Subex Telecom Fraud Alerts

September 2013

Multiple Cases of SIM Box Frauds in Ghana

A tier 1 operator working closely with the Criminal Investigations Department of the Ghana Police Service helped bust a SIM Box Fraud Syndicate. Police uncovered two hyper media SIM gateway equipment, each with the capacity to accommodate 160 SIM cards and a large quantity of SIM cards in the single room apartment.

SIM box fraud is a set up in which some fraudsters in Ghana connive with partners abroad to route international calls through the internet using voice over internet protocol (VOIP) and terminate those calls through a local phone number in Ghana to make it appear as if the call is a local call. The caller is often not aware of the activities of these cyber fraudsters whose activities result in the loss of revenue to the state.

**Source: www.ghanabusinessnews.com*

In another case, an anti fraud collaboration between the National Communications Authority (NCA), all telecom service providers in the country and the Criminal Investigations Department (CID) of the Ghana Police Service has led to the arrest of a six-members SIM Box syndicate operating between Oregon in the United States of America and Accra, Ghana.

Members of the syndicate had according to investigators, carried out the illegal termination of telephone calls in the last seven months during which, it deprived telecom operators and the state revenue in the region of GH¢7.2 million about US $ 4.5m.

A SIM box server capable of holding at least two thousand SIM cards belonging to a Nigerian National resident in Ghana was retrieved. A total of nine SIM box machines were retrieved from the suspects which were loaded with SIM cards belonging to an operator.

**Source: News – www.nca.org*

IRSF Fraud Busted in Nepal

IRSF, said to be one of the most critical telecommunication crimes, was tracked in Nepal for the first time, with two Pakistani nationals found using the gateway of a local operator to make calls from SIM cards issued with UK-based companies. The duo had been making telephone calls to Estonia, Latvia and Lithuania, the countries with high telecommunication tariffs. In the past couple of weeks, they had made calls for over 13,333 minutes.

In roaming service, the home network, has to pay a certain amount of revenue to the visited network based on the talk-time. The visited network then shares the revenue with the carrier service providers (CSP) to whom it passes the call. The CSP again passes the call to another such service providers to route the call to the destination country, according to telecom companies. The longer the talk-time, the higher the revenue that the CSPs and the destination network get.

**Source: www.thehimalayantimes.com*

Base Station Equipped Telecom Fraud Gangs Busted in China

Chinese police, in a recent cross-provincial raid, have busted 72 gangs involved in a new type of telecom fraud facilitated by illicit base stations. During the raid, the police captured 217 criminal suspects, destroyed four dens in which illicit base stations were produced and confiscated 96 sets of such equipment.

In these cases, gangsters used forged base stations to intercept SIM card information and send duping or commercial text messages to these intercepted phone numbers.

A base station, a piece of wireless transmitting equipment usually composed of a main unit and a laptop, can acquire SIM card information from mobile phones within a certain range. Duping or commercial text messages can then be sent to the intercepted numbers.

Duping messages are usually randomly sent to a great number of users, attempting to fool them to transfer money to a designated bank account. Or swindlers may pretend to be someone whose mobile phone-related information they have intercepted, and cheat their families and friends out of money.

By using illicit base stations, instead of SIM cards, to send duping messages, the swindlers also saved costs and dodged telecom operators' monitoring.

**Source: www.english.peopledaily.com, August 2013*

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