Telecom Fraud Alerts

April-June 2016

The terrifying new mobile phone scam that leaves you with a £300 bill for calls you never made

Thousands of mobile customers are falling victim to a terrifying new scam that leaves them with a giant bill for a phone call they insist they never made. Some victims are being hit with charges of more than £300 for mystery calls lasting up to 12 hours. But they only find out about the calls when they get an itemised bill or receive a text message saying their phone is being blocked due to high usage.

In every case seen by Money Mail, involving Vodafone, EE and O2 customers, the scam begins with the customer receiving a call from an unfamiliar number that starts with 0845 or 0843. The customer never answers the call typically lasts just a fraction of a second and it's recorded on their mobile handset as a missed call. Weeks later, the bewildered victim receives a bill showing they called that number back and owe a huge sum. In almost all the cases we have seen, the return call supposedly made by the customer is shown to have lasted between three and 12 hours.

Yet the victims have no recollection at all of calling the number on their bill. Many say they didn't even see the missed call, let alone ring back. Others say they did notice a strange number pop up on their phone, but just ignored it. Customers who ask their mobile supplier to waive the charges are being fobbed off and told to pay up. All of the cases seen by Money Mail so far have involved phone giant Vodafone, which insists the problem is not its fault. EE and O2 customers have also come forward to say they have been handed refunds, but the companies are yet to comment.

**Source: http://www.thisismoney.co.uk*

Simboxing Ghanaian Real Estate Boss Gets 2 Years in Prison

Dr Alexander Tweneboah, the former CEO of the Ghana Real Estate Developers Association (GREDA) has been given a two year prison sentence and a GHS24,000 (USD6,200) fine for illegally terminating international calls using a simbox with a 64-slot SIM server.

Commsrisk has reported previously about the ways Ghanaians are encouraged to treat simbox fraud like a low-risk business activity. The arrest and imprisonment of a relatively well-connected figure like Tweneboah should make Ghanaians wary of the consequences of simbox crime.

**Source: http://commsrisk.com*

Ghana National Auditor Claims to Have Cut 300K Simbox Lines

The new centralized Ghanaian simbox test regime claims to have already identified and disconnected 300,000 lines used by fraudsters. Afriwave Telecom Corporate Affairs Director Donald Gwira said 'Working with the National Communications Authority (NCA) and the law enforcement agencies in Ghana, we will be stepping up our strategy of Test Call Generation, which is what we are currently doing to include Geo-location solution, which will expose the location of the equipment and their operators for confiscation and prosecution so that SIM-Boxing is reduced to levels where it is no longer profitable for the fraudsters to stay in business'.

**Source: http://commsrisk.com*

Abu Dhabi Commercial Bank warns over 'sim card fraud'

Fraudsters are gaining access to UAE residents' sim cards and obtaining important information such as bank notifications and the ability to make and receive phone calls, according to a report.

Abu Dhabi Commercial Bank sent an email to customers advising them of the scam, which has been termed 'sim swap fraud'.

It sees fraudsters obtain personal information about someone's identify, forge official documents, then approach the telecoms provider to request a new sim card.

When the card arrives, the telco will deactivate the old one, enabling the fraudster to insert the new sim into his own phone and receive a host of information via text message, such as money transfer requests and bank statements, and PIN codes used for security purposes.

**Source: http://www.arabianbusiness.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 our linkedin group: https://www.linkedin.com/groups/2285100/profile, twitter: https://twitter.com/SubexTweets and blog http://www.subex.com/blog/

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