"EL NEGOCIO DEL FRAUDE EN LA INDUSTRIA DE LAS TELECOMUNICACIONES"

Introducción

Todas las empresas de la Industria de las Telecomunicaciones y Tecnología son vulnerables y están expuestas al fraude

El fraude en la industria de las telecomunicaciones ha seguido 2 diferentes líneas.

- La primera, el fraude en redes fijas ha estado inserta en las empresas por décadas.

- La segunda, el fraude en redes inalámbricas ha empezado ha ser mejor entendida y manejada recientemente.

Evolución del Fraude en Redes fijas

Por muchos años, hasta ahora, los estafadores simplemente se enganchan a la red y adjuntan un dispositivo que les permite obtener el servicio. El servicio es facturado como cualquier servicio legítimo al propietario de la línea.

Los estafadores comprendieron que las cabinas telefónicas funcionaban cuando las monedas eran insertadas y así se idearon un modo de hacer sus llamadas sin gastar el dinero. Era fácil inventar una técnica simple que permita depositar temporalmente monedas en el teléfono y luego recuperar las monedas después de que la llamada era colgada. Los estafadores ataban una cuerda o un cable a una moneda, depositaban la moneda, y después que la llamada era colgada daban un tirón y la moneda era recuperada. Gradualmente, los teléfonos que utilizaban monedas fueron diseñados de tal manera que tenían caminos de recolección de monedas más complicados o de dirección única, impidiendo que esto sucediera.

El servicio de prepago al principio fue pensado como la solución al fraude de la suscripción, por lo que el operador no se preocupó realmente quién era el cliente, o a donde fueron hechas las llamadas. Sin embargo, se han desarrollado métodos para cometer el fraude en estos servicios.

El fraude de suscripción es utilizado por personas que no tienen el suficiente conocimiento técnico para incursionar en fraude de otro tipo, y funciona tanto en redes alámbricas como inalámbricas.

Con la explosión de nuevos proveedores de servicio y revendedores de larga distancia, han aparecido proveedores de servicio ilegítimos y los revendedores de llamadas encuentran métodos de añadir sus gastos a una factura telefónica de suscriptores reales.

En un principio los operadores no se preocupaban por el fraude, pero ahora gradualmente comienzan a hacer caso y encontrar el medio de descubrir el fraude

Tipos de Fraude

- **Fraude Técnico (alámbrico e inalámbrico).** El Fraude Técnico es definido como el acceso no deseado o no autorizado a la red telefónica. El Fraude técnico en el presente, ha empezado a ser la preocupación más significativa para redes análogas inalámbricas, y representa un riesgo para redes digitales. Hubo numerosos casos de clonación descubiertos en redes análogas. Al principio se descubre este tipo de fraude cuando un suscriptor llama para quejarse de su alta cuenta. La única manera para prevenir el fraude de red inalámbrico es la autenticación de equipo.

  - **Fraude clip-on.** Los dispositivos son conectados a un teléfono o la línea para simular llamadas legítimas (son hechas a veces paralelamente con una llamada normal), o frustrar la capacidad que tienen las redes de facturar una llamada en curso.

  - **Cajas de Colores.** Los dispositivos llamados " cajas azules " "y cajas negras" proveen funciones diferentes, y pueden ser usados en el lugar mas cómodo para el estafador. Una Caja Azul es un dispositivo que permite a un estafador hacer llamadas simulando las señales, tonos, o los pulsos que serían hechos por una llamada legítima. La llamada es aprobada y el propietario de la línea es facturado. Una caja negra permite que un estafador frustre una llamada entrante a la red convenciéndola que no fue contestada. Una llamada entrante es planificada en un tiempo de juego. El receptor de la llamada contesta el teléfono, pero rápidamente cuelga otra vez dentro del ½ segundo (después, entre ½ y 1 segundo, la red envía el mensaje Llamada Contestada al switch y empieza la facturación). Con la caja negra conectada, el teléfono puede contestar otra vez (dentro del ½ segundo) y la conversación empieza. Los estafadores pueden hablar mientras ellos quieren ya que la red no tiene la pista de la llamada (porque la red piensa que la llamada no fue contestada). Estas técnicas se usan frecuentemente en las llamadas 3-way especialmente los que tienen el feature call forwarding.

