Telecom Fraud Alerts

Fraud Alerts October - December 2014

PBX Hackers leave a firm with bills over $166,000

An architecture firm in San Francisco suffered from a PBX Hack which resulted in bills exceeding $166,000 within a week. Hackers had broken into the phone network of the company and routed calls from the firm to premium-rate telephone numbers in Gambia, Somalia and the Maldives. It would have taken 34 years for the firm to run up those charges legitimately, based on its typical phone bill, according to a complaint it filed with the Federal Communications Commission.

PBX hacking which is one of the easier frauds to pull off and is highly profitable, cost the telecom industry a whopping $4.73 billion last year according to CFCA.

Hackers break into a business's phone system and make calls through it to their premium number, typically over a weekend, when nobody is there to notice. With high-speed computers, they can make hundreds of calls simultaneously. The hacker gets a cut of the charges, typically delivered through a wire transfer.

**Source: www.nytimes.com*

The £3.5 billion mobile theft and PRS racket

Worldwide, more than 300,000 mobiles are reported stolen to police each year. Many are never reported, as they are snatched overseas. A report by global mobile phone trade body the Communications Fraud Control Association estimated that, last year, globally, £3.9 billion was lost to fraudulent international calls, and a further £3.02 billion to premium-rate line fraud. Around half of this bill, £3.5 billion, was footed by consumers who had phones stolen and businesses who have been scammed.

Within a few minutes of stealing a phone, the criminals make calls to premium rate lines located in countries such as Somalia, North Korea and little-known Pacific islands and are controlled by middlemen. Every minute the line is connected, both take a cut from the charges they run up. The fraudsters connect several calls from the same phone at one time - by dialing one premium-rate number, putting it on hold and then dialling another.

**Source: www.thisismoney.co.uk*

SIM-swap fraud: A new way of stealing money

With mobile phones becoming a convenient tool for banking, fraudsters have begun to use SIM-swap as a mode of stealing money.

The modus operandi: A fraudster obtains bank account details of a victim and registers the mobile phone number through phishing or malware. He approaches the victim's mobile service provider with a fake identity proof and, claiming loss of handset or SIM damage, seeks a duplicate SIM card. Following verification, the original SIM is deactivated and a new one is issued to the fraudster. He then initiates financial transactions from the victim's bank account, details of which he had earlier stolen, and receives payment confirmation requests on the duplicate SIM. Since the original SIM has been deactivated, the victim remains unaware about the fraudulent transactions being made.

Though not a telecom fraud directly, telecom operators become partially responsible for the theft considering the fact that the SIM-swap allowed by the operator was the main step in carrying out the theft.

**Source: http://www.business-standard.com/*

Ghana loses USD 40 million on SIM Box Fraud yearly

The government of Ghana loses around 40 million dollars each year through the activities of bypassing the Approved International Gateway (SIM Box Fraud). The National Communication Authority along with the industry players, the judiciary and the law enforcement agencies has been trying to wage a war against fraudsters since 2010 in the country. SIM Box Fraud is more prevalent in many countries where the cost of terminating international call exceeds the cost of a national call by a considerable margin. Fraudsters, through the use of different Bypass mechanisms, sell capacity to terminate calls cheaply in these countries, on the open market or through direct connections with interconnect operators. CFCA estimates that the industry lost over 2 billion USD to this kind of fraud last year.

**Source: http://www.biztechafrica.com*

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.