Guía de recomendaciones para evitar el Fraude

“¡NO RESPONDAS ESA LLAMADA!”

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

SERNAC
Servicio Nacional del Consumidor

Te llaman fingiendo ser del banco u otra entidad confiable. Te dicen: “Detectamos un movimiento sospechoso en tu cuenta.”

Te generan ansiedad o urgencia: “Si no actúas ahora, perderás todo tu dinero.”

Te piden verificar datos o dictar claves: “Necesito validar tu identidad con un código que recibirás.”

¡Comparte esta información!

¿QUÉ ES EL VISHING?

El vishing (llamada fraudulenta) es un tipo de estafa telefónica en la que el delincuente se hace pasar por una entidad confiable (banco, proveedor de servicios, institución pública, etc.) para engañarte y obtener tus datos personales, claves o autorizar transferencias.

EJEMPLO

El reclamante señala que recibió una llamada de un supuesto ejecutivo bancario, que habló con formalidad y conocía sus datos personales: nombre completo, su RUT, detalle sobre sus tarjetas, incluyendo montos y compras recientes que realmente había realizado. Esta información específica y precisa generó confianza en la víctima, quien creyó estar hablando con alguien legítimo.

El criminal se puede hacer pasar por un tercero de confianza

- Ejecutivo bancario
- Funcionario público
- Amigo
- Pariente
- Otros

Usan mensajes alarmantes que aluden a beneficios o supuestos incovenientes.

- Vulneración de la seguridad de la cuenta bancaria.
- Supuesto beneficio o devolución de dinero
- Actualización de datos, etc.

🚫 Nunca digites claves durante una llamada telefónica. Ninguna institución confiable te pedirá hacerlo.

Acceso a claves vía Dual-Tone Multi-Frequency (DTMF)

Algunos estafadores simulan ser ejecutivos de confianza y, durante la llamada, te piden no decir tu clave en voz alta, sino digitarla directamente en el teclado del teléfono. Esto puede parecer más seguro... ¡pero no lo es!

Cada número que pulsas emite un sonido distinto, gracias a una tecnología llamada DTMF (Multifrecuencia de doble tono). Los delincuentes graban esos sonidos y, con herramientas especiales, pueden descifrar exactamente qué números marcaste... ¡incluyendo tu clave secreta!

Modus operandi del Vishing

1.Preparación

Los delincuentes utilizan información real, obtenida mediante filtraciones o robo de datos personales, o por engaños anteriores (phishing)
Configura un sistema VoIP que falsifica el identificador de llamada (“caller-ID spoofing”).

2.Contacto Inicial

El estafador prepara un guion (“soy del banco…”) y exhibe datos legítimos del cliente para ganar credibilidad.

3.Generación de Urgencia

Comunica un problema crítico (“movimientos irregulares”, “bloqueo por fraude”) o una oportunidad (“devolución de excedentes”) y exige actuar en menos de 5 minutos.

4.Petición concreta

El estafador solicita:

- Códigos que llegan por SMS (OTP) o codigo de seguridad de la tarjeta (CVV).
- Grabación de la palabra “sí” para autorizar cargos.
- Instalar una app de “soporte remoto”.
- Transferir fondos a una “cuenta segura”.

5.Ejecución del Fraude

Con los datos/claves:

- Realiza transferencias no autorizadas
- Cambia credenciales.
- Solicita créditos a tu nombre.
- Desvía SMS (SIM swapping) para saltarse 2FA.

6.Encubrimiento y cierre

Pide no cortar la llamada “para mantener la seguridad” o envía correos/SMS falsos de confirmación. Al colgar, bloquea el número y borra señales.

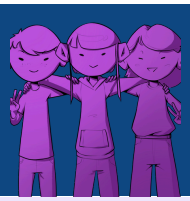
RECOMENDACIONES

Protege tu información. Nadie más puede hacerlo por ti.

🔐 *1. Nunca entregues claves, códigos ni datos personales por teléfono.*
📞 *2. Si te llaman, cuelga y verifica por canales oficiales.*
⏳ *3. No actúes bajo presión, urgencia o miedo. Están intentando manipularte.*
🧠 *4. Detente y haz una pausa mental antes de seguir instrucciones.*
🛑 *5. Desconfía si te dicen que no cortes la llamada o no hables con nadie más. Ese aislamiento es una señal clara de fraude.*
📱 *6. No confirmes códigos que tú no hayas solicitado. Si recibes un SMS o notificación con un código, y no estabas haciendo una transacción, no lo digas ni ingreses en ninguna parte.*
📵 *7.No instales aplicaciones por sugerencia telefónica. Algunos fraudes incluyen el pedido de instalar apps para “ayuda remota”. No lo hagas.*

¿CÓMO TE MANIPULAN?
¿POR QUÉ CAEMOS EN EL FRAUDE?

1. Autoridad Aparente El estafador se presenta como funcionario de banco, empresa o institución pública, usando lenguaje formal y seguro.	**¿Por qué caemos?** Tendemos a confiar y obedecer figuras de autoridad, sobre todo si parecen profesionales o conocen datos personales.
2. Urgencia y Presión de Tiempo Crean situaciones de emergencia (“hay un fraude”, “tu cuenta será bloqueada si no actúas YA”) para que respondas rápido.	**¿Por qué caemos?** La presión del tiempo bloquea nuestro pensamiento crítico, hacemos lo que nos piden para resolver el supuesto problema.
3. Miedo o Pánico Alertan sobre pérdidas, robos o fraudes inminentes.	**¿Por qué caemos?** El miedo hace que prioricemos la acción sobre la reflexión, bajando la guardia y olvidando verificar la información.
4. Peticiones Escalonadas Empiezan pidiendo datos “inofensivos” (nombre, RUT) y luego solicitan información clave (claves, códigos).	**¿Por qué caemos?** Aceptar una primera petición nos predispone a seguir colaborando, sin notar el riesgo creciente.
5. Aislamiento del Canal Piden que no cortes la llamada o que no hables con nadie más hasta terminar el proceso.	**¿Por qué caemos?** Al aislarnos, impiden que consultemos o pidamos ayuda a alguien más, y caemos solos en el engaño.
6. Refuerzo Multicanal Complementan la llamada con mensajes por SMS, WhatsApp o email para dar sensación de legitimidad.	**¿Por qué caemos?** Recibir mensajes desde varios canales parece más confiable y coordinado, lo que refuerza el engaño.
7. Reciprocidad Simulada El estafador finge estar ayudándote y espera que “correspondas” colaborando.	**¿Por qué caemos?** Sentimos la obligación de devolver el “favor” y seguimos sus instrucciones.



¿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