  - **Fraude de Cabina telefónica.** Uno de los trucos más viejos es el fraude para no pagar en las cabinas telefónicas, se produce al unir a la moneda una cuerda o cable, y dar un tirón a la moneda después de que el teléfono ha registrado el depósito y ha permitido que se haga la llamada. En el mundo de hoy, aquel truco ha sido complementado con un nuevo juego de esquemas. Los dispositivos pueden ser conectados al teléfono para simular el encaje de la moneda usando sonidos. La cabina telefónica entonces provee al estafador la capacidad de hacer las llamadas que desee. Cuando la red requiere monedas adicionales

para seguir la llamada, se repite el proceso. Un tercer truco es aprovechar las puertas traseras en ciertos teléfonos, y entrar con un código para poder realizar la llamada.

- **Recarga Fraudulenta en el servicio prepagado.** El servicio prepago es sujeto de abuso cuando los minutos/unidades adicionales pueden ser añadidos de manera automatizada. Cuando se emplea tarjetas de prepago robadas o tarjetas de crédito robadas para rellenar el saldo (esta técnica última es en realidad el fraude de tarjeta de crédito).

- **Evitar la reducción del saldo en una llamada cursada.** Algunos handset inalámbricos tienen el medio para poder violar su seguridad, este método impide que se deduzca el saldo de una llamada en curso. Estas son situaciones no muy conocidas por los estafadores. Otra manera de estafa consiste en colocar una película delgada (como la cinta adhesiva) sobre el dispositivo magnético de una tarjeta prepago. La película delgada permite al handset leer el saldo cursado de la tarjeta, pero degrada la capacidad para la operación de escribir. Cuando esto pasa, el nuevo saldo (mientras la llamada cursa esta siendo deducida) no puede ser escrito a la tira magnética de la tarjeta, así se conserva el viejo saldo). Esto es una cuestión entre teléfono - sistemas, y no sistemas sobre la central de conmutación.

- **Robo o pérdidas de tarjetas de prepago.** El robo de tarjetas prepago cuando se encuentran en el paso entre los distribuidores y la venta representan una exposición significativa al fraude a los proveedores de servicio, tanto inalámbricos como fijos. Esta exposición puede ser reducida al mínimo incorporando procedimientos de inventario cuidadosos y respuesta rápida. Por ejemplo añadiendo números de serie de tarjeta robados/perdidos a una lista negra. El sistema entonces debería rechazar cualquier tarjeta de prepago que ha sido puesta en la lista negra

- **Antes de la validación para llamar.** Los estafadores crearon un teléfono con un MIN correspondiente a una gama de operadores con números de teléfono válidos. Se realizó también la creación de ESN falsos, lo que permitió el acceso inicial a la red para la primera llamada. Sólo después de que la primera llamada era completada, se detectaba que era un suscriptor inválido, por lo que la combinación MIN/ESN era puesta en una “Lista de Números Malos” para comprobar futuras llamadas fraudulentas. Los estafadores conocieron de este sistema por lo que usaron una combinación diferente MIN/ESN cada vez que se llamaba.

- **Después de la validación para llamar.** Usando la tecnología más sofisticada, los estafadores comenzaron a interceptar señales de los teléfonos cuando ellos enviaban el MIN Y ESN a la red para el registro. Interceptando estas

combinaciones válidas MIN/ESN, los estafadores fueron capaces de programar a los teléfonos con estas combinaciones, creando reproducciones que harían que la red les concediera el acceso. Las llamadas de estos teléfonos reproducidos por lo general causaban al legítimo suscriptor una gran cuenta. Se introduce un sistema de detección de fraude, este sistema buscaba llamadas del mismo teléfono en diferentes zonas geográficas, pero esto ocasionó que los estafadores se vuelvan más sofisticados, usaron teléfonos mágicos (para extender las llamadas fraudulentas alrededor de muchas COMBINACIONES válidas MIN/ESN), reduciendo la probabilidad de detección.

