



Fraudes financieros: ¿Conoces el **SIM Swapping**?

¿Qué es el SIM Swapping?

- Se trata de la **duplicación de tu tarjeta SIM** con el fin de **suplantar tu identidad** ante las Instituciones Bancarias.
- Mediante engaños se **apropian de tu número telefónico**, y **acceden a tus cuentas bancarias** con las que está asociado.



¿Cómo funciona el SIM swap?

Conoce la manera en que operan los delincuentes que realizan este tipo de fraude:

1. Manipulación para obtener la tarjeta SIM:



- Se hacen pasar por ti y solicitan un **cambio de SIM** a la compañía telefónica por **supuesto daño o pérdida**.

2. Empleo de una identificación falsa



- Recogen el chip con una **identificación falsa**, para **acceder a tu información y cuentas bancarias**.

3. Inician sesión en tus cuentas



- Usan la SIM para **recibir códigos de verificación** e **iniciar sesión** donde tienes tus recursos financieros.

4. Las consecuencias: fraudes financieros



- Obtienen información bancaria y personal que les permite **cometer fraudes mediante transacciones financieras**.

Formas de protegerte de la clonación de chips telefónicos

- Añade una **clave o PIN** de seguridad a tu SIM.
- Evita guardar **información confidencial** en la tarjeta SIM.
- Utiliza **doble factor de autenticación**.
- Revisa frecuentemente tus **movimientos bancarios**.
- Navega desde **redes privadas** y evita redes públicas.
- Desconfía de **correos, llamadas o mensajes sospechosos**.
- **No compartas tus datos** personales por internet.
- Crea contraseñas robustas y **cámbialas regularmente**.



¿Cómo reportar un número robado?



Si notas que tu **chip ha dejado de funcionar**, contacta inmediatamente a tu proveedor.



Ten a la mano tu **número IMEI** para bloquear el celular. **Marca *#06#** para obtenerlo.

Pon en práctica estas recomendaciones y actúa rápidamente si ocurre un fraude para **minimizar el daño**.

