subex
powering the ROC

Telecom Fraud Alerts

January-March 2016

Advertising Fraud Will Cost $7.2 Billion in 2016

Digital advertising revenue surged 19% to $27.5 billion in 2015, a landmark high for the industry, according to the Interactive Advertising Bureau. However, the increase in revenues has also attracted an increasing amount of fraud in the industry. According to a report by ANA (Association of National Advertisers), $7.2 billion is expected to be lost globally as a result of nonhuman traffic in 2016, and that the problem is just as pervasive as it was last year. Automated software programs known as bots, the primary vehicle for ad fraud, infected a range of advertisers, which reported that bots represented from 3% to 37% of the impressions for their ads. That's up from last year, where bot percentages ranged from 2% to 22%, the study said.

To better combat ad fraud, the study's authors recommended a better understanding of the programmatic supply chain. Language on non-human traffic should be included in terms and conditions when making ad buys, they added, suggesting that buyers should consider writing into insertion orders that they will not pay for fraudulent impressions. In a scenario wherein a large number of telecom operators are investing heavily on advertising, using stringent techniques to keep fraudsters at bay is the way forward.

**Source:* http://www.adageindia.in/

Fraudsters Launder $19.6 Million in PBX Hacking Scam

Fraudsters in South East Asia admitted laundering over $19.6 million, in support of a massive international computer hacking and telecommunications fraud scheme. According to court files, hackers first compromised businesses' PBX systems -- the computer systems that run internal telephone systems of the businesses. They would then identify unused extensions, reprogram them so they could be used to make long distance phone calls charged back to the victim business. The hacked phones were then used to make calls to phony premium telephone numbers -- essentially recordings made to sound like the voicemail messages or prompts of adult chats, psychic hotlines, and other services that charge per-minute.

The hackers laundered and transmitted money to approximately 650 individuals involved in the scheme over four years.

**Source:* http://www.darkreading.com

11 People Including 5 Telecom Employees Arrested in Bangladesh for Mobile Banking Fraud

Eleven fraudsters, five of them employees of a leading telecom operator, have been arrested for siphoning off funds from customer accounts by cloning mobile banking data. The issue came to lignt when the owner of a mobile banking outlet had complained that on Jan 31 someone had withdrawn Tk 24,500 and Tk 5,000 in two fake transactions using his mobile number. The owner then informed the bank about these fraudulent transactions and later came to know that someone had cloned his SIM card and was using it for cash withdrawal from his account.

Five employees of the telecom operator, working in its customer care cell were arrested after meticulous investigations proved their involvement in passing on mobile banking details to the fraudsters. This gang used the customer care staff to clone the SIM of agents and customers to siphon off money from customer accounts.

**Source:* http://bdnews24.com/

Ghana: SIM Box Fraud - Government Lost USD 900,000

Ghana is believed to have lost a little over $900,000 in just five months according to communications and security experts due the activities of SIM box operators in the country in collaboration with their foreign counterparts. According to experts, these loses could have been avoided if the nation had instituted functional regulatory measures to check the telecom industry.

SIM box operators allow calls from international destinations to be diverted to Ghana as local calls and at a cheaper rate charging international carriers 19 cents per minute of call as against the local interconnect charge of four pesewas thereby depriving the nation of revenue.

**Source:* http://allafrica.com/

For all previous fraud alerts click on the following link: http://www.subex.com/fraud-alerts To follow active discussions on various topics log on to or subscribe to: Telecom Fraud Professional Group LinkedIn, @ SubexTweets and Subex Blog.

Write to us at info@subex.com to know more about dealing with telecom frauds.