Telecom Fraud Alerts

July-September 2015

Europol 'dismantles' Spanish cyber-crime group

EU law enforcement agency Europol and the Spanish police force have been able to take down a cyber-crime group operating with a 'sophisticated' illegal call center from Barcelona.

Under a joint operation, raids and arrests took place in Barcelona and the telecommunications-based cyber-crime in this case is classified as International Revenue Share Fraud (IRSF).

The cyber-crime group had established a channel to receive mobile phones stolen from tourists in Spain. A further network of premium rate numbers had been set up and managed by other members of the criminal group based outside the EU. Stolen device phone numbers were then harvested and exploited until the point at which they were blocked by telecom operators in their country of origin.

Europol explains that it analysed thousands of financial transactions to reconstruct the money flows and destinations across several international jurisdictions. The criminal damage wreaked by the group has been estimated to be at least €2 million.

**Source: www.scmagazineuk.com*

Mobile Advertising Fraud now costing close to $1 billion per year

According to a report from a fraud-detection firm, as much as $1 billion of mobile advertising money is being lost to fraud in a number of ways-including malicious apps that hijack mobile phones and turn them into an ad-viewing botnet.
In this process, malicious mobile applications pretend to exhibit human behavior by loading new pages or cycling through functions in an app, all of which loads advertising. But they load far more ads than any normal application would-as many as 20 ads per minute-and in many cases they do so in the background when the app isn't being used-which means they are never seen.

It is understood that fraudulent apps drive traffic through most of the major mobile ad exchanges and networks, and in some cases establish 1,000 connections per minute, connecting to more than 300 networks, servers, exchanges and ad providers in less than an hour.

**Source: www.fortune.com*

SIM Box Fraudsters arrested in Ghana

Three persons who allegedly engaged in the termination of international calls and caused the government a revenue loss of $196,992 have been arrested by the police in Ghana.

The suspects reportedly used voice over Internet protocol (VOIP) technology to route calls to landlines and cell phones from any part of the world to Ghana and vice versa.

In addition to the three arrested, another accomplice who is a distributor for a leading telecom operator is absconding and efforts are being made to get him apprehended.

During the raid, the task force confiscated two SIM boxes, as well as 800 top-up cards belonging to major telecom operators in the country.

Additionally, the task force found one generating set, two heavy-duty batteries, one uninterruptable power supply (UPS) equipment, one laptop, one mini tablet, two Internet modems and 16 antennae.

**Source: www.dailyguideghana.com*

Fraud Investigator held in a case of Internal Fraud

A man who worked as a fraud investigator for a telecommunications company in Australia has been arrested for alleged fraud and cash embezzlement during his employment. NSW Police arrested the fraudster following an 18-month investigation.

The case was investigated when the Sydney-based telecommunications discovered misappropriation of 120 mobile phones as well as embezzlement of cash payments. The accused is claimed to have fraudulently distributed the mobile phones to professional sports players, clubs and others from 2008 to 2012. Police said they believed those accepting the phones were told the devices were either a gift from the telecommunications company or a part of a sponsorship deal. The police also allege that the man embezzled funds by not passing on payments he received for his work onto the company.

The man has been charged with 68 offences including 28 counts of fraud, 35 counts of obtaining benefit by deceit, three counts of embezzlement and two counts of indenting to defraud by using false or misleading statements.

**Source: www.itnews.au*

For all previous fraud alerts click on the following link: http://www.subex.com/fraud-alerts To follow active discussions on various topics log on to or subscribe to: Telecom Fraud Professional Group LinkedIn, @ SubexTweets and Subex Blog.

Write to us at info@subex.com to know more about dealing with telecom frauds.