Guía de recomendaciones para evitar el Fraude

PORTABILIDAD NUMÉRICA FRAUDULENTA

¡Conocer cómo operan los fraudes es tu mejor defensa! ¡Infórmate, mantente alerta y actúa con precaución!

SERNAC
Servicio Nacional del Consumidor

El fraude por **portabilidad fraudulenta** y **SIM swapping** ocurre cuando un delincuente logra que el número telefónico de una persona (normalmente vinculado a sus cuentas bancarias y sistemas de autenticación) sea transferido a una nueva SIM o compañía telefónica sin su consentimiento, utilizando técnicas de suplantación de identidad.

Ambos métodos tienen el mismo objetivo: tomar control del número de teléfono de la víctima, lo que permite interceptar códigos de verificación (OTP) y mensajes sensibles, facilitando fraudes financieros.

La mayoría de los operadores móviles en Chile comenzaron a enviar un SMS con un código de autorización (CAP) de 4 dígitos que tiene una vigencia limitada (por ejemplo, 60 minutos) cuando alguien solicita la portabilidad de tu número telefónico (port-out).

Este código funciona como una doble validación para evitar portabilidades fraudulentas, ya que solo quien tenga acceso al teléfono original y al código puede autorizar el traspaso.

Si recibes ese código sin haberlo solicitado, es una alerta clara de que alguien está intentando portar tu línea sin tu consentimiento, y debes llamar inmediatamente a tu compañía telefónica para informarlo y bloquear el proceso.

¡Comparte esta información!

FRAUDE POR PORTABILIDAD NUMÉRICA FRAUDULENTA Y SIM SWAPPING

1. Recolección de datos personales de la víctima

- El delincuente recopila información clave: Nombre completo, RUT, Fecha de nacimiento, Dirección, Número telefónico actual.
- A veces, escaneo/foto de cédula de identidad (extraída por filtración, redes sociales o phishing).

2. Suplantación ante una compañía de telefonía móvil

El estafador se hace pasar por la víctima para:

- Solicitar la portabilidad numérica del número a otra compañía.
- Solicitar reposición de SIM en una sucursal (con cédula clonada o pretexto convincente).

Técnicas comunes:

- Uso de documentos de identidad falsificados.
- Argumentos de "robo del celular" o "cambio de teléfono".
- Manipulación en centros de atención que no validan adecuadamente la identidad.

3. La víctima pierde señal en su teléfono

Una vez completada la portabilidad o reposición fraudulenta:

- El chip original queda inhabilitado.
- El número es redireccionado a una SIM controlada por el delincuente.
- La víctima no se da cuenta hasta que pierde conectividad y es demasiado tarde.

4. Ataque a cuentas bancarias, billeteras y redes sociales

Con acceso al número, el estafador:

- Solicita claves temporales (OTP) enviadas por SMS o llamada.
- Recupera contraseñas en bancos, billeteras digitales, e-mails y apps.
- Ingresa a cuentas si la sesión ya estaba iniciada o se salta 2FA (autenticación en dos pasos).

🛡️Recomendaciones clave para proteger tu información

🔒 Antes del ataque:

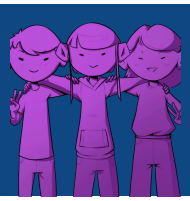
1. Activa la autenticación de dos pasos (2FA) en todas tus cuentas, pero usa apps de autenticación (ej.: Authy, Google Authenticator) en lugar de SMS.
2. Nunca compartas tu Clave Única, OTP, ni claves bancarias por teléfono, correo o redes sociales.
3. Consulta a tu compañía móvil si ofrece bloqueo preventivo de portabilidad (port-out lock) o reposición de SIM.
4. Activa un PIN o NIP permanente para cualquier gestión en la cuenta.
5. Desvincula tu número telefónico como segundo factor de autenticación en cuentas críticas si puedes usar un método más seguro. Migra tus 2FA a app autenticadora (TOTP) o llave FIDO2; evita SMS.
6. Nunca publiques número + RUT juntos.

<u>Señales de alerta</u>

- **Tu móvil pasa a “Sólo llamadas de emergencia”.**
- **Notificación de portabilidad que no solicitaste.**
- **E-mails de “cambio de contraseña” que no iniciaste.**

📲 Si se dan las señales de alerta

1. Sospecha inmediatamente si tu celular pierde red sin explicación.
2. Intenta contactar a tu compañía móvil desde otro equipo.
3. Revisa si se hizo portabilidad de tu número en el portal www.numerosportados.cl.
4. Cambia contraseñas de inmediato en tus cuentas (correo, banco, apps).
5. Llama a tu banco para bloquear preventivamente todas tus operaciones.
6. Presenta una denuncia en la PDI o Fiscalía (Cibercrimen).



¿QUÉ HACER FRENTE A UN FRAUDE?

1.AVISA Y BLOQUEA

Tu primera acción: Llama a tu banco o ingresa a la aplicación inmediatamente. Exige el bloqueo de tus tarjetas y productos para detener el fraude.

- Ten presente: ¡Cada segundo cuenta!.

2. RECLAMA

Tienes 30 días hábiles desde el aviso para hacer el reclamo formal en tu banco por las operaciones que no reconoces. Recuerda que puedes incluir operaciones realizadas hasta 60 días anteriores al aviso. Si el banco lo exige. Realiza una declaración jurada, el banco te dará el formulario que necesitas.

- ¡Ojo! Avisar para bloquear no es lo mismo que presentar el reclamo formal. ¡Debes hacer ambos!
- Recuerda: Hacer una declaración jurada no es un riesgo. Es tu herramienta más poderosa.

3. DENUNCIA

Para formalizar tu reclamo, dirígete a Carabineros, PDI o Ministerio Público y realiza la denuncia oficial del fraude. Pide un comprobante de tu denuncia. Una "constancia" no es suficiente, debe ser una denuncia formal.

- Ten en cuenta: No es un juicio en tu contra. Es tu testimonio oficial para que la investigación comience. Es el primer paso para recuperar lo que es tuyo.

Un aviso no es un reclamo:

Un **aviso** es la comunicación inmediata al emisor para bloquear el medio de pago y limitar tu responsabilidad.

Un **reclamo** es la presentación formal que inicia el procedimiento de cancelación de cargos o restitución de fondos. Sin este reclamo no se inicia la revisión de las operaciones ni los plazos legales para devolver el dinero.

¡PLAZO CRÍTICO!

Para que el banco restituya los fondos debes entregar el comprobante de tu denuncia. Tiene un plazo máximo de 30 días corridos desde que diste aviso o desde que presentaste tu declaración jurada (según sea el caso). Si no lo haces, ¡Se entenderá que te retractas!

Conoce todo sobre fraudes en www.SERNAC.cl

SERNAC
Servicio Nacional del Consumidor