Social media hackers are a threat to business security - Broeke

Recently, a growing number of South African Facebook profiles have been cloned for malicious and criminal reasons. These cyber attacks on social media users could have dire consequences for businesses as well as individuals.

So says Richard Broeke, regional sales manager at specialist IT security company, Securicom: "The growing and almost unrelenting use of social media and mobile devices by today's consumer has opened up new avenues for online criminals to steal people's identities or personal information, and infect their machines and devices with malware and spyware.

"They are following users onto social media platforms and literally spying on them, with the intent to steal money, information or both. In 2012, there was a dramatic increase in hacks and attacks on individuals. It's likely to get worse this year," he warns.

Vulnerable, valuable information

According to Broeke, scammers are using social media platforms as spam and phishing tools. This includes sites such as Facebook, Twitter, Pinterest, LinkedIn, and Tumblr. In the recent South African example, local Facebook profiles were cloned and used to solicit money (according to The Times Newspaper).

Users have also had their accounts hacked, allowing the hacker to distribute spam and other offensive content. Typically, affected users have put themselves at risk by clicking on links to external games, applications, and shopping sites which are unsafe.

"When you consider the type and volume of personal information people share on social media, from birthdates, home addresses, and their places of work, to photos of their children, and their whereabouts, it's not difficult to see why these platforms are fertile hunting grounds for online scammers and criminals. All of this information is very valuable for identity thieves, spammers and scammers," says Broeke.

Think before you click

In its 2013 Internet Security Threat Report, Symantec reports a significant increase in spam and phishing on social media sites, even as these attacks via traditional routes, such as email, have fallen slightly. The ultimate goal of cyber spies is to make money by stealing banking details, personal information, and the email addresses and contact details of their victims' friends and business associates.

Citing from the report, Broeke says typical threats include fake gift cards, competitions and survey scams. These kinds of fake offer scams account for 56% of all social media attacks. For example, in one scam the victim sees a post on somebody's Facebook wall or on their Pinterest feeds that says "Click here for a free gift card". In another scam, users are lured to enter a competition with the chance to win prizes.

When the user clicks on the link, they go to a website where they are asked to sign up for any number of offers, turning over personal details in the process. The spammers get a fee for each registration and, of course, there's no gift card or competition at the end of it all.

Other common methods of attack include Manual Sharing Scams, which rely on victims to share intriguing videos, fake offers and messages, and "likejacking", where attackers trick users into clicking fake "like" buttons which install malware and may post updates on the user's newsfeed to spread the attack.

Beware what you share

Broeke says increasing social media threats and attacks is a business concern: "The use of online social media platforms by a company's employees creates a gateway for web-based malware to enter and compromise corporate networks. By inadvertently clicking into websites infected with malware, users make company data, customer information and employee information vulnerable."

He stresses that the ever-burgeoning use of social media coupled with the growing use of these channels by online criminals point to an urgent need for companies to implement robust measures to protect their networks against web-based malware: "This means having a comprehensive web security solution in place, multiple-layer security software at the network perimeter, and robust endpoint security on all endpoints used by employees, including PCs, laptops, and mobile devices.

"Companies should also have strict policies in place to define and limit the amount of personal and business information their employees can share online. Corporate IT security and email and internet usage policies formalise the rules relating to the usage of company assets and internet access, and establish how the organisation intends to secure their infrastructures, data, and ultimately the business. Employees also need to be aware that online and email usage is being tracked.

"Also, educate employees about the risks of social engineering and sharing information online. They must also be aware of the dangers of downloading applications, and understand how to optimize their privacy and permission settings on the various platforms they frequent.

"Appropriate training and effective policies can reduce the risk of accidental data loss and other risks," concludes Broeke.

For further information on Securicom, go to www.securicom.co.za.