- **Cloning inalámbrico.** Los Números de identificación válidos Móviles (MIN´s) y Números de serie Electrónicos (ESN´s) son obtenidos sobre la red. Estas combinaciones válidas MIN/ESN pueden ser adquiridos de varias maneras:

    - Cuando la red no esta cifrada (encriptada, protegida), Las combinaciones de MIN/ESN y/o las contraseñas son obtenidas sobre la red de esta manera se tiene acceso a canales para la transmisión de esta información.

    - Los estafadores usan teléfonos tumbling para encontrar números válidos de ESN/MIN sobre la red.

- **Autenticación y Redes Digitales.** Muchos esfuerzos han sido realizados por la industria para autenticar el equipo. Sin embargo, la carencia de verificación tanto de la identidad como de los antecedentes crediticios de los suscriptores antes de la concesión del acceso a la red ha conducido repentinamente al fraude de la suscripción. El fraude de la suscripción es fácil desde una perspectiva tecnológica, ya que la mayor parte de operadores, tratan de aumentar rápidamente el tamaño de su base de suscriptores, literalmente invitan a estafadores a su red. El desafío hoy para prevenir a portadores de fraude inalámbricos debe ser, seguir autenticando el equipo (teléfonos) y realizar la validación del individuo. Cuando el Cloning disminuye, aumenta el fraude en la suscripción.

- **Teléfonos Mágicos.** Esto en una extensión del Cloning en la que un teléfono celular puede almacenar y presentar, a la red, numerosas combinaciones válidas MIN/ESN. El teléfono entonces puede presentar una combinación diferente válida con cada llamada subsiguiente realizada. Estos teléfonos son mucho más difíciles de descubrir debido a que la misma combinación se usa pocas veces, y es muy difícil de relacionar " un teléfono mágico " con las combinaciones de MIN/ESN usadas. Con la clonación los suscriptores válidos están siendo muy afectados, debido a que el teléfono mágico abarca gran número de suscriptores. La utilización de técnicas de detección de cloning unidos con el conocer el perfil

del suscriptor y técnicas de detección de umbrales permiten reducir al mínimo esta amenaza.

- **Clonación digital.** La clonación en redes digitales inalámbricas (GSM, CDMA TDMA, etc.) ha sido reportado sólo en casos aislados El método de clonación digital implica el compromiso tanto de la A-key como de MIN/IMSI para una SIM o microteléfono, con esta información, se duplica la SIM o microteléfono y se produce un clone. Como la información está " sobre el aire " igual que en las redes análogas, se utiliza un escáner en este caso digital para clonación. Por suerte los Escáneres digitales son caros y así no son usados en abundancia. Esto podría cambiar si el costo del escáner disminuye con el tiempo.

- **Abuso de features.** Un ejemplo de este abuso es el call forwarding en llamadas internacionales. En este ejemplo un individuo llama a un teléfono móvil y el teléfono móvil será entonces usado para hacer una llamada a un tercero. el tercero es a menudo un destino internacional. Aquí un teléfono será puesto para tener todas las call-forwarding internacionales, de manera fraudulenta. A menudo los teléfonos que están implicados con la clonación o el fraude de la suscripción son los objetivos de este tipo de abuso. Para reducir la exposición a este tipo de fraude, muchos operadores desactivan la opción de call forwarding internacional o alternativamente inician la supervisión de códigos de destino sospechosos. Cuando el abuso es por la llamada de 3 vías, la solución de bloquear la llamada internacional de tres vías podría tener un impacto negativo significativo sobre la base de suscriptor.

- **Tumbling.** Es una asignación arbitraria de ID MÓVIL y presenta este número aleatorio a la red. La red entonces proporciona el servicio a la unidad sin realizar la primera verificación para la validez de ID MÓVIL. Este mecanismo era muy común en cualquier parte donde la validación de prellamada no fuera realizada. Ahora la mayor parte de operadoras inalámbricas emplean la validación de prellamada para todas las redes, por lo que la detección de tumbling no tiene que ser puesta en práctica . El fraude en estos números de suscriptor válidos será descubierto usando otros mecanismos. Si un teléfono tumbling encuentra un ID de Mòvil válido , el teléfono se convierte en clone y es descubierto como tal. Una variación de tumbling es en cambio presentar ID Roamer Móvil a la red. Esto está basado suponiendo que algunas redes, que no pueden validar un roamer, proporcionen el servicio hasta que la validación pueda ser establecida. Todo lo que se requiere es que el ID Móvil presentado este dentro de una gama conocida de IDS Móvil para el roaming.

