Guía de recomendaciones para evitar el Fraude

"¡NO REALICES ESA COMPRA!"

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

SERNAC
Servicio Nacional del Consumidor

Tipos de Fraudes que se materializan a través de las compras digitales

01

PHISHING / SMISHING

02

SITIOS WEB CLONADOS ("SPOOFED" SITES)

03

OFERTAS FANTASMAS EN REDES SOCIALES/ MARKETPLACES

04

CARD-NOT-PRESENT & "CARDING"

05

ENLACES DE SEGUIMIENTO/ DELIVERY FALSOS

06

PUBLICIDAD ENGAÑOSA Y "OFERTAS QUE NO ERAN TALES"

07

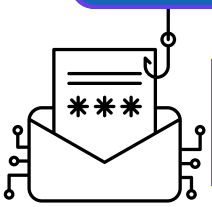
QUISHING (QR PHISHING)

08

APLICACIONES FALSAS

¡Comparte esta información!

Tipos de Fraudes que se materializan a través de las compras digitales



1.Phishing / Smishing

MODUS OPERANDI

1. Un SMS te invita a escanear un cupón o link para "20 % de descuento" en una tienda. El enlace abre una página que solicita registro y datos de tarjeta "para validar tu oferta".
2. Te llega un SMS de "Tu pedido está detenido" o "Entrega fallida" con un enlace de "reprogramación". El link conduce a un portal falsificado de la empresa de paquetería que pide datos de tarjeta o credenciales de cuenta.
3. Recibes un "recordatorio de pago" o "factura pendiente" con un PDF o enlace. El PDF te pide habilitar macros o el enlace lleva a un portal falso de pago.
4. Envían un correo que parece de una tienda conocida (logo, estilo, pie de página). Incluye un enlace a una "oferta" o tu "carrito abandonado" que redirige a un dominio muy parecido. Al "finalizar compra" tus datos de tarjeta y dirección van directo al atacante.

CONSECUENCIAS ESPERABLES

- Robo de credenciales bancarias o de billeteras digitales.
- Riesgo de suplantación de identidad, permitiendo que el estafador contrate servicios o cometa otros delitos a nombre de la víctima.

2. Sitios web clonados ("spoofed sites")

MODUS OPERANDI

1. **Clonación visual:** Copian el diseño, logos y textos de un e-commerce o banco legítimo.
2. **Dominio engañoso:** Registran URLs muy parecidas (p. ej. www.tienda-oficial.com → www.tienda-0ficial.com).
3. **Atracción de tráfico:** Usan anuncios pagados, SEO o envíos masivos de email/SMS para llevarte allí.
4. **Captura de datos**: Al "comprar", solicitan datos de tarjeta y credenciales que son enviados directamente al atacante.

CONSECUENCIAS ESPERABLES

- Pérdida de dinero por productos que nunca llegan;
- Robo de información bancaria y personal;
- Posible instalación de malware en sus dispositivos;
- Suplantación de identidad;
- Graves dificultades para reclamar o recuperar el dinero, ya que la transacción no se realizó a través de un canal oficial.

3. Ofertas fantasmas en redes sociales / Marketplaces

MODUS OPERANDI

1. **Publicación de anuncio**: Publican productos a precios muy bajos en Facebook Marketplace, Instagram o grupos de venta.
2. **Contacto privado**: Te piden chatear por WhatsApp o Messenger para "cerrar mejor el precio".
3. **Pago por adelantado**: Solicitan transferencia o pago vía móvil antes de enviar el producto.
4. **Desaparición:** Tras recibir el dinero, bloquean tu número y borran el anuncio.

CONSECUENCIAS ESPERABLES

- Pérdida del dinero transferido;
- Exposición de datos personales,
- Dificultad para rastrear al estafador,
- Al no existir una transacción respaldada por una plataforma formal, no hay posibilidad de reclamo ni restitución del dinero.

4. Card-not-present & Carding

MODUS OPERANDI

1. **Obtención de datos:** Compran datos de tarjetas robadas en foros clandestinos o mediante phishing.
2. **Validación por micro-pruebas:** Hacen pequeños cargos ("prueba de $1") para confirmar que la tarjeta está activa.
3. **Fraude masivo:** Una vez validada, procesan compras de alto valor o venden esos datos a terceros.

CONSECUENCIAS ESPERABLES

Cargos desconocidos en su tarjeta, que pueden pasar desapercibidos entre las compras legítimas.

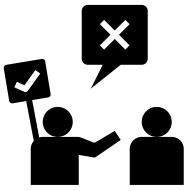
5. Enlaces de seguimiento/delivery falsos

MODUS OPERANDI

1. **Notificación de envío:** Recibes un email o SMS con un enlace para "rastrear tu pedido".
2. **Redirección a phishing**: El enlace lleva a un sitio que solicita datos de inicio de sesión o descarga malware.
3. **Explotación:** Con tu credencial, vacían cuentas asociadas o instalan spyware.

CONSECUENCIAS ESPERABLES

- Captura de credenciales bancarias o de correo.
- Descarga de malware en tu dispositivo.
- Phishing secundario a través de formularios falsos.



6. Publicidad engañosa y "ofertas que no eran tales"

MODUS OPERANDI

1. **Anuncios atractivos**: Banner o pop-ups prometen grandes descuentos o regalos.
2. **Clickbait:** Te llevan a un formulario que pide datos personales o pagos "para reservar la oferta".
3. **Revelación tardía:** Tras pagar, descubres que no existe descuento ni producto.

