Subex Telecom Fraud Alerts

January-March 2012

Premium Rate internal fraud hits operator in Indonesia

A senior executive belonging to a telecom operator in Indonesia is being questioned by the police on suspicions of participating in a premium rate SMS scam. This scam is said to have resulted in criminals getting away with $1.3million per month.

Police claim that the executive conspired with a mobile content provider to spam customers with premium rate text messages without their consent. Almost 2 million customers are said to have been affected by the scam. The police have also expanded their investigation into other network operators to find out if more customers have been affected. The senior executive has been suspended post the police questioning.

Operators are advised to implement strict internal policies as internal fraud seems to be growing steadily.

**Source: cellular-news, March 2012*

Premium Rate Phone Regulator in UK hits out at malware racking up premium rate charges

Premium rate regulator says it might disregard evidence of consumer consent from paid-for mobile applications if those apps turn out to contain malicious code.

As per the PhonepayPlus Code of Practice, premium-rate service (PRS) providers are prohibited from charging consumers' without their consent. Certain PRS providers must hold evidence that consent has been obtained. This rule is important as the malware targeting innocent customers is on the rise. The malware contained in mobile apps sends text messages containing keywords that result in consumers being charged for using PRS "shortcodes" without their knowledge or consent. Also in certain cases, malware is known to dial PRS numbers without consumers' consent. It is also known to illicitly accesses consumer contact list such as phone numbers of social networking contacts, which is then relayed to others to populate unauthorized marketing lists.

The new guidance issued by the regulator, advices PRS providers to obtain robust consent from customers before charging , since if malicious software is found to be present in the app, then any proof of consent would not be enough.

**Source: The Register, March 2012*

French authorities arrest 2 people over Euro 100,000 Android malware scam

French authorities arrested 2 men on suspicion of developing mobile malware which ended up on 2000 Android devices. These two fraudsters were arrested in Bobigny. One of them was the brain and the other was the technician for this scam. According to the police, the fraudsters conned users out of an average of Euro 20 to Euro 30 and racked up almost Euro 100,000.

The malware used in this instance was the Foncy Trojan, which spreads via file-hosting website 'SuiConFo.apk'. After installation, it appeared on the main menu of Android smartphones and send four SMS messages to premium-rate numbers. The four SMS messages were sent using the sendTextMessage method. Through this method, the Trojan sends an SMS message to a French cell-phone number with the text taken from a reply from a premium-rate number. This helps the cyber criminals find out how many premium SMS messages have been sent.

The Foncy Trojan has also been appearing recently in the form of a fake EA Sports game, exploiting a vulnerability to root the phone, sending SMS messages and silently joining an IRC channel to receive further commands from remote hackers.

Operators are advised to educate their customers regarding such Trojans and issue instructions for safeguarding their mobile devices to prevent such scams.

**Source: ITNetworks, Feb 2012*

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