TOP 10 - TELECOM FRAUDS

Telecom fraud is not a new crime, but it has emerged into a big business. There are two major types of telecoms fraud; subscription fraud and toll fraud. In Subscription fraud the criminals make use of carrier business process compromise (BPC) to pose as a legitimate customer and gain access. In Toll fraud, which is more damaging, criminals exploit how money moves within the global telecom network.

These top 10 Telecom Frauds funnel billions every year from carrier, or subscriber accounts directly into the pockets of criminals. Unfortunately, Network operators incur the cost of fraud themselves, because traditional law enforcement channels take too long to investigate and prosecute. It is up to the Network Operators to protect themselves. It is a daunting job and luckily there is help.

The faster the fraud is identified, the greater the potential of Network protection and Revenue Assurance. The FAST (Fraud Analysis & Security Technologies) Fraud management solutions, exclusively from OpTech, protect Operators from these top 10 and many, many more…

1. INTERNATIONAL REVENUE SHARE FRAUD (IRSF)

Criminals use hacked phones, stolen SIM cards, and compromised corporate PBXs to direct calls to their own, or leased lines with billing of incoming connections. The unsuspecting business pays a high rate for these calls and may be faced with huge phone bills for calls they do not recognize. They only realize they have been duped when they have to pay the bill, which goes directly into the pockets of the criminals. Another IRSF attack method is a drop-call that forces the victim to call back a premium number. In addition, the victim network also has to pay the international carriers for the traffic generated by its network towards the destination network.

2. INTERCONNECT ABUSE

Interconnect bypass fraud is a fraud scheme where the criminal exploits the difference between high international interconnect rates and low retail rates. For example, as voice traffic is routed from its origin to its destination, passing from carrier to carrier, each carrier charges for receiving traffic and, at the same time, pays to route traffic on to the next carrier in the chain. Corrupt carriers and criminals find opportunities to manipulate traffic routes for profit, by taking advantage of the difference between low and high termination rates.

3. ROAMING FRAUD

Roaming fraud is a special case where criminals steal the victim's cell phone, or SIM card. Often, the victim is traveling, and the criminals use them from overseas markets to call international revenue share numbers. It takes a minimum of 3 - 4 hours for call records to get back to the home network in the form of NRTRDE files (Near Real Time Roaming Data Exchange) for analysis and decision making. During that time, criminals can generate huge amounts of traffic.

4. PBX HACKING

PBX hacking criminals scour the Internet looking for vulnerabilities in a company's PBX (private branch exchange/telephone system). Once inside, the criminals make international calls, which are charged to the unsuspecting PBX owner. As long as they are connected, illegal revenue can be generated; so many PBX attacks are launched at night, or on weekends.

5. SIM BOX ABUSE

In SIM BOX abuse criminals illegally exploit the difference between low cost local calls and international calls. They use low-cost prepaid SIM cards to bypass international interconnect fees, so they only pay for the local call. In many cases, free minutes are also included with the SIM card and they pay nothing at all. The criminals make huge profits based on the difference between these local and international tariffs.

6. SPOOFING

CLI Spoofing (Calling Line Identity) is used in common fraud scenarios like robot-calls, one-ring scams, and phishing. Criminals falsify the information transmitted to the victim's caller ID (the A-number) to disguise their identity, making it appear the call is coming from a trusted brand or company. The criminals then use scripts to steal valuable personal information, without the victim even being aware that anything has happened.

7. SUBSCRIPTION FRAUD

Subscription fraud is when criminals use a false or stolen identity to obtain mobile devices with no intention to pay. Obtaining a false identity is easy for identity fraud experts. They have a huge pool of stolen identities to choose from, either acquired via phishing techniques, or bought on the dark web. Criminals love high-end smartphones they can acquire through contracts with little to no upfront costs and then resell on second-hand markets for lucrative profits. In the meantime, all calls they make are at the cost of the network.

8. ACCOUNT TAKEOVER

An account takeover (ATO) is when a criminal steals information to take control of a victim's account. Mobile subscribers are extremely vulnerable, because many platforms rely on a one-time PIN sent via text, or phone call to authenticate their customers. Criminals only need to find the PIN, and sign in in their place. This kind of Telecom ATO is also known as "SIM swapping," which allows the criminal to send and receive calls and texts as if they were the customer. This also makes it easy for them to bypass multi-factor authentication and get into other accounts owned by the victim.

9. SMISHING/SMS PHISHING

With Smishing (a combination of SMS and phishing), criminals rely on consumers to unknowingly reveal access to their data, or to download malware. Smishing is one of the easiest ways for hackers to steal user data, because the victim is literally handing the hacker all of their information by clicking on a link. And since people are increasingly glued to their phones, it's no surprise that the number of Smishing attacks has skyrocketed in recent years. Criminals also benefit from the Network Operators, because international text messages can be routed to their destination in a variety of ways, where each route is calculated differently. Grey routes are prevalent where the mobile operator has an imbalance between international and local termination charges for SMS.

10. SIGNALING ATTACKS

Signaling attacks are widespread due to vulnerabilities of SS7 and newer Diameter protocols. If the home network does not provide adequate protection, attackers can gain access to the SS7/Diameter interconnection network and launch attacks against any mobile network, or subscriber in the world. Attacks on core network infrastructures can affect millions of subscribers. As soon as criminals have access to the system they can track the location of SIM cards, customers, modify their profiles, or find out the IMSI. These criminal attacks range from privacy breaches, to fraud, to denial of service, to loss of customer confidence, or worse.

Criminals have discovered many other ways of stealing from Network Operators. View the Fraud and Revenue Assurance page for a full listing of Telecom Fraud schemes protected by FAST. Use the followiig link:

https://www.optech-informatik.de/top-10-telecom-frauds/