

Subex Telecom Fraud Alerts

January 2011

Romanian police bust €11m telecom fraud

Police in Romania claim to have busted a telecom call charge fraud amounting to more than €11m (\$14.6 million) of losses. The police arrested 42 suspected members of the gang, reckoned to be led by two Romanians.

The fraudsters hacked into the corporate phone systems of Western firms before making calls to premium rate numbers under their control and earning a commission in the process. The fraud victims include corporates in the US, UK, South Africa, Italy and Romania.

Operators are advised to regularly review the security of their corporate customer's phone systems to prevent such incidents of fraud.

**Source: The Register, Dec 2010*

Fraud Watch Exercise busts 59180 fraudulent mobile phone lines

A total of 59180 fraudulent mobile phone lines were detected and reported by the Ministry of Telecommunication Fraud Watch Exercise, in Ghana. According to the Ministry, an average 5,918 fraudulent lines were discovered and immediately disconnected every two hours between March and December 9, 2010.

These lines were used for fraudulent international call termination. The fraudsters would re-route (i.e. bypass) international calls through local SIM cards and make them appear on people's mobile phones as though they were local calls. This way, the fraudsters managed to siphon money from international calls actually meant for telecom operators and the state.

The government task force arrested fraudsters in June, November and December. It is suspected that the fraudsters colluded with some domestic telecom operators and other collaborators abroad to commit the crime. The three main networks belonging to major telecom operators in Ghana had fraudulent lines. In addition to the detection of the fraudulent numbers, the task force also seized equipment used. This included one Cisco router 1800 series SN: FHK1243F4BM, eight GSM Gateways, one SVC port, three FE port, one COM port and one VGA port. It was noted that each of the GSM Gateways processed eight cards, and each card could hold four SIM cards.

This seized equipment was helpful to the task force in determining, how the fraudsters had bought large quantities of SIM cards and scratch cards and how they were registered by the telecom operators.

The Ministry also said that it would be able to identify who the fraudsters were buying international traffic from, in order to alert the telecom operators and prevent them from sending Ghana traffic through the unauthorized routes.

**Source: Ghana News, Dec 2010*

Thieves disrupt 400 South African traffic lights by stealing their mobile phone SIM cards

In Johannesburg, some 400 South African traffic lights were rendered out of action after thieves stole the mobile phone SIM cards contained within them. The thieves then used these SIM cards to make calls, running up bills amounting to thousands of dollars.

According to the Johannesburg Road Agency (JRA), the cards were fitted in order to notify them when the traffic lights were faulty. JRA is investigating a possibility of an inside job as only those lights containing the cards were targeted. According to the agency, no one apart from JRA and the supplier knew which of the intersections employed the system and hence believe that a syndicate with inside knowledge is behind the thefts.

JRA has blocked all the stolen SIM cards so that they cannot be used to make further calls, but this happened after the thieves had run up large bills. One of the cards had a bill of 30,000 rand (\$4,500; £2,900) and there were about 150 SIM card bills. As well as these direct financial losses, repairing the faulty traffic lights will cost the JRA about 9m rand (\$1.3m; £870,000).

**Source: BBC News, Jan 2011*

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