Subex Telecom Fraud Alerts

May 2010

Malicious worm used for IRSF fraud

A malicious worm used for IRSF fraud was detected on the number +3396003964. On investigation, it was found that a virus installed on the phone is used to send SMS to this number. Around 0.5million SMSs were sent to this number. These SMSs were sent as local SMSs and were also active while on roaming, resulting in roaming rates being charged to the subscriber. The following preventative measures can help subscribers from falling prey to these types of frauds.

- Refrain from phone sharing or swapping. Do not let others use your phone without your discretion.
- Refrain from memory card sharing or swapping. Do not let others use your memory card without your discretion.
- Avoid downloading free mobile applications from suspicious WAP sites or from Internet.
- Do not install a pirated version of the anti-theft software Guardian v 0.95

Operators are advised to inform customers about these kinds of malware and preventative measures.

Ghana government losing $5.8million monthly due to fraudulent international calls termination

The Ghana government reported losing $5.8 million in March 2010 alone, due to fraudulent termination of international calls coming into Ghana. It was found that international calls were being terminated on mobile phones as local cell phone numbers. So far 3000 landlines and mobile phones have identified as being used for the fraud. The perpetrators use a device called SIM Box or GSM gateway to hack into mobile networks and route international calls to local mobile or landline numbers within the same network the call was to terminate, then re-route the call from that local number to the number the international call was originally intended for. The fraudsters make it look like the call originated and terminated within the same network so the payment of international interconnectivity fee is avoided and government loses in terms of taxes on such calls.

International calls to Ghana usually terminate on the receiver's phone as either 'Private Number', 'Unknown' or '000000', but lately some international calls terminate with local cell phone numbers, as if they are local calls. It is also suspected that some employees of telecom operators are conniving with external contractors to commit this fraud.

The government of Ghana is implementing a uniform tariff of $0.19 per minute on all in-bound international calls to safeguard government's revenue earnings of about $60 million a year from in-bound international calls.

Telecom operators in Ghana are also losing money to fraud, as initially customers were not compelled to register their simcards and hence some would use their phone numbers for fraudulent practices and get away with it. To curb the losses, the operators have made registrations of landline numbers and mobile phone simcards compulsory, else they would be blocked.

**Source: Ghana News Agency, May 2010*

Phishing – the latest technique used for telecom fraud

In phishing, essentially the phisher sends out an email that gets the user to respond to it by providing one of the following:

- User ID and password
- Information required to set up online access to the account

Once the phishers have on-line access, they perform one of the following activities:

- Set up a second line (wireline) and then set international call forwarding on the additional line to go to an international location (often an IRSF number). The second line is activated, but never used by the real subscriber, as they don't actually know that there's a second line on their landline.
- Order a new mobile phone after changing the account address or by specifying a ship to address. That way, they receive the handset.
- Set international call forwarding on an already existing line and start calling the existing line. This is often done for international call forwarding to IRSF numbers.

In a case found in India, phishing was used to gain access into a subscriber's account and order a new handset. The innocent subscriber got an SMS from the operator stating that his "handset change request has been processed". When a telecom customer loses his handset, he typically places such a request with the service provider. While the number could remain the same, calls would be directed to the SIM on the new phone .After this, the SIM in the victim's phone became invalid and he could make no more calls, except to the telecom company's customer care number. All the while, his number remained valid but was being used by whoever had perpetrated this fraudulent change. The moment this occurred, the victim notified its operator. Also the very next day, the victim found his bank account drained.

Investigations are on but operators are advised to alert their customers to not fall prey to these kinds of phishing attacks.

**Source: The Hindu Business Line, April 2010*

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