¿ QUÉ ES EL FRAUDE EN PORTABILIDAD?

SIM Swapping, *SIM Splitting* o *SIM Jacking* son los nombres más conocidos para los fraudes de Portabilidad.

¿En qué consiste?

El fraude consiste en transferir tu número de teléfono a otro operador, es decir, **portarte sin tu consentimiento**, y el objetivo no necesariamente es obtener solo tu número, si no robar tu información, claves de tus cuentas bancarias, solicitar servicios o préstamos a tu nombre.

Los delicuentes pueden obtener tu información de diferentes maneras como hackeando tu teléfono móvil o llamándote haciéndose pasar por otra persona para lograr obtener tus datos.

Con todos los datos necesarios, se pondrán en contacto con tu operador, fingirá ser tú e intentará que tu número se transfiera otro operador a través de la solicitud de portabilidad.

¿Qué pasa si los delicuentes logran la portabilidad?

Tendrán total control de tu línea telefónica y recibirán todos los mensajes que lleguen a tu línea como los códigos de aprobación que envía tu banco para cambios claves, pagos, retiros etc. También podrán acceder a a tus redes sociales y cualquier otra plataforma que requiera una autenticación complementaria utilizando los códigos que lleguen a través de los mensajes de texto.

Para disminuir este fraude por suplantación de identidad, la CRC modificó la información del mensaje de texto que se recibe en el momento de iniciar una solicitud de portabilidad.

Este mensaje de texto contiene el NIP (Número de Identificación Personal) advirtiendo que el código corresponde al cambio de operador de tu línea móvil, para que, en caso de no haber solicitado la portación, te comuniques con tu operador inmediatamente:

Su Código NIP es 12345 y es personal. Se usará para pasar su línea 3331234567 a (Nombre Operador). Si no solicitó este cambio, contacte a su proveedor de inmediato

¿CÓMO EVITAR SER VÍCTIMA DE FRAUDE EN PORTABILIDAD?

- Si recibes mensaje de texto (SMS) con remitente 88892 o 88891, en el que te informan el NIP para realizar una portabilidad y NO lo has solicitado:
  - ✓ No le informes a nadie este código.
  - ✓ Contacta a tu operador informando lo sucedido para que cancele cualquier proceso no solicitado.
  - ✓ Te recomendamos borrar el SMS para evitar que quede la información en tu teléfono móvil.
- Si recibes una llamada en la que te solicitan el NIP o información personal de tu línea, **no la entregues**, mejor contacta a tu operador y confirma la veracidad de esta llamada.
- Si evidencias que te quedaste sin servicio, es decir no entran, salen llamadas o no puedes navegar contacta de inmediato a tu operador y así validas lo que está sucediendo.

- No te confíes de SMS o correos electrónicos que te pidan que hagas algo de manera inmediata para proteger supuestamente tu cuenta o servicios.

- Presta atención a la comunicación recibida: si está incitándote a que hagas algo rápidamente como insertar el NIP, cambiar tu clave, o que tu cuenta ha sido bloqueada “da clic aquí”, no sigas estas instrucciones. Esto lo hacen los delincuentes con la intención de generar miedo e inmediatez y así lograr que caigas en una trampa, los operadores no enviamos este tipo de mensajes.

- En caso de evidenciar que has sido objeto de fraude en portabilidad y tu número fue portado, contacta de manera inmediata a tu operador para cancelar la portabilidad que no autorizaste. Ten presente que esta solicitud solo la podrás realizar **el mismo día que tu número fue portado a otro operador**. Y no olvides llamar a tu entidad bancaria, cambiar claves de tu correo y aplicaciones.

Te recordamos nuestros **Medios de Atención**:

Líneas de atención telefónica:

- Desde línea LOV : *777 opción 9
- Línea 01 8000 413788
- Línea fija Bogotá : 601 7957000

Chat en línea:

- www.lov.com.co
- Facebook: LOV Colombia

Correo electrónico:

- info.lov@lov.com.co