- **Desconexión Intencional.** Esto puede ser un problema para un portador que no toma en cuenta las llamadas caídas. Una llamada caída es una llamada completada que dejó la red antes de ser colgada (desconexión anormal). Algunos portadores no facturarán las llamadas caídas, por motivos de

satisfacción de cliente, sobre todo si hay problemas con la cobertura de la celda y la calidad de servicio. En estos casos, hay un riesgo que un suscriptor hará una llamada (más a menudo una llamada internacional) y después de mucho tiempo de conversación se irá hacia una zona donde conocen que no se tiene buen servicio, la llamada se cae y esta no es facturada.

- **Fraude de PBX.** Este tipo de fraude es a menudo cometido contra los propietarios de un PBX. Estos servicios privados (normalmente se tiene en corporaciones) proporcionan muchas funciones útiles para la gente que usa sus servicios, como voicemail, asistentes automatizados, etc. Lamentablemente, estas características del PBX a menudo son abusados por extraños que los usan para obtener una señal de marcar (al exterior). Una vez que la señal de marcar es obtenida, un estafador puede colocar cualquier tipo de llamada, y el costo es para el propietario PBX.

- **Fraude de Suscripción.** El fraude de suscripción es la presentación inexacta de información para fraudulentamente obtener un contrato de servicio, o de otra manera la no realización de las obligaciones de aquel contrato. El Fraude de suscripción es un riesgo significativo para todas las redes, incluyendo redes inalámbricas digitales donde otros tipos de fraude de red son más difíciles de cometer. La mejor forma de prevenir el fraude de suscripción es validar al individuo antes de brindar el servicio.

- **Fraude Interno.** El fraude es cometido cuando un individuo en el interior de la empresa ayuda a otros en la obtención de información, o en el equipo que permitirá a una persona tener el acceso a la red u obtener el servicio. A continuación se menciona algunos indicadores de este tipo de fraude: Distribución de MINs y ESNS, o Llaves de autenticación Creación de suscriptores no facturados (teléfonos fantasmas) Abuso de cuentas de prueba o de emergencia. El dar features adicionales que no fueron pagados por el suscriptor. Handset de telèfonos que son "perdidos" o extraviados. Borrar pruebas o encubrimiento de fraude

- **Fraude en el Distribuidor.** Muchos suscriptores son aceptados y aprobados sin la verificación apropiada de identidad o información suficiente. El distribuidor no puede ser culpado de tal acción ya que a menudo son pagados basados sólo sobre el número de activaciones y no sobre la calidad de la activación. Si un suscriptor no paga sus cuentas no es problema del distribuidor sino del operador. Otros ejemplos más serios de fraude de distribuidor implican el cambio de documentación del contrato después de que el nuevo suscriptor dejó la oficina del distribuidor. Por ejemplo cuando un posible comprador está inseguro de seguir con el servicio, y un distribuidor concedió un plan de tarifa o promoción para engatusar al aspirante y cerrar el contrato. Después de que el aspirante firmó una solicitud exacta y se marchó, el distribuidor cambió la solicitud para hacer que la persona aparezca como idónea para la tarifa o la promoción. Otra manera cada vez mayormente popular para aumentar las comisiones del distribuidor es activar a personas inexistentes, o

aún activar a la gente quien ha fallecido, etc. Estos nuevos suscriptores nunca pagarán sus cuentas, y también nunca harán llamadas. Después de un período de delincuencia, estos suscriptores simplemente serán desactivados y el operador pensará que no se hizo ningún daño (ya que no había ningún tráfico impagado). Sin embargo, el distribuidor consiguió su comisión. El Fraude de Distribuidor puede ser controlado solicitando a los distribuidores que verifiquen la información proporcionada sobre las solicitudes y realizando las revisiones regulares de la calidad de los suscriptores certificados o activado por el distribuidor. Además, los incentivos o desalientos pueden ser implementados para recompensar la exactitud en suscriptores buenos, y castigar la inexactitud o el alto número de clientes fraudulentos.

