Telecom Fraud Alerts

Fraud Alerts October – December 2013

Loss due to SIMBOX Fraud Exceeds $2 Million in West Africa

Loss due to SIM Box fraud on a leading operator in West Africa was estimated to be around $2 million in the last 8 months. This also includes the USD 770,000 lost by the government of Ghana. In this period, it was detected that over 30,000 SIM cards had been used by SIM Box fraudsters to terminate international traffic in Ghana. It is understood that the operator's network became attractive to fraudsters because it was new on market and some of its tariff plans offered extremely low off-net call rates in the market.

**Source: CellularNews – www.cellular-news.com*

PBX Hacking Incident in Belton

Hackers attacked the Bell County phone system and rang up potentially thousands of dollars in fraudulent charges.

It is learnt that on two separate occasions hackers were able to exploit weaknesses in the county's phone system to enable them to place outgoing calls that appeared to be coming from, and be billed to, Bell County. The hackers targeted a weak password on an extension in one of the departments. Part of the problem was the minimal password requirements currently in place for the county's phone system.

Once they gained access to the phone's automated menu system, the hackers were able to activate the remote-dial feature, which allowed them to route international calls from a third-party number through the Bell County switchboard.

By routing the calls through Bell County's phone system, all the relevant charges would be billed to the county.

PBX Hacking one of the most common types of phone fraud in the world and these attacks cost companies billions of dollars per year. An October report from the Communication Fraud Control Association, a communication security organization, estimated that total phone fraud costs communications companies more than $40 billion annually. Private branch exchange hacking alone cost telecom carriers $4.42 billion last year.

A large part of the reason for the high cost of private branch exchange hacking is the attack is relatively easy to execute.

**Source: Temple Daily Telegram – www.tdtnews.com*

Internal Fraud Causes Massive Losses to Liberian Operator

In what could be the biggest cellular technology fraud in recent memory for Liberia, a cellular carrier, is pressing criminal charges against one of its own employee, for a case of SIM box fraud causing losses to the operator, the Liberia Telecommunications Authority (LTA), the government of Liberia as well as rival carriers. The operator had noticed some SIM boxes missing a few months ago but never reported the matter to the LTA or authorities.

Police sources indicated that the theft is costing massive losses to the Liberia Telecommunications Authority and the other two major carriers. Investigators have also informed that the company's CEO is being considered a Person of Interest in the case and that more people may be involved in the scam.

SIM Boxes remain a major problem for many network operators, having also negative effects on roaming hub providers and customers alike because they decrease operator revenues due to call redirection, service inaccessibility and missing callbacks. The quality is also said to decreases significantly when SIM Boxes redirect calls over inadequate, highly compressed IP connections, which results in image loss and dissatisfied customers.

**Source: AllAfrica News – www.allafrica.com*

Weak Password Leaves Private Company with Huge Bills

A private company whose telephone system was hacked and the lines used to make more than $30,000 worth of international calls has been left to foot the bill. The company blamed the telecom operator for not informing/warning them about high usage. However, the telecom operator maintains that the security of such PBX systems is the responsibility of the user.

Hackers targeted the company's Private Automated Branch Exchange (PABX), a computerized system that manages a company's internal phone extensions. The hack was discovered after a staff member noticed that there were about 20 voicemail messages consisting of clicking noises and dial tones.

Hackers had used the default access code - 0000 - to dial into the voicemail system, and then from there to dial out, making a large number of overseas calls.

**Source: NelsonMail – www.nelsonmail.co.nz*

For all previous fraud alerts click on the following link: http://www.subex.com/fraud-alerts.php

To follow active discussions on various topics log on to or subscribe to: Telecom Fraud Professional Group LinkedIn, @SubexTweets and Subex Blog

Get in touch with our experts to know more about delaing with telecom frauds.