Guía de recomendaciones para evitar el Fraude

“¡NO DESCARGUES ESE ARCHIVO!”

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

Fraude a través de Malware

Todo lo que necesitas saber sobre los virus que roban tu información y tu dinero

¿Qué es un malware?

Malware es un software malicioso que se instala en tu dispositivo (computador, celular o tablet) sin tu consentimiento, con el fin de espiar, manipular o robar información sensible, muchas veces para cometer fraudes financieros, suplantación de identidad o extorsión.

SERNAC
Servicio Nacional del Consumidor

¡Comparte esta información!

Tipos de Malware más usados para cometer fraude

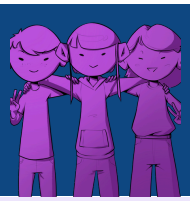
	¿Qué hace?	Modus Operandi	Consecuencias
1	**1. Keylogger (registrador de teclas)**: Graba todo lo que escribes: contraseñas, mensajes, búsquedas, claves OTP.	Se instala al descargar un archivo o app infectada. Funciona en segundo plano y registra cada pulsación.	• Robo de claves bancarias. • Suplantación de identidad. • Acceso a correos, apps y redes sociales.
2	**2. Spyware (software espía):** Monitorea tu actividad, ubicación, correos, cámaras, apps, y datos del dispositivo.	Viene camuflado en apps falsas, adjuntos infectados o actualizaciones falsas.	• Robo de datos personales o corporativos. • Vigilancia remota sin consentimiento. • Extorsión o chantaje.
3	**3. RAT (Remote Access Trojan):** Permite al atacante tomar control total de tu equipo sin que te des cuenta.	Enlace o adjunto malicioso que otorga acceso remoto completo al delincuente.	• Acceso y vaciado de cuentas bancarias. • Instalación de más malware. • Uso del dispositivo como bot para otros fraudes.
4	**4. Banking trojan:** Se enfoca en robar información de tus apps bancarias, wallets o sistemas de pago.	Simula ser una app legítima o se superpone a la app real para capturar tus credenciales al iniciar sesión.	• Transferencias no autorizadas. • Solicitud de créditos o préstamos express. • Robo de billeteras digitales.
5	**5. Ransomware:** Cifra todos tus archivos y exige un pago (rescate) para recuperarlos.	Se propaga por correos, redes públicas o sitios inseguros. Una vez instalado, bloquea el acceso a tu sistema.	• Pérdida de todos tus archivos (fotos, documentos, etc.). • Extorsión financiera. • Daño a empresas, escuelas o sistemas públicos.
6	**6. Adware con fraude oculto:** Inunda tu pantalla de anuncios, pero también puede redirigir tus pagos o capturar tu navegación.	Se instala al descargar apps de fuentes no oficiales o software gratuito con “publicidad incluida”.	• Redireccionamiento a sitios de phishing. • Pérdida de dinero por “pagos invisibles”. • Robo de sesión (cookies, tokens).

Recomendaciones clave para protegerte de los Malware

- ✅No abrir archivos o enlaces sospechosos en correos o mensajes. Desconfiar de mensajes que generan urgencia o presión para actuar rápido.
- ✅Descargar programas y apps sólo desde fuentes oficiales y confiables, como Google Play o App Store.
- ✅Nunca abras archivos adjuntos inesperados, aunque parezcan “facturas” o “comprobantes”.
- ✅No conectar dispositivos desconocidos o no verificados.
- ✅ Mantén tu sistema operativo, navegador y antivirus siempre actualizados. Usa buen antivirus y firewall.
- ✅ Revisa los permisos que tienen las apps en tu celular.
- ✅ No instales apps que pidan acceso a SMS, llamadas o pantalla sin justificación.
- ✅ Usa contraseñas fuertes y distintas. Evita usar la misma clave en varios sitios. Prefiere contraseñas largas y difíciles.
- ✅Usar autenticación de dos factores (2FA).
- ✅Evitar redes Wi-Fi públicas no seguras o usar VPN si es necesario.
- ✅Haz respaldos frecuentes de tus archivos importantes (por si enfrentas ransomware).
- ✅No uses cuentas con permisos de administrador si no es necesario. Evita que los programas maliciosos tengan control total de tu equipo.
- ✅ Protege tus cuentas con más de una barrera. Activa la autenticación en dos pasos en tus cuentas clave.
- ✅ Utiliza lectores de QR y antivirus que analicen enlaces antes de abrirlos.
- ✅Si se sospecha infección, desconectar el dispositivo de internet y consultar a un experto.

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

1. Disfraz de documentos importantes Envían correos con archivos infectados que simulan ser facturas, contratos o reportes laborales.	**¿Por qué caemos?** Asumimos que si parece profesional o laboral, es seguro. Abrimos sin verificar.
2. Ofertas atractivas o apps gratis Prometen software “premium”, juegos, cracks o apps útiles sin costo**.**	**¿Por qué caemos?** Queremos obtener beneficios sin pagar, lo que reduce nuestra desconfianza.
3. Mensajes de alerta o amenaza Dicen que tienes una multa, cuenta bloqueada o problema urgente.	**¿Por qué caemos?** El miedo nos impulsa a actuar rápido y sin pensar. Queremos evitar una pérdida.
4. Camuflaje como herramienta o extensión útil Se presentan como apps de productividad, conversores PDF, optimizadores, etc.	**¿Por qué caemos?** Si la herramienta parece útil y conocida, asumimos que es segura.
5. Falsa autoridad o remitente Simulan ser de bancos, soporte técnico, empresas públicas o colegas.	**¿Por qué caemos?** Si creemos que quien lo dice tiene poder o legitimidad, obedecemos sin dudar.
6. Petición de ayuda o favores Simulan ser un amigo o familiar que necesita algo urgente.	**¿Por qué caemos?** Queremos ayudar, y eso nos hace actuar sin verificar la autenticidad.
7. Normalización digital Justifican la instalación como “una app más que todos usan”.	**¿Por qué caemos?** Instalamos sin revisar permisos ni procedencia. La rutina domina.
8. Suplantación mediante mensajes personales Usan frases como “mira esta foto”, “urgente” o “no lo compartas” desde contactos infectados	**¿Por qué caemos?** Al venir de alguien conocido, asumimos que es legítimo.
9. Malvertising y sitios confiables infectados Insertan anuncios falsos en sitios aparentemente seguros.	**¿Por qué caemos?** Al navegar en sitios conocidos, bajamos nuestras defensas.



¿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