- **Fraude en Tarjetas de Llamadas.** Uno de los fraudes mas conocidos en líneas fijas (de larga distancia o internacional) son el empleo no autorizado del número de calling card de un cliente. La tarjeta sí es robada, o el número de la calling card es adquirido. Estos números son robados por individuos que quieren usar los números ellos mismos, o por las personas que revenderán el número. El riesgo consiste en que una vez que un número de calling card es robado, puede ser revendido a las empresas que lo revenderán otra vez. Dentro de unos minutos, un número de tarjeta robado puede estar en las manos de numerosas personas por todo el mundo y gastos inválidos que ascienden a grandes sumas del dinero comenzarán a acumularse inmediatamente. Las técnicas para robar el número de calling card son varias unas de las cuales pueden ser:

    - Observando sobre el hombro de alguien el número de tarjeta ingresado sobre un teclado numérico telefónico

    - La utilización de una cámara de vídeo con un fuerte zoom para registrar los números ingresados por las personas.

    - Usando un micrófono remoto para registrar los tonos que generan los números.

- **Fraude en Handsets. Este tipo de fraude incorpora:**

    - Reciclar handset robados.

    - Reventa de handset

    - Venta de handset falsificados.

  Cuando disponemos, de los archivos de lista negra de handsets robados y estos son introducidos a la red el sistema de detección de fraude genera alarmas entonces el handset es encontrado. Aunque las pérdidas directas de handsets

robados no son una parte significativa de las pérdidas de fraude de un operador, los handsets robados tarde o temprano terminarán por ser usados sobre la red, y la mayor parte de dueños de handsets robados probablemente están implicados en otros tipos de fraude y/o otras actividades ilegales.

- **Fraude Social Ingenieríl.** Es cuando un estafador es capaz de convencer al personal de una organización de revelar la información sensible requerida para cometer el fraude, o es en realidad capaz de conseguir a un individuo para realizar un acto específico para que ellos mismos cometan el fraude. Muchas veces la victima no conoce que se está cometiendo el fraude. Por ejemplo el estafador llama por teléfono haciéndose pasar por el Gerente de Seguridad Corporativo (usando el nombre de la persona real) y realiza la petición para la información sensible. Como el estafador mencionó el nombre familiar de alguien en una alta posición, la víctima asume que la petición es legítima y proporciona los datos. La mejor protección contra este tipo de fraude es el educar al personal a los peligros de este tipo de estafa, y comunicar procedimientos estrictos para la liberación de información.

- **Fraude Amigable.** Es cuando un suscriptor demanda que las llamadas que le fueron facturadas no fueron hechas por él, con la esperanza que el operador quitará las llamadas en disputa de su cuenta. Si el operador es incapaz de determinar que ellos realmente hicieron las llamadas, entonces a veces el operador quitará estas llamadas de su cuenta para promover las buenas relaciones con los clientes. Actualmente, el fraude amistoso no es un factor principal en ningún operador cuando se compara con otros tipos de fraude, pero esto realmente representa un síntoma de debilidad en la credibilidad de un operador.

Blancos potenciales de fraude.

- Empresas de telecomunicaciones (Tanto con redes alámbricas e inalámbricas están expuestas al fraude)
- Otras empresas que tienen canales de telecomunicación (distribuidores)
- Organismos estatales
- Empresas
- Personas naturales

Como prepararse para el fraude.

