Guía de recomendaciones para evitar el Fraude

“¡NO CONFIES EN ESE CANAL DE RECLAMO!”

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

EJEMPLO

- ***Carolina no podía ingresar a su app bancaria un sábado por la mañana. Al no obtener respuesta por teléfono, publicó en sus Redes Sociales pidiendo ayuda.***
- ***Minutos después, recibió respuesta desde una cuenta falsa (@BancoXX_Soporte), que imitaba a su banco.***
- ***En mensaje directo, le pidieron su RUT, correo y un código SMS para “validar su identidad”.***
- ***Carolina entregó los datos pensando que era atención oficial.***
- ***Poco después, cambiaron su clave, accedieron a su cuenta y transfirieron $1.800.000. Recién al intentar ingresar de nuevo, descubrió que había sido víctima de fraude.***

HAZTE ESTAS PREGUNTAS

“**¿Te contactaron ellos... o los contactaste tú?”**
👉 Si no fuiste tú quien inició la conversación, sospecha.

“¿Estás seguro de que esa cuenta es oficial?”
🔍 Verifica el nombre, el check azul y el enlace al sitio web. No confíes solo en el logo.

“¿Te pedirían un código por mensaje directo?”
❌ Ninguna institución seria solicita claves, tokens ni datos personales por redes sociales.

“**¿Por qué tanta urgencia si es un canal de atención?”**
⚠️ La presión emocional es una señal de alerta. Respira, duda, verifica.

¡Comparte esta información!

SERNAC
Servicio Nacional del Consumidor

¿QUÉ ES EL ANGLER PHISHING?

El angler phishing es una forma de phishing en redes sociales, donde delincuentes crean perfiles falsos que suplantan a instituciones legítimas (bancos, empresas, servicios públicos) y se hacen pasar por atención al cliente para engañar a usuarios que buscan ayuda.

🎯 Su objetivo es que tú, como víctima, entregues datos personales o bancarios creyendo que estás hablando con el canal oficial.

MODUS OPERANDI DEL ANGLER PHISHING

1.Monitoreo de quejas o comentarios reales

El estafador busca usuarios que han publicado quejas, dudas o reclamos en redes sociales (Twitter/X, Facebook, Instagram, etc.) a cuentas oficiales de bancos, servicios de pago o delivery.

2. Contacto desde perfil falso

Un perfil falso, que imita el logo, nombre y estilo visual de la cuenta oficial, responde al usuario:

"Hola, lamentamos los inconvenientes. Por favor, envíanos un mensaje directo con tu número de contacto para ayudarte."

3. Conversación privada y solicitud de datos

En mensaje privado, te solicitan:

- RUT o número de cuenta
- Clave de acceso
- Código de verificación (OTP)
- Número de tarjeta
- Teléfono o correo

"Para validar tu identidad, por favor confírmanos el código que te acaba de llegar por SMS."

4. Acceso y materialización del fraude

Con esos datos, acceden a tu cuenta bancaria o app digital. Realizan transferencias, cambian contraseñas o suplantan tu identidad.

CONSECUENCIAS DEL ANGLER PHISHING

- Pérdida inmediata de dinero desde tu cuenta.
- Suplantación de identidad.
- Estafas a tus contactos desde tus redes sociales.
- Robo de datos personales y sensibles.
- Pérdida de control sobre tus cuentas bancarias o apps.
- Dificultades para demostrar que el acceso fue fraudulento si entregaste datos voluntariamente.

🛡️Recomendaciones clave para protegerte del Angler Phishing

📌 Antes de interactuar en redes sociales:

1. Verifica siempre que la cuenta sea oficial

- Revisa el check azul (verificación), la ortografía y la fecha de creación. ¿tiene ✓, número de seguidores coherente y enlace al sitio oficial?. Consulta el sitio web oficial de la institución para ver sus canales reales.

2. Nunca entregues datos personales en mensajes directos

- Ninguna empresa seria te pedirá claves, números de tarjeta ni códigos OTP por redes sociales.

3. Evita publicar públicamente tu número, RUT o problema con detalle

- Mientras más información entregues, más fácil es para un estafador personalizar el engaño.

4. Evita links acortados:

- Escribe manualmente la URL en el navegador o usa tu app ya instalada.

5. Activa 2FA robusto (app o llave FIDO) en banco y redes;

- Así, el atacante necesita algo más que tu contraseña.

6. Configura alertas de inicio de sesión y revisa sesiones activas cada semana.

7. Reporta y bloquea la cuenta sospechosa;

- Notifica al perfil oficial para que la gestione con la plataforma.

🚨 Si ya fuiste contactado:

Corta la conversación si te piden claves o códigos

- Aunque suene legítimo, ese tipo de solicitud nunca es válida por redes sociales.

Contacta tú a la entidad por su canal oficial

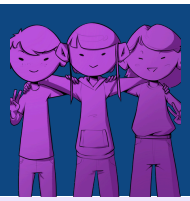
- No respondas a quien te contacta primero: tú inicia la comunicación.

Captura pantalla del perfil falso y repórtalo

- Denuncia a la plataforma (Meta, Twitter/X) y guarda evidencia para tu reclamo.

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

1. Autoridad Aparente La cuenta fraudulenta se presenta como soporte oficial, usando logos, nombres y lenguaje corporativo.	**¿Por qué caemos?** Si parece la cuenta oficial, asumimos que tiene poder y conocimiento, y seguimos sus instrucciones sin dudar.
2. Urgencia y Resolución Rápida Ofrecen soluciones inmediatas (“Resolvemos tu problema ahora mismo”, “Evita bloqueos o demoras”).	**¿Por qué caemos?** El deseo de solucionar rápido hace que no verifiquemos la autenticidad de la cuenta ni de los enlaces.
3. Empatía y Personalización Usan mensajes empáticos (“¡Lamentamos tu situación!”, “Estamos para ayudarte”, “Queremos solucionarlo contigo”).	**¿Por qué caemos?** Al sentirnos bien tratados y comprendidos, queremos colaborar y corresponder entregando datos.
4. Simulación de Comunidad Muestran que atienden a muchos usuarios, responden públicamente o etiquetan a otros clientes.	**¿Por qué caemos?** Si vemos que otras personas interactúan con esa cuenta, asumimos que es legítima y actuamos igual.
5. Refuerzo Multicanal Contactan por mensaje directo, comentarios, y a veces también por mail o WhatsApp, dando sensación de atención real y seguimiento. El QR o link puede llega justo debajo de tu queja pública.	**¿Por qué caemos?** La comunicación por diferentes vías parece más profesional, lo que refuerza la credibilidad del fraude.
6. Peticiones Escalonadas Comienzan pidiendo información “básica” (nombre, RUT, datos de contacto) y luego solicitan información crítica (claves, códigos, datos bancarios).	**¿Por qué caemos?** Empezamos ayudando y se vuelve difícil decir “no” a nuevas solicitudes.
7. Lenguaje técnico intimidante Utilizan lenguaje técnico: “Procederemos a reinicializar tu token HSM de doble capa”.	**¿Por qué caemos?** Cuando algo suena demasiado especializado, delegas la decisión al “experto”.



¿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