Telecom Fraud Alerts

Fraud Alerts January – March 2014

PRS Fraud racket worth £2.8 Million busted in UK

A gang which hijacked mobile phone accounts to swindle £2.8million from customers of a leading operator by making £2.50-a-minute calls to a premium has been busted in UK. The fraudsters assigned phone numbers of genuine customers to a SIM card in their possession by calling up and posing as the account holder. They then used the SIM cards to repeatedly call premium rate lines they had purchased, which typically had connection charges of around £2.50 per call.

The operator would pay those premium rate lines for the calls before billing the genuine customer, whose only knowledge of the fraud would be that their own phone had ceased to operate. Some bills received by genuine customers were in excess of £80,000.

**Source: www.dailymail.co.uk*

PBX Hackers going unnoticed in the industry

A new industry study has revealed that a shocking 45 per cent of IT managers are not aware of PBX phone fraud - a malicious practice which leaves businesses at risk of footing huge phone bills from fraudulently made calls. The figures come from a new survey by a leading internet hosting and communications service provider. The figures also reveal that 59% of those surveyed have a PBX system that is more than five years old - or are unaware of its age altogether.

As voice networks have become more sophisticated, so have the scams used by phone hackers, fraudsters and other malicious perpetrators to make an illegal profit - meaning that PBX hacking is now a growing threat to any business connected to the public telephone network.

**Source: www.techzone360.com, March 2014*

Operators lost €500,000 in a short-lived Fraud operation in Barcelona

Agents of the National Police in Barcelona have broken up an organized group that defrauded 500,000 Euros with fraudulent calls to premium numbers. Based on the allegations made by various mobile operators affected by fraud, the agents had discovered that a common modus operandi. The group was highly specialized and organized with a clear division of functions between its members. The fraudsters are known to have used fake websites and IMSI manipulation to build a web of corruption.

With SIM cards illicitly obtained, the team members conducted massive call traffic in a short period of time to international premium rate numbers. The gang was relying on the delay between the resolution of roaming bills between operators to generate more than half a million Euros in revenues.

**Source: www.policia.es, January 2014*

IRSF Fraud on the rise in the United States of America

Telephone companies in the United States are seeing missed calls used to enable International Revenue Share Fraud (IRSF). Fraudsters are using call generators with automated spoofing capabilities to place calls to a large volume of US cell phone numbers. The calls typically ring once. The number displayed on the recipient's caller ID is a high cost international number, usually located in the Caribbean. The recipient calls the number back and is greeted with a message designed to keep them on the line, such as "Hello, you have reached the operator, please hold." The longer the caller stays on the line, the more revenue fraudsters generate.

Area codes used in the spoofed numbers are from Anguilla, Antigua, Barbados, British Virgin Islands, the Commonwealth of Dominica, Grenada, Montserrat, and the Turks and Caicos Islands. These countries' numbers are part of the North American Numbering Plan and do not require 011 to be dialed as with other international calls.

Some operators are beginning to block these area codes to avoid this type of charge.

**Source: Internet Crime Complaint Center, February 2014*

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 dealing with telecom frauds.