Guía de recomendaciones para evitar el Fraude

“¡NO RESPONDAS ESE CORREO!”

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

🔒 “Piensa • Revisa • Confirma”

🧠 **Piensa antes de hacer clic:** Si el mensaje te apura, asusta o promete algo tentador, ¡detente!. Puede ser un fraude.

👀 **Revisa los detalles con atención:** ¿El remitente es conocido? ¿La URL es legítima? No hagas clic: escribe tú mismo la dirección en el navegador.

📞 **Confirma por un canal seguro:** No respondas el mensaje. Llama, escribe o entra tú mismo a la app o sitio oficial para validar la solicitud.

¡Comparte esta información!

SERNAC
Servicio Nacional del Consumidor

¿QUÉ ES EL PHISHING?

El phishing es un tipo de fraude digital en el que los estafadores envían correos electrónicos falsos que simulan provenir de entidades legítimas (bancos, instituciones públicas, servicios digitales), con el objetivo de:

- Robar tus claves, datos personales o acceso a cuentas.
- Llevarte a sitios web falsos para que ingreses voluntariamente tu información.
- Infectar tu dispositivo con malware al hacer clic o descargar archivos adjuntos.

⚠️ La víctima participa activamente, creyendo estar frente a un correo verdadero.

SEÑALES HABITUALES DEL PHISHING

Contienen mensajes alarmantes

Simulan un premio, un beneficio o una emergencia. Te manipulan creando contextos creíbles

Se hacen pasar por instituciones legítimas

El remitente del correo tiene modificaciones o es desconocido. Buscan ganarse tu confianza.

Tienen pedidos urgentes

Te amenazan y presionan para que tomes acciones rápidas para evitar consecuencias nefastas.

Tienen una redacción inadecuada y/o faltas de ortografía

Sirven como un filtro para detectar a las personas que tienen más probabilidad de ser engañados.

Contienen enlaces o archivos infectados

Al hacer click, los enlaces te dirigen a páginas falsas y los archivos descargables pueden ser virus que roben tus datos.

Solicitan información privada

Buscan obtener tus datos personales y financieros como n° de cuentas bancarias, tarjetas y tus distintas claves de autentificación.

Posibles consecuencias del phishing

- Pérdida de dinero. Se realizan transferencias no autorizadas.
- Robo de identidad. Se abren productos o cuentas a tu nombre.
- Infección del equipo con malware.
- Estafa a tus contactos. Usan tu correo para enviar nuevos fraudes.
- Acceso a tus redes sociales, apps y cuentas bancarias.
- Dificultades para demostrar que el acceso fue fraudulento si entregaste datos voluntariamente.

🛡️Recomendaciones clave para protegerte del Phishing

🧠 **Antes de hacer clic:**

🔎 **1. Examina cuidadosamente el remitente**

- Revisa si el correo termina en un dominio legítimo.
- Sospecha de remitentes largos, con errores o direcciones extrañas.

🌐 **2. Coloca el cursor sobre los enlaces (sin hacer clic)**

- Verifica si la dirección web es confiable.
- Ejemplo: www.banco-cl.com no es www.banco.cl

🧠 **3. Desconfía de los correos que apelan a miedo, urgencia o beneficios**

- ¿Por qué te pediría tu institución financiera que ingreses un código por correo?

📂 **4. Nunca descargues archivos de remitentes desconocidos**

- Los adjuntos pueden contener virus o programas espía.

🔒 **5. Nunca ingreses datos personales tras hacer clic en un correo**

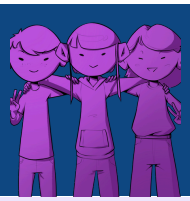
- Ninguna entidad legítima solicita contraseñas, tokens o datos sensibles por correo electrónico.

🚨 **¿Qué hacer si caíste en un correo phishing?**

1. Cambia tus contraseñas inmediatamente (correo, banco, apps) y cierra todas las sesiones.
2. Contacta a tu banco para bloquear operaciones.
3. Verifica que no hayan instalado software malicioso. Activa escaneo antivirus y restaura desde copia limpia si detecta malware.
4. Denuncia el incidente en las entidades competentes.
5. Avisa a tus contactos si tu correo fue comprometido.

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

1. Autoridad Aparente El correo parece venir de un banco, empresa, organismo oficial o jefe.	**¿Por qué caemos?** Si el mensaje "parece" legítimo y de alguien importante, tendemos a cumplir lo solicitado sin sospechar.
2. Urgencia y Presión de Tiempo Mensajes que exigen acción inmediata ("su cuenta será bloqueada hoy", "responda en menos de 24 horas").	**¿Por qué caemos?** El miedo a perder algo importante nos lleva a responder antes de analizar, saltándonos la verificación.
3. Miedo o Pánico Alertan sobre fraude, multas, pérdidas, accesos no autorizados.	**¿Por qué caemos?** El miedo nubla el juicio; queremos solucionar el "problema" cuanto antes y caemos en la trampa.
4. Atractivo o Gancho Emocional Correos que prometen premios, reembolsos o beneficios especiales.	**¿Por qué caemos?** La promesa de obtener algo nos hace bajar la guardia y actuar impulsivamente.
5. Peticiones Escalonadas Solicitan primero datos simples (nombre, correo), luego información sensible (contraseña, RUT, datos bancarios).	**¿Por qué caemos?** Una vez que comenzamos a colaborar, nos resulta más difícil decir "no" a solicitudes adicionales.
6. Simulación de entornos familiares Usan logos, colores y lenguaje idéntico al de instituciones conocidas.	**¿Por qué caemos?** Lo familiar nos relaja; bajamos las defensas y aceptamos el mensaje como auténtico.
7. Refuerzo Social / "Todos lo están haciendo" Mensajes que dicen "este mensaje es para todos los clientes", o "la mayoría ya actualizó sus datos".	**¿Por qué caemos?** Creemos que, si "todos" lo hacen, es seguro o necesario.



¿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