Guía para el Consumidor

Fraude con Teléfonos Celulares

Se define como fraude con teléfono celular al uso no autorizado, alteración o manipulación de un teléfono celular o sus servicios. Entre los tipos de fraude con teléfonos celulares se incluyen el intercambio o clonación de tarjetas SIM y la estafa de suscriptor.

¿En qué consiste la estafa de intercambio o transferencia de tarjetas SIM?

Su teléfono celular podría ser la clave de ingreso para sus cuentas financieras más importantes. Los bancos, empresas y servicios de pago a menudo usan mensajes de texto para verificar su identidad cuando usted pide actualizaciones de su cuenta.

Los números telefónicos móviles pueden ser transferidos legalmente de un proveedor a otro, cuando usted cambia su servicio telefónico móvil, y también pueden ser transferidos legalmente cuando usted mejora o cambia equipos. Pero, si los estafadores disponen de suficientes datos personales suyos, podrían pedir la transferencia de su número telefónico a un equipo que ellos posean.

Cuando los estafadores inician una solicitud de transferencia, engañan a la compañía telefónica móvil que provee servicios a la víctima, haciéndole creer que la solicitud proviene del usuario de cuenta autorizado. Si tienen éxito, el número telefónico será transferido a otro equipo telefónico, controlado por el estafador.

Otra forma usada para efectuar esta estafa es hurtar físicamente la tarjeta SIM de la víctima. La tarjeta SIM es un dispositivo removible en algunos teléfonos celulares y contiene una identificación única, además de los archivos con la información personal del usuario. Entonces el estafador puede instalar y usar, la tarjeta robada, en su propio equipo móvil.

En ambos casos, el estafador puede apoderarse de los textos y llamadas de la víctima e incluso podría intentar recomponer las credenciales de acceso a los datos financieros y cuentas de medios sociales de la víctima. Si tiene éxito, el estafador podría así apoderarse del dinero existente en las cuentas bancarias de la víctima, además de vender o exigir pagos por la devolución de sus datos en los medios sociales.

Averigüe más sobre esta estafa y cómo protegerse.

¿En qué consiste el fraude de clonación de teléfono celular o de tarjeta SIM?

Todo teléfono celular debe contar con un número de serie único de fábrica (ESN) y con un número de identificación móvil (MIN). Cuando un teléfono celular es reprogramado para transmitir el ESN y el MIN pertenecientes a otro teléfono celular, se trata de un teléfono clonado. Los estafadores pueden apoderarse de las combinaciones ESN/MIN mediante el seguimiento ilegal de la transmisión de ondas de radio emitidas por los teléfonos celulares de suscriptores legítimos. Tras la clonación, tanto el teléfono celular legítimo como el fraudulento poseen la misma combinación ESN/MIN y los proveedores de servicios móviles no pueden distinguir el teléfono clonado del legítimo. Los estafadores entonces pueden efectuar llamadas, generando altos cargos que aparecerán en la cuenta telefónica del usuario legítimo y que corresponden en realidad al teléfono clonado. Alerte a su proveedor de servicios si descubre llamadas o cargos no autorizados en su cuenta telefónica.

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol

¿En qué consiste el fraude de suscriptor?

El fraude de suscriptor ocurre cuando un estafador se registra en un servicio de telefonía celular con la información de un cliente, obtenida de manera fraudulenta, o lo hace con una identificación falsa. Los delincuentes pueden obtener la identificación personal de un usuario y utilizarla para establecer una cuenta de telefonía celular a nombre de la víctima. Llegar a descubrir este fraude podría tomar tiempo. Y más tiempo aún podría demorarse la víctima en probar que no fue él o ella quien generó los cargos adeudados. Cada año, se registran millones de dólares en pérdidas debido al fraude de suscriptor.

Si usted piensa que ha sido víctima de un fraude de suscriptor:

- Contáctese con las fuerzas de orden y presente un informe a la policía. Usted también puede presentar un informe de robo de identidad ante la Comisión Federal de Comercio (*Federal Trade Commission*, FTC, por sus siglas en inglés).
- Notifique a su actual proveedor de servicios y también al proveedor de servicios de la cuenta fraudulenta.
- Presente una alerta de fraude ante una de las tres principales compañías calificadoras de crédito: Equifax, Experian o TransUnion. La que usted elija para dar la notificación compartirá su alerta con las dos restantes.

Continúe vigilando su calificación de crédito en cada una de las compañías calificadoras, por lo menos una vez al año. Considere consultar una compañía calificadora diferente, cada cuatro meses de manera gratuita, ingresando a annualcreditreport.com (en inglés).

Centro del Consumidor

Averigüe más sobre este tema y otros asuntos del consumidor, visitando el Centro del Consumidor de la FCC en www.fcc.gov/consumers (en inglés).

Formatos accesibles

Para obtener esta publicación en formato accesible -- Braille, letra grande, Word, o documento de texto o de audio -- escríbanos o llame a la dirección o teléfonos indicados abajo o envíe un correo electrónico a fcc504@fcc.gov

Última edición: 22 de enero de 2020

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 445 12th St. SW. Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · Fax: 1-866-418-0232 · www.fcc.gov/espanol