Subex Telecom Fraud Alerts

December 2010

Digital telephony emerges as a new form for phishing

A new phishing scam was detected in Africa, in which fraudsters were using fake caller ID numbers to solicit personal information and money. The fake caller ids (caller id spoofing) enabled the culprits to convince the victims that they are representatives of a legitimate bank or credit card company. Once convinced, the fraudsters found it easy to obtain personal and financial information from the victim.

Fraudsters were able to succeed because very few people would think that the name and number appearing on their caller id may be false.

This kind of spoofing facility is provided by suspect VOIP providers who want to make a quick buck.

Operators are advised to educate their customers regarding such scams. Given below are few tips which can be used to educate customers

- The information displayed on the caller id may not always be accurate as it can be easily spoofed
- Do not give out personal or financial information to anyone unless you are sure about the identity of the person
- In case of doubt, call up the main number of your bank or Credit Card Company and confirm, instead of talking to the person on the phone.

**Source: Telecom Regulation, Nov'10*

More than 1 million cell phones in China hit by malware

Hackers in China hijacked more than 1 million cell phones with zombie virus which automatically sends text messages. This attack cost the users a combined 2 million Yuan ($300,000) per day.

The zombie virus which is hidden in a fake antivirus application sends the phone user's SIM card information to hackers, who in turn remotely control the phone to send URL links. The dispatched text invariably contains links to other viruses and cell phone users inadvertently click on the link and get their phones infected. Other text messages are automatically dispatched to premium-rate phone numbers, generating profits for the attackers while draining subscribers' accounts.

This is the second such act to occur this year. The previous one used the Troj/SymbSms-A malware which infected Symbian phones and was targeted at Russian subscribers.

According to a recent analysis of mobile device security trends, operators should expect an increase in such malicious viruses which target cell phones for profit.

**Source: InformationWeek, Nov'10*

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