Outstanding Features Make Voip A Fraud Target

Two-thirds of South African respondents to a PricewaterhouseCoopers (PwC) global survey indicated they have been victims of economic crime over the preceding 24 months. Almost one-third of local organisations reported experiencing cybercrime.

Debit card fraud is up, as is Card Not Present (CNP) fraud, according to the South African Banking Risk Information Centre (SABRIC). What's also up on the fraud front, are hacking attempts perpetrated primarily by foreign nationals attempting to compromise South African telecoms networks for financial gain. Here, reverse-billing takes centre stage.

That's according to Rad Jankovic of local independent telecoms provider, OTEL, who says that while reliable statistics are hard to come by, South African telecoms networks successfully fend off overseas-based hacking attempts "every minute of every day".

'VoIP's cost-saving potential and its ability to easily offer a plethora of value-added services means it is quickly overtaking traditional landlines as the world's telecoms technology of choice. Greater usage means greater visibility and VoIP has certainly been noticed by the world's fraudsters," said Mr Jankovic.

According to industry news platform, Fraud & Technology Wire, VoIP fraud can occur is many ways. One of the more common techniques is service abuse, also referred to as subscription fraud. Service abuse fraud occurs when a fraudster signs up for a VoIP service under an alias, runs up a large bill and doesn’t pay. Premium rate service fraud is also an example of subscription fraud that can be accomplished by fraudulent use of VoIP, says Fraud & Technology Wire.

VoIP fraud can affect any organisation which uses VoIP services, just as debit or credit card fraud can affect any consumer or company that uses financial services. The solution to beating fraud is not to stop using targeted services, but to become smarter when using them. Mr Jankovic outlined four common sense ways to beat VoIP fraud:

The vast majority of attacks by telecoms hackers occurred outside of normal business hours as this is when company server security staff were most likely not on duty. OTEL offers clients automated, realtime VoIP system monitoring meaning your VoIP security comprises many layers of protection.

A great password tip is not to use passwords on VoIP systems that are single words. Rather, join many words together that tell a familiar story. For example, IMETJANEONMYFIRSTDAYOFSCHOOL.

With a business VoIP number, it’s important to ask your service provider to set a credit limit on your account. This will help stop hackers from running up postpaid bills.

Voicemail systems can be unsecured entry points into your business. Ensure that PINs used to access enterprise voicemail systems are not generic or left as default options.

Finally, OTEL's VoiP services include multilayered fraud detection for end user clients and resellers.

From a modest operation in 2008, OTEL is today a licensed business-to-business provider of VoIP & broadband Infrastructure-as-a-Service (IaaS) solutions. Its nationwide dedicated network and cutting-edge technology positions OTEL as one of South Africa's leading telecoms providers with a specific focus

on meeting the needs of SMMEs. Its wholesale and retail fibre solutions are designed to increase profitability and reduce downtime and include hosted PBX, free email, server hosting, cloud services, as well as full-featured call centre solutions amongst other value-added voice and data services.