Guía de recomendaciones para evitar el Fraude

“¡PROTEGE TU CELULAR Y TUS DATOS!”

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

SERNAC
Servicio Nacional del Consumidor

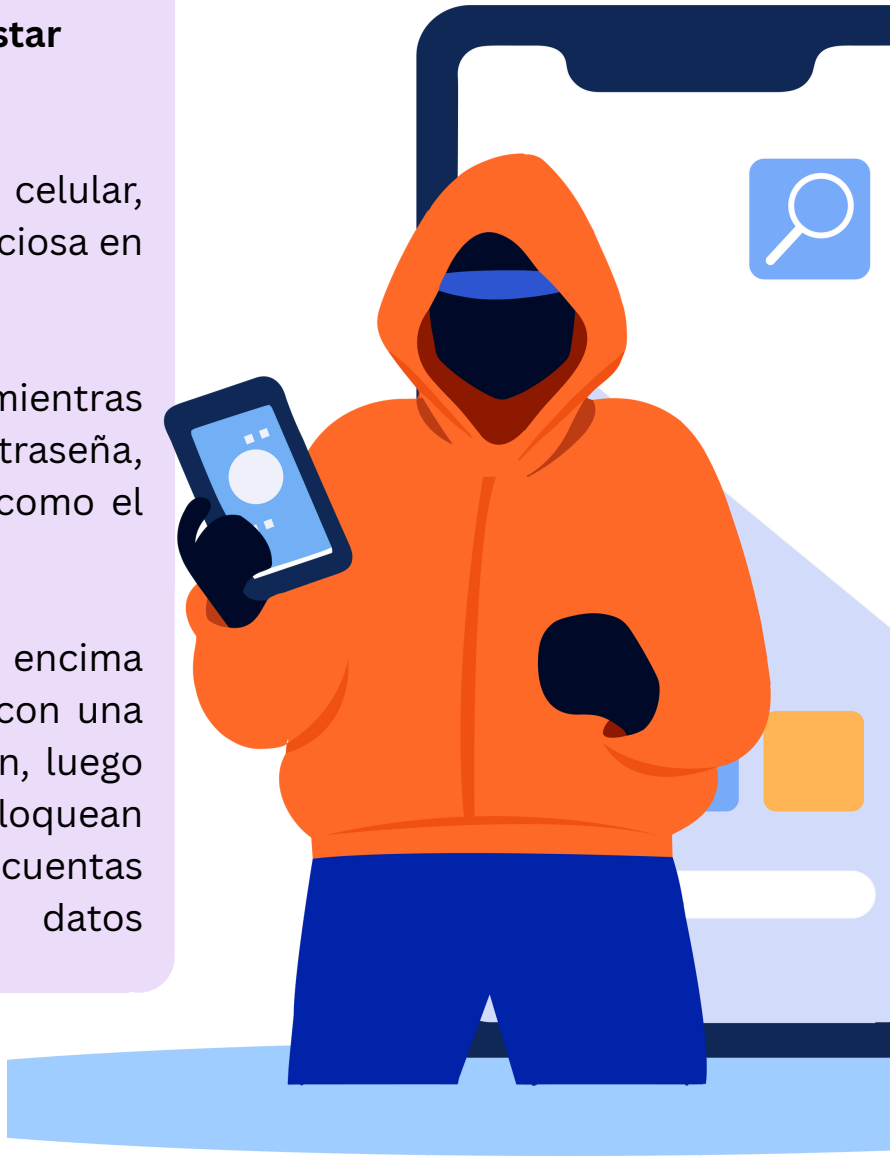
Cada día, cientos de personas pierden el acceso a sus cuentas y su dinero solo porque les robaron el celular. Los delincuentes saben exactamente qué hacer cuando tienen uno en sus manos.
¿Estás preparado para protegerte?

¿Sabías que te pueden estar vigilando sin que lo notes?

Antes de que ocurra el robo del celular, muchas veces hay una técnica silenciosa en juego: el **shoulder surfing.**

Consiste en espiar a la víctima mientras ingresa su PIN, patrón o contraseña, generalmente en lugares públicos como el metro, la micro o una fila.

Los delincuentes pueden mirar por encima del hombro o grabar el momento con una cámara oculta. Con esa información, luego roban el teléfono y lo desbloquean fácilmente para acceder a tus cuentas bancarias, redes sociales o datos personales.



¡Comparte esta información!

¿Qué buscan los delincuentes?

⚠️Los delincuentes no buscan solo el equipo físico. Su objetivo es acceder a tus datos personales y cuentas:

- **Acceso a apps bancarias o billeteras digitales**

Si el dispositivo está desbloqueado o tiene autenticación débil, el acceso a apps financieras es inmediato.
También pueden intentar resetear contraseñas mediante SMS o correo.

- **Lectura de correos y SMS**

Muchos usuarios tienen sus correos abiertos permanentemente.
El acceso a SMS permite interceptar códigos de verificación, validar cambios de contraseña, o completar fraudes tipo SIM swapping.

