Building cyber-savvy workplaces in SA

By Dan Thornton

3 Oct 2022

South Africa is globally ranked as one of the most vulnerable countries when it comes to cybercrime. The lack of a strong, centralised approach for protecting the country's national and privately-owned digital assets is just one of many weaknesses. Throughout our society, there's a pervasive lack of awareness of cyber threats and how to properly mitigate them. This may be because cybercrimes can seem complex, opaque and ethereal.

Image supplied

The vast majority of cyber-attacks against South African businesses and individuals are carried out by international cyber criminal groups operating far outside of our borders and jurisdiction. What is needed is much stricter security minimum standards enforced on the country's enterprises handling personal data and providing essential services.

Enforcement of these standards and the data protection laws of the PoPI Act need to be better implemented.

Staggeringly, the World Economic Forum has estimated that 95% of data breaches occur due to human error. Cybercrimes represent billions of dollars in lost revenue every year, and it's clear that there's an urgent need for training and mobilising people to be actively involved in cybersecurity.

International Cyber Awareness Month is celebrated in October, and in 2022 the theme is 'See yourself in Cyber'. It's a straightforward appeal to individuals; consumers and employees, business owners and leaders to recognise that like all crime, cyber wrongdoing is all about people.

There are basic steps that everyone can take to protect their online information and privacy on the job, at home and at school.

In the workplace, it's not enough for the tech team or IT department to be cyber-savvy - every employee working on the company system in the office or remotely needs to understand threats such as phishing and social engineering so that they can recognise and report them.

According to CSO Online, phishing attacks account for more than 80% of reported cybersecurity Incidents. This happens on this scale because too many people simply cannot discern this criminal tactic and are duped.

Many organisations deploy spam filters, advanced firewalls, network access controls and endpoint scanning tools to mitigate increasing cyber threats, but unfortunately, no technology can account for human error entirely.

This is not just relevant to big companies, small and medium businesses, which tend to deploy less cybersecurity tools, are viewed by cybercriminals as the 'low hanging fruit'.

This means that no matter the size of your company, effective security awareness training is essential in educating all your end-users so that they understand the security risks associated with their actions and use best practices for staying security-savvy.

Creating a secure working culture in businesses today is essential. Business owners, company executives and board of directors are beginning to take cyber risk just as seriously as any other form of business risk, such as financial risk. This top-down driven prioritisation of cybersecurity is a critical success factor in protecting a company's digital assets, and the consumer data you may be storing.

Cybersecurity should be front of mind in all activities and at all levels of the organisation. Employees should be rewarded for secure behaviours and managers should be equally rewarded for effectively driving cybersecurity awareness and encouraging behavioural change in the organisation.

In recognition of Cyber Awareness Month and the impact of cybercrime on us all, South African consumers can take these three basic steps to keep their data safe at work, home or school:

- Set up Multi-Factor Authentication (MAF) on every one of your online accounts - especially your email, banking and social media accounts.
- Use strong passwords and use a reputable password manager to keep them safe.
- Be informed so that you can recognise phishing and social engineering tactics, and always report a suspected attack.

ABOUT DAN THORNTON

Dan Thornton, CEO and co-founder of GoldPhish Cyber Security Training, is a former Royal Marine Commandos Officer. During his seven years of service, he was deployed all over the world including multiple operational deployments leading teams in both Iraq and Afghanistan. He then transitioned from the military into a career in Corporate Security Risk Management helping international oil and gas companies operate safely and securely in some of the most high-risk locations around the world, including West Africa, North Africa, and the Middle East.

- SA shoppers warned of online scams ahead of shopping season - 20 Oct 2022
- Building cyber-savvy workplaces in SA - 3 Oct 2022
- Cyber savvy parents keep kids safer online - 22 Aug 2022
- Cyber fraud has steep collective costs - 27 Jul 2022
- Why cybersecurity needs to tighten up as cryptocurrencies plummet - 22 Jun 2022

View my profile and articles...