

Subex Telecom Fraud Alerts

February 2011

Value added service fraud

A new fraud trend has been spotted doing the rounds in Nigeria. This type of fraud uses a deceptive type of value added service number longer than most short codes. The victim gets a message on his mobile from this number saying "Hi, I tried to call you, call me back on this number. +96XXXXXXXXX". The victim upon receiving the message quickly dials the number and is greeted by an IVR asking him to wait while his service is sorted. This turns out to be an unending Interactive Voice Response (IVR) leading the victim through a maze of options and encouraging him to stay longer online. Eventually, the victim's air time runs out. Each minute cost N100, but the text doesn't specify that and also does not mention the details of the service provider. One victim spent five minutes on the call but never got to speak to anyone and could not find out who it was that wanted to reach him. He hung up and upon checking his balance found out that he was billed N500 for the five minutes he spent with the IVR.

In a similar scam, another victim received text from a different 10 digit number saying that a secret admirer had sent a love song. The text instructed the victim to call +67XXXXXXXXX to hear the song and the identity of the person that sent the song. The victim upon calling is again subjected to an unending IVR and is billed for that.

In another incident, a victim received a message from a short code 5XX, which was being used by a legitimate service provider in Nigeria for promotional purposes. The message said that the victim has been selected to participate in a contest where he/she could win N10 million and a car. To participate, simply reply "yes" to the text. The victim upon answering the first question was immediately pulled into in a maze of unending question and answer texts which lasted five days and cost a total of N35, 000 on his contract plan.

Operators are advised to inform their customers to be wary of this threat and not to respond to such messages, or indeed any form of unsolicited communications. Operators can detect these frauds using typical high volume/value based rules on B-number. .

**Source: Next, Feb 2011*

VOIP fraud on the rise

VOIP fraud is slowly but steadily on the rise. A small Manhattan company was subjected to this kind of fraud recently. The company's VOIP telephone system was hacked and billed for long distance calls to Cuba to the tune of \$45,000 in just three days. The hackers apparently managed to gain access to the phone system due to insufficient security features. The fraudsters were then able to dial in locally to the company's digit and obtain dial-tones on their trunk shape, allowing them to make numerous outbound calls to Cuba.

Although the company's long distance provider initially managed to warn the customer, it was slow to cut off the traffic. Also, instead of just cutting traffic to Cuba, the carrier cut off all long distance service, thus preventing the customer from doing business.

There were basically two reasons that led to the huge losses. First, after installation of the VOIP system, certain default features that were activated from the factory should have been restricted. Secondly, the company's long distance carrier's response time to blocking the traffic should have been faster.

To avoid such instances of fraud in the future, the following precautionary measures should be taken

- *Ensure that all manufacturer default passwords for system administration are altered promptly, using lengthy and complex alphanumeric passwords.*
- *Lock out administrative access ports after three successive invalid access attempts.*
- *Configure the system to send an alert of the lock-out to system administrators.*
- *Ensure that all remote access to system administration portals is with encrypted challenge/response authentication.*
- *Ensure that all VOIP system administration ports are on a secure subnet, with Access Control Lists allowing only specific IP addresses necessary for maintenance and administration.*
- *Ensure that all multi-media and voice messaging interfaces to call managers or PBXs are appropriately restricted.*
- *Ensure that access to system speed dialing is controlled by business need.*
- *Review and control all thru-dialing and out-mission from adjunct gear. Do not allow default entries in restriction/permission lists.*
- *Set and enforce standards for complex passwords for voice message mailboxes. Ensure period password resets for these mailboxes and regularly check for default passwords in end-user mailboxes.*
- *Check transfer restrictions in all integrated peripheral and adjunct gear. Block access to ARS codes and trunk access codes.*
- *Check endpoint targets for keyed entry and time-out transfers in call dispensation mailboxes and auto attendants.*
- *Verify all off-net target endpoints in ACD vectors and VDNs.*
- *Protect often-abused features with forced account codes, authentication codes or barrier codes.*

**Source: Report News, Jan 2011*

For all previous fraud alerts click on the following link: <http://www.subexworld.com/fraud-alerts.html>