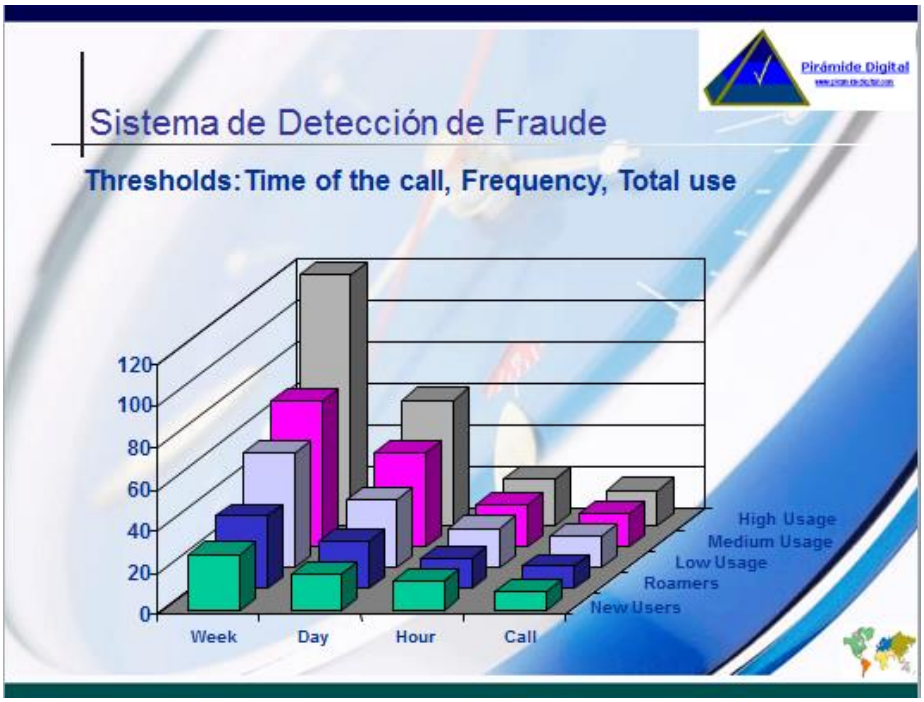
Un proveedor de servicio de comunicaciones esta listo para evitar el fraude, cuando ha tomado medidas en tres dimensiones:

- **Personal**: es la gente en la organización equipada con la conciencia apropiada y entrenada para ayudar en el manejo del fraude.
- **Infraestructura:** Obtenga instrumentos y recursos suficientes para permitir a la organización prevenir, detectar y disuadir el fraude.
- **Procedimientos:** es la política y procedimientos del operador que contribuyen a la prevención, la detección, y la fuerza de disuasión de fraude

Que herramientas tecnológicas existen para evitar el Fraude.

Un proveedor de servicio de comunicaciones esta listo para evitar el fraude, cuando ha tomado medidas en tres dimensiones:

- **Prevención de Fraude.**
  - Sistemas de Autenticación
- **Detección**
  - Sistemas de control de patrones y definición de umbrales



CONCLUSIONES

- La naturaleza de fraude es encontrar y explotar el eslabón más débil dentro de una organización.

- Como los operadores ponen en práctica nuevos métodos de prevenir el fraude en estos puntos débiles, el actor del fraude cambiará para encontrar otra debilidad y creará nuevos métodos de cometer el fraude. por consiguiente el fraude constantemente cambia dentro de una organización.

- El fraude en la suscripción representa el riesgo más grande al operador. Los motivos primarios para el incremento en el fraude de suscripción son la facilidad de cometerlo y el precio bajo de hacerlo.

- En el fraude social ingenieríl, el acceso de una persona interna a información sensible sobre el procedimiento, datos de cliente, etc., por desconocimiento debe ser controlado.

- Finalmente, mientras no se cuente con el respaldo legal necesario, en vano se invierten recursos y esfuerzos en el control del fraude, pues los mismos actores que hoy son detectados y suspendidos sus servicios, después del debido proceso, mañana operarán de nuevo bajo un nombre diferente y algunas cuadras más allá.

Bibliografía

- TELECOM MANAGEMENT NETWORKS. Telia - Ericsson (2000).

- COMPAQ TELECOM FRAUD MANAGEMENT SYSTEMS (2000).

- http://www.elmayorportaldegerencia.com

AUTOR:

Pablo G Páez Post-PhD
.:. CEO
pablo_paez@piramidedigital.com
Cel. + (593) 991 699 699
skype: ppaezec

www.piramidedigital.com
www.elmayorportaldegerencia.com