It's official: South Africa is the cybercrime capital of Africa - here's how to protect yourself from becoming a statistic

By Jackie Smith

18 Jul 2023

Recent data from TCG Forensics shows that South Africa is rapidly emerging as the 'cybercrime capital' of Africa, poised to surpass Nigeria and its notorious 'Nigerian Prince' scams in terms of cyber-criminal activity.

Source: Supplied. Jackie Smith, head of Buyers Trust.

Despite substantial investments from both the private and public sector in boosting cyber security and the passing of the Cybercrimes Act in 2021, thousands of innocent South Africans continue to fall prey to these types of crimes each year.

Highlighting the surge in cybercrime, the Southern African Fraud Prevention Services reported a staggering 356% increase in impersonation fraud between April 2022 and April 2023.

Why is South Africa so vulnerable to cybercrime?

Several factors contribute to South Africa's vulnerability to cybercrime, the first being the last two decades' economic expansion and evolving digital landscape, which makes it an attractive target for criminals seeking quick financial gains.

Cybercrimes can be committed by anyone with access to a cellphone and an internet connection, making these crimes incredibly easy to perpetrate. And with only an estimated 10% of cybercrimes reported to the police, criminals feel that they can operate without consequence.

Another reason why cybercrime has escalated to such a degree is that there are only a small number of police officers equipped with the specialised skills needed to address cybercrimes. Consequently, the prosecution and policing of cybercrimes become exceedingly difficult, allowing sophisticated organised crime syndicates to operate with relative ease in the country.

The property industry and cyber threats

The property industry has become an attractive target for cyber criminals due to the vast amount of valuable personal data involved and financial transactions that take place daily. As a company that was developed in part to give the highest level of security to the deposit component of real-estate transactions, we have first-hand insight into how vulnerable the industry is to cyber threats.

Here are the two primary types of cybercrimes that the property industry should prioritise and be wary of:

- **Data breaches:** Property companies handle large volumes of personal and financial data related to buyers, sellers, tenants, and landlords – including addresses and debit- and credit-card details. Cybercriminals may attempt to hack into online databases and gain unauthorised access to this data to commit identity theft, financial fraud, or sell the information on the dark web.

- **Deposit phishing schemes:** Here, fraudsters will intercept emails between a buyer and seller to pose as a legitimate real-estate agent or conveyancing attorney to divert the buyer's deposit into their own bank account.

Unfortunately, it can be very difficult to tell the difference between a legitimate email communication and one sent by a fraudster. This is because cybercriminals are becoming increasingly sophisticated, hacking into the attorney or real-estate agent's firm to study the language used, company letterhead and transaction types.

4 ways to manage the human threat to cybersecurity

Carey van Vlaanderen 18 Jul 2023

This allows them to craft phishing emails that appear totally legitimate, while the unsuspecting buyer is cheated out of their hard-earned deposit. Attorneys and estate agents are not cybersecurity experts - nor are they expected to be - but that does increase the likelihood of these crimes occurring.

The best way to minimise the risk of falling victim to a phishing scheme is by entrusting your deposit to a highly secure and transparent third-party alternative, which also offers a bank guarantee.So to protect yourself from email phishing scams:

- **Be cautious with email links and attachments.** Avoid clicking on suspicious links or opening attachments from unknown or untrusted sources.

- **Double-check email senders.** Scrutinise the email sender's address carefully and be wary of emails that have slight variations or misspellings in the sender's name or domain.

- **Verify website authenticity.** Before entering any personal or sensitive information on a website, ensure it is secure. Look for "https://" in the URL and a padlock icon in the browser's address bar.

- **Don't share sensitive information.** Avoid sharing details like passwords, identity numbers, or account numbers over email or unfamiliar websites.

- **Take the 'human element' out of the equation.** The Buyers Trust platform employs the highest level of cybersecurity measures, ensuring that your deposit will be protected until the property transfer process is complete.

ABOUT THE AUTHOR

Jackie Smith is the head of Buyers Trust, a subsidiary of ooba Group and a safe and secure bank-hosted deposit solution for homebuyers.

For more, visit: https://www.bizcommunity.com