

# Subex Telecom Fraud Alerts

August 2010

## Top brass involved in telecom fraud

Top executives of a well known private telecom operator in India have been charged with telecom fraud. The fraudsters masked international calls as local ones to evade payment of fee to the exchequer. According to the CBI, the fraudsters would mask incoming international calls as local ones through one of the three gateways -- Chennai, Kolkata and Mumbai. The calls would be put on the Public System Telephone Network as local. This was done with the help of specially designed software and accomplices in the state-owned telecom behemoth. This was allegedly done to avoid paying Access Deficit Charges (ADC). Private telecom operators have to pay the state-owned telecom behemoth Rs 4 on every incoming international call as ADC. This fraud resulted in a loss to the government and its PSUs to the tune of several crores of rupees.

Source: Express India, Aug2010

## Premium rate SMS Trojan detected again

A new premium-rate SMS Trojan named as Trojan-SMS.AndroidOS.FakePlayer.a has been spotted doing the rounds. It is masked as a movie player. The malicious program penetrates smart phones running Android in the guise of a harmless media player application. Users are prompted to install a file of just over 13 KB with the standard Android extension .APK. Once installed on the phone, the Trojan silently begins sending SMSs to premium rate numbers without the owner's knowledge or consent, resulting in money passing from a user's account to that of the cybercriminals. As of now it has been affecting devices only in Russia.

Operators are advised to be wary of such Trojans and advise their customers accordingly.

Source: CFCA, Aug 2010

## Balance Transfer schemes hit with large value frauds

A middle-east operator was recently hit by high value frauds through its balance transfer services. The operator launched a service where postpaid subscribers could transfer a certain amount to prepaid accounts so as to use the balance for regular mobile services. Fraudsters exploited flaws in prepaid to postpaid migration process controls and as a result the operator lost about 1 million USD in a month through postpaid nonpayment / write-offs. The loss was further exacerbated by the fraudsters who availed high-valued smart phones through EMIs as part of the contract but never paid for them.

The modus operandi was as follows:

- Fraudsters buy prepaid SIMs in bulk and use it for a few days
- Operator provides a service for prepaid to postpaid migration, fraudsters abuse this service and do bulk migration with minimal / false documentation
- Fraudsters sell top-ups to genuine prepaid subscribers at lower rates through their postpaid accounts. Top-ups are usually in small denominations and high frequency to avoid high value checks.
- The bills do not get paid for 2-3 months running up huge amounts before being disconnected by the operator. Additionally, phone costs are also not recovered.

## Essex General Practitioner set ups website to help victims of telecommunications fraud

A General Practitioner in Essex, UK has set up his own scam-busting website after being targeted in a telecommunications scam. The GP set up the website in the hope of fighting back against the various short-lived companies that operate in the area. Practices have been stung with bills of over £20,000 after being told they must upgrade their phone systems in order for them to work when local lines 'go digital'. The fraudsters claimed to be calling on behalf of a well known telecom giant in UK and informed the victims that initially the upgrades would be free. Victims would then be pursued by large companies who would take on the debt or lease for the equipment. The upgrades were sold by a company which has since been liquidated and reappeared under different names.

Operators should warn their customers to be wary of such scams.

Source: Healthcarerepublic, Aug 2010

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