How SA's property industry can avoid falling victim to cybercrime

According to the South African Banking Risk Information Centre (Sabric) Annual Crime Statistics report for 2018, digital crime increased by 4.9% from the previous year, amounting to R2.6 million in losses for unsuspecting victims. The report lists phishing, vishing, SMiShing and e-mail hacking or business e-mail compromise as the most prominent digital fraud examples in South Africa.

© Jakub Jirsak – 123RF.com

Handré van der Merwe from identity and IT security solutions consultants BUI says that South Africa's property industry hasn't kept pace with the changing cybercrime landscape, leaving itself open to a variety of possible data and financial breaches. "The property industry is in a challenging state in the current economic climate, which means that normal safety processes aren't necessarily being followed to the letter. Buyers aren't being properly vetted and security checks are being overlooked. In addition, small business owners very often don't have the budget available to adequately secure their data, processes and operations."

Cybercrime is a major concern for businesses, with South Africa ranking in the top five cybercrime hotspots globally. "The perception is that hackers are only targeting big businesses, but it's often small-to-medium sized businesses that unwittingly provide gateways for cyber villains to exploit," says van der Merwe.

PayProp CEO Jan Davel says potential for cybercrime is rife in residential sales and rental transactions. "Property businesses such as estate agencies handle substantial financial transactions including monthly rent and upfront damage deposit payments, making them ideal targets for criminal activity. An example of this is a man-in-the-middle attack, where electronic communication between an agent and buyer is intercepted and important information like banking details is altered, redirecting payment to the wrong account."

Van der Merwe lists a few ways in which property-related businesses can avoid falling victim to cyber criminals:

1. ***Plan to mitigate attacks:*** Have a plan in place that encompasses a good mix of technical controls and best practice if a breach takes place. Nominate a team in advance to deal with the attack and mitigate risks as much as possible. For example, one team member could be a direct line of contact to the organisation's banking partner, while another could be in charge of customer communication, with draft communications at their disposal.

2. ***Raise awareness within your business of the risk:*** Encourage staff members to research data security best practices, including e-mail security. Many publicly available tools exist, including a confidentiality setting on Gmail, which is as simple as ticking a box before sending an e-mail.

3. ***Strengthen business processes:*** A major cyber risk to any business is access to business e-mail and servers from the devices used by employees. Take time to redesign communications and access policies governing on-boarding and termination of employees – including how data is accessed on their mobile phones, tablets and computers, and how it is eventually removed once their employment is over.

4. ***Use common sense:*** Many security breaches could easily have been avoided using common sense. Van der Merwe says it's a case of setting a baseline in your own business. "Once a baseline of 'normal' interactions and business is defined, then it's just a case of looking for anomalies, which will trigger alarms."

"We cannot throw the dice and depend on luck for protection," warns Davel. "It's important to be aware of the risks, to query anything that looks suspicious, and to stay informed about the latest industry-specific scams. We're all busy. We all get tired and frustrated. But we've got to focus on the finer details." So, check that payment authorisation form one more time. Call that client with the strange e-mail address. Stop, think, evaluate, and then act responsibly.

Davel says opportunity exists for property industry business owners to put themselves ahead of their competition and pre-empt any possible breach situations that might arise. "Taking the steps and making the financial investment to protect yourself and your business will mean there are no nasty surprises in future and, ultimately, your business operations aren't unduly interrupted."