- **Contraseñas guardadas**

Las contraseñas suelen estar guardadas en navegadores (Chrome, Safari) o apps como Google Smart Lock o iCloud Keychain. El acceso a estos almacenes de contraseñas puede permitir tomar control de múltiples servicios.

- **Códigos 2FA (OTP) enviados por SMS o email**

Si tienen acceso al dispositivo, pueden interceptar los códigos 2FA y sortear mecanismos de seguridad. Es de los mayores riesgos del robo de celular.

- **Acceso a redes sociales y apps financieras**

WhatsApp, Instagram, Facebook, X, y otras redes suelen estar abiertas. Permiten suplantar la identidad, cometer fraudes o phishing a terceros.

- **Acceso no autorizado al ID de Google o Apple**

Muchas veces se accede fácilmente si la cuenta está abierta en el dispositivo. El atacante puede cambiar contraseñas, cerrar sesiones en otros dispositivos o activar funciones remotas.

- **Uso de fotos personales para realizar chantaje/extorsión**

Es una amenaza real (sextorsión o extorsión digital), especialmente si se encuentran imágenes íntimas o comprometedoras en el dispositivo.

🛡️Recomendaciones clave para proteger tu información

ANTES DEL ROBO (prevención):

🔒 **1. Bloquea tu equipo con biometría fuerte.** Usa PIN complejo, huella o reconocimiento facial real.

🔐 **2. Activa el bloqueo de apps sensibles.** Usa segundo factor para entrar a apps bancarias, billeteras, correos y redes sociales.

🧩 **3. No guardes claves en navegadores ni en notas del celular**. Usa un gestor de contraseñas con clave maestra o autenticación biométrica.

📴 **4. Desactiva la vista previa de mensajes en pantalla bloqueada.** Evita que puedan leer SMS con códigos desde la pantalla sin desbloquear el equipo.

📲 **5. Usa autenticación de dos pasos con apps como Google Authenticator.** No dependas solo de SMS o correo electrónico para validar accesos.

🔐 **6. Configura el bloqueo remoto (Google "Find My Device" o iCloud).** Asegúrate de poder bloquear o borrar el equipo a distancia.

🪪 **7. Ten tu IMEI anotado.** Es clave para bloquear el equipo con tu compañía telefónica.

DESPUÉS DEL ROBO (reacción inmediata):

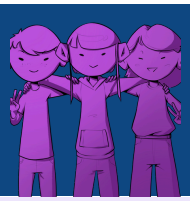
🚫 **1. Llama a tu compañía para bloquear la SIM**. Esto corta el acceso a SMS y llamadas.

📴 **2. Bloquea el equipo con herramientas remotas.** Usa "Buscar mi iPhone" o "Encontrar mi dispositivo" en Android.

🛑 **3. Cambia inmediatamente las contraseñas desde otro dispositivo.** Correo, redes sociales, banco, apps de pago.

📝 **4. Reporta el robo y el fraude** a tu institución financiera y a las entidades competentes.

🛡️ **5. Solicita el bloqueo financiero**. Evita que pidan créditos a tu nombre.



¿QUÉ HACER FRENTE A UN FRAUDE?

1.AVISA Y BLOQUEA

Tu primera acción debe ser contactar de inmediato a tu institución financiera o ingresar a su aplicación. Solicita el bloqueo urgente de tus tarjetas y productos asociados para frenar cualquier operación fraudulenta.

- Recuerda: ¡Cada segundo cuenta!

2. RECLAMA

Dispones de 30 días hábiles desde el aviso para presentar un reclamo formal ante tu institución financiera por las operaciones que no reconoces. Este reclamo puede incluir transacciones realizadas hasta 60 días corridos antes del aviso. Si la entidad lo requiere, deberás presentar una declaración jurada, para lo cual te entregarán el formulario correspondiente.

- ⚠ Importante: Avisar para bloquear productos no sustituye el reclamo formal. Ambas acciones son necesarias.
- 💡 Recuerda: Presentar una declaración jurada no implica un riesgo; por el contrario, es tu herramienta más poderosa para recuperar lo que es tuyo.

3. DENUNCIA

Para formalizar tu reclamo, debes realizar una denuncia oficial del fraude. Puedes hacerlo ante Carabineros, la PDI, el Ministerio Público o en cualquier tribunal con competencia penal (Juzgado de Garantía o Tribunal Oral en lo Penal). Solicita siempre un comprobante de la denuncia.

- ⚠ Una simple constancia no es suficiente; debe tratarse de una denuncia formal.
- Ten presente: No se trata de un juicio en tu contra, sino de tu declaración como víctima. Es el testimonio que activa la investigación y constituye el primer paso para recuperar lo que te pertenece.

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 la institución financiera pueda restituir los fondos, debes entregar el comprobante de tu denuncia formal.

El plazo máximo para hacerlo es de 30 días corridos, contados desde que diste el aviso o desde que presentaste tu declaración jurada, según corresponda.

- ⚠ Si no entregas este comprobante dentro del plazo, se entenderá que desististe del reclamo.

Conoce todo sobre fraudes en www.SERNAC.cl

SERNAC
Servicio Nacional del Consumidor