Subex Telecom Fraud Alerts

April - June 2011

Unlocked smart meter SIM card racks up loss of $200,000

A 33 year old disability pensioner was sentenced to 18 months imprisonment and ordered to repay nearly $200,000 by Hobart's Supreme Court. The fraudster stole the SIM card from the energy meter. Since the SIM card was unlocked it could be used in smartphones and 3G modems. The SIM card was used to download movies, surf the net and social networking sites, presumably also check email, as well as make phone calls, all of which were being billed to energy meter provider.

The telecom operator noticed that the bill for less than four month's usage grew to nearly $200,000. This prompted the operator to find out what happened to the stolen SIM card and thus helped them nab the fraudster. This incident obviously proved to be a wakeup call for the energy company and telecom operator who promptly locked its smart meter SIM cards.

This episode is an example of how the fraudsters could misuse smart meter SIM cards in the absence of proper security. Operators are advised to take precautions for their smart meter SIM cards so that such frauds can be avoided.

**Source: ITWire, May 2011*

International call forwarding fraud forces South African telecom operator to cut services

A South African telecom operator is in the process of disabling international roaming, calling and forwarding functionality on all customers SIM cards in a proactive effort to protect them from fraudsters who steal SIM cards and use them to run up massive international phone bills. The operator is removing the above mentioned services, from all customers that have not used these functionalities over the past 12 month period by notifying them via SMS. If customers want to reactivate these services they would be required to formally request the operator.

This is in response to the growing occurrence of international call forwarding fraud where fraudsters use stolen SIM cards to place international collect calls against the subscriber's account. Unsuspecting cellphone subscribers fall prey to this scam and are saddled with bills of thousands of Rands.

The telecom operator has alerted all its customers via sms to be aware of international call forwarding fraud and to ensure that all lost and stolen SIM cards are reported immediately.

In an effort to curb the fraud, the telecom operator has advised all its customers to take the following precautions:

- Report the loss or theft of a voice or data SIM card immediately
- Contact the operator if the SIM card has been tampered with in any way
- Deactivate International Calling and Roaming on the phone when not travelling
- Remove any call forwarding activated on the phone unless absolutely necessary
- Ensure that the call forwarding option on the SIM card isn't activated without consent
- Activate a SIM card PIN on the cell phone under security settings
- Ensure that the phone is locked when not in use
- Always check the monthly billing activities on your account
- When requesting a new SIM card to be activated, ensure that the international roaming/ calling and forwarding functionality is deactivated at the same time

**Source: Leadership, May 2011*

New Android Trojan AdSMS targets users in China

A new Android Trojan, the AdSMS, has been targeting users in Mainland China via a malicious link spammed SMS. The infected SMS fools the users into downloading a supposed Android security update that is actually an SMS distributing Trojans.

The SMS is made to look like it's from a valid telecom operator and the download link deliberately spoofs a domain name associated with the operator. Once users click on the link, the malware is downloaded. Most users tend to overlook the permissions they grant to Android applications and that's the profile of users the trojan is targeting.

Once installed, AdSMS doesn't add an icon for itself on the application menu; it just runs silently in the background. The Trojan then steals phone details, connects to a remote site to download more files. It also has the capacity to read, write and send SMS messages, much like the preceding Trojan:AndroidOS/Fakeplayer.A. The Trojan sends messages to a premium rate number and thus enriches virus distributors and their partners in crime, at the expense of infected users.

Operators are advised to inform their customers to take necessary precautions against such Trojans.

**Source: The Register, INFOSEC INDIA, June 2011*

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