CONSECUENCIAS ESPERABLES

- Pago sin entrega de producto.
- Robo de datos personales y financieros.
- Infección con malvertising (descarga escondida de malware).

7. Quishing (QR phishing)

MODUS OPERANDI

1. **Código QR malicioso:** Pegatinas sobre códigos legítimos o envío digital de QR.
2. **Redirección oculta:** El QR apunta a un sitio de phishing o descarga de APK malicioso.
3. **Robo de credenciales** / **infección:** Igual que en el phishing web o malware.

CONSECUENCIAS ESPERABLES

- Captura de credenciales bancarias o de cuentas online.
- Instalación de malware o spyware en tu dispositivo.

8. Aplicaciones falsas

MODUS OPERANDI

1. **Clonación de apps:** Recrean apps populares (banco, tienda) y las suben a tiendas no oficiales o incluso a Play/App Store con nombre similar.
2. **Instalación voluntaria:** Ofrecen "funciones extra" o "versión premium gratis".
3. **Permisos excesivos:** Piden acceso a SMS, contactos o almacenamiento para robar datos o interceptar OTP.

CONSECUENCIAS ESPERABLES

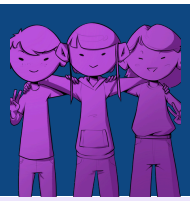
- Robo de credenciales o datos almacenados (fotos, chats).
- Acceso remoto al dispositivo.
- Transacciones no autorizadas en apps bancarias.
- Compromiso total del dispositivo si se instala malware.
- Acceso no autorizado a otras cuentas (correo, redes, apps).

Recomendaciones clave para protegerte de los fraudes

1. **Verifica siempre la URL / dominio**
   - Teclea manualmente la dirección oficial o usa marcadores.
   - Busca el candado HTTPS y revisa el certificado.
   - Evita links acortados o dominios con errores.
2. **Compra sólo en plataformas confiables**
   - Prefiere marketplaces con escrow o protección al comprador.
   - Revisa calificaciones y comentarios de otros usuarios.
   - Nunca compres desde mensajes o publicaciones sospechosas.
3. **Paga con métodos que ofrezcan protección al consumidor**
   - como WebPay o tarjetas virtuales.
   - Desconfía si te piden CVV, PIN o contraseñas por adelantado.
4. **No pagues por adelantado fuera de la plataforma**
   - Evita transferencias directas a cuentas desconocidas.
   - Usa métodos con reclamación (tarjeta de crédito, plataformas que permiten disputa).
5. **Previsualiza enlaces de seguimiento**
   - Copia y pega en el navegador en lugar de abrir directamente.
   - Comprueba que coincida con la web oficial del courier.
   - No escanees QR fuera de contexto ni instales apps desde enlaces no verificados.
6. **Descarga apps sólo de tiendas oficiales**
   - Revisa el desarrollador, número de descargas y comentarios.
   - Evita APKs de fuentes desconocidas.
7. **Actualiza y protege tu dispositivo**
   - Mantén sistema operativo y apps de seguridad al día.
   - Activa bloqueo de pantalla y cifrado.
   - Activa alertas de compra en tu tarjeta para detectar fraudes en tiempo real.
8. **Cuidado con ofertas “demasiado buenas”**
   - Si un precio está muy por debajo del mercado, investiga primero.
   - Comprueba que el vendedor exista y tenga reputación.
   - Lee con atención la letra chica de las promociones.

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

1. Heurística de urgencia / escasez El estafador incluye frases como: “¡Últimas unidades!”, “Descuento solo por hoy”, “Oferta expira en 10 minutos”.	**¿Por qué caemos?** La presión del tiempo activa decisiones impulsivas. El consumidor compra o hace clic sin verificar, por temor a perder la oportunidad. El pensamiento reflexivo se inhibe.
2. Aversión a la pérdida Usan mensajes como: “Si no lo reclamas hoy, lo pierdes”, o “Tu paquete será devuelto”.	**¿Por qué caemos?** El consumidor actúa para evitar una pérdida, no necesariamente para ganar. Esto genera ansiedad y lo lleva a actuar apresuradamente, confiando en el mensaje
3. Sesgo de optimismo Las personas creen que el fraude “le pasa a otros”, no a ellas. El delincuente lo aprovecha con mensajes como: “Este es un sitio seguro” o con diseños visualmente confiables.	**¿Por qué caemos?** El consumidor baja la guardia, subestima los riesgos y omite verificaciones básicas, como revisar la URL o la autenticidad de la cuenta.
4. Prueba social (social proof) Usan testimonios falsos, números inflados de compradores (“+10.000 vendidos”), estrellas o comentarios positivos (muchas veces automatizados o inventados).	**¿Por qué caemos?** Las personas confían en lo que parece popular. Si otros compraron, “debe ser confiable”. La decisión se basa en la imitación, no en la información objetiva.
5. Sesgo de autoridad Los estafadores copian logos, nombres y estilos visuales de bancos, instituciones, SERNAC, empresas de retail o transporte.	**¿Por qué caemos?** Si algo parece oficial, el consumidor asume que lo es. Se activa obediencia automática: entrega datos, descarga archivos o sigue instrucciones sin cuestionar.
6. Anclaje de precios Muestran un precio inflado como “precio anterior” (Ej: $99.990 tachado) y luego un “descuento especial” (Ej: $29.990).	**¿Por qué caemos?** El consumidor compara con el precio inflado, no con el valor real de mercado. Esto crea la ilusión de oportunidad o de estar ante un “tremendo ahorro”, favoreciendo compras impulsivas.



¿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