore it.

  To help detect fraudulent activity, businesses should monitor regular customers and the devices they normally use for purchases. If an alternative device is used, they can challenge the transaction with additional checks – which includes the above-mentioned mail.

- Organisations must ensure that they can gather enough transactional data, and therefore evidence, to prove the fraudulent nature of a transaction or its validity in the case of 'friendly fraud'. Tactics such as using e-signatures or voice verification can help keep high-value transactions secure.

- It's vital to be able to detect new accounts that have been opened on an online store that may be used for fraud purposes. This information can be hooked into shared real-time fraud databases to cross-reference known fraud data such as flagged delivery addresses and mobile numbers, as well as highlighting inconsistencies in sales transactions.

- Cyber attacks also mainly involve distributed denial-of-service (DDoS) attacks that saturate bandwidth, consume network resources, and disrupt application services.

  To defend against this, it's important for organisations to look at deploying an advanced firewall manager that can mitigate threats before they disrupt critical data centre resources.

- App security that detects financial malware identifies fraudulent transactions, and combats phishing scams without requiring customers to download anything is also quite essential.

- Teach and learn – often time many organisational cyberattacks are due to minor mistakes like opening a link in phishing emails or unintentionally allowing backdoors into a network.

  As a result, it is critical for organisations to keep abreast with the latest hacking tricks and educate employees on how to best stay protected.

Tips for consumers

- Limit your transactions on public Wi-Fi networks. Hackers can easily tap into public networks and install malicious malware that gathers sensitive information and passwords.

- Consumers should use well-established, trusted websites, which are much easier to find if you avoid shopping via search engines. Signs of flawed authenticity such as wording or formatting errors are often an indication of fake websites.

- Only shop on locations that are encrypted demonstrated by the 'https' prefix in a retailer's website and a padlock symbol in the browser.

- It's important to keep an eye out for phishing emails and SMSes. These usually appear to come from a well-known

brand and ask for personal or financial information – something a retailer would never normally do.

- Consumers should avoid retailers that ask for payments via money order, pre-loaded money card or wire - methods often associated with scammers.

- Download apps from trusted sources. Each device comes with operation software and a store where users can download verified and safe applications instead of downloading application of the internet where links may very well direct you to an untrusted site or replica of the application you wish to download.

ABOUT SIMON MCCULLOUGH

Major Channel Account Manager at F5 Networks
- Try to tackle cybersecurity during #RWC2019 - 20 Sep 2019
- Stay safe from cybercrime with what's left of 2019 - 30 Aug 2019
- Multi-cloud's new multiculturism - 21 Aug 2019
- A new phase of cyber warfare has begun - 7 Aug 2019
- The ABC of DevOps - 27 Jun 2019

View my profile and articles...