Guía de recomendaciones para evitar el Fraude

“¡NO ESCANEES ESE CÓDIGO QR!”

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

SERNAC
Servicio Nacional del Consumidor

¿VAS A ESCANEAR?

- Mira si el QR está intacto.
- Lee la URL completa.
- Si pide datos o pagos, detente y revisa.

Antes de escanear un QR, pregúntate: ¿Confío en el lugar y el momento, o solo sigo la rutina? El peligro puede ser invisible.

POSIBLES CONSECUENCIAS DEL FRAUDE

- Robo de claves bancarias, tarjetas o billeteras digitales.
- Instalación de malware que permite monitorear el equipo.
- Suplantación de identidad en sitios o servicios.
- Uso no autorizado de servicios (pagos, apps, suscripciones).
- Estafa a tus contactos si acceden a tus redes sociales.
- Solicitudes de crédito usando tus datos.

¡Comparte esta información!

SERNAC
Servicio Nacional del Consumidor

Fraude mediante Códigos QR (Quishing)

Quishing es una modalidad de phishing en la que los delincuentes utilizan un código QR malicioso para redirigirte a un sitio web falso o para instalar malware. Al escanearlo, tú mismo autorizas una acción riesgosa, creyendo que estás accediendo a un contenido legítimo.

⚠️ El código QR actúa como "anzuelo visual" para engañar a la víctima.

EJEMPLO

La víctima relató que llegó apurada al centro comercial un sábado por la tarde. Al estacionar su auto, notó un cartel en la máquina de pago que decía: "Pague fácil escaneando este QR con su celular – Evite filas."
Sin sospechar nada, escaneó el código con su cámara y fue redirigida a una página web que imitaba a la del operador del estacionamiento. Ingresó los datos de su tarjeta de crédito, incluyendo el CVV, para pagar $2.000.
Esa misma noche, su banco le notificó movimientos inusuales por más de $600.000. Los delincuentes habían utilizado sus datos para realizar compras internacionales. Al revisar, se dio cuenta de que el sitio al que accedió tenía una URL casi idéntica al original, pero con una letra cambiada.

MODUS OPERANDI DEL FRAUDE

1.Creación del código malicioso

El atacante genera un QR que apunta a una URL controlada por él (landing page falsa, descarga de APK malicioso, enlace de pago fraudulento).

2. Distribución o sabotaje físico

Pegado en lugares públicos: cajeros automáticos, parquímetros, menús de restaurantes, afiches en la calle, máquinas expendedoras.
Envío virtual: por correo, WhatsApp, redes sociales o SMS simulando ser ofertas, encuestas o recordatorios.

3. Engaño del usuario

Texto de acompañamiento atractivo: "¡Gana un descuento escaneando este código!", "Actualiza tu app escaneando aquí" o "Confirma tu pedido".
Diseño profesional para generar confianza: logos de bancos, empresas de delivery, instituciones estatales

4. Ejecución del ataque

Redirección web: abre un sitio que solicita credenciales (banca en línea, cuentas de e-commerce) o información personal.
Descarga de malware: inicia la descarga de una app que contiene troyano bancario o spyware.
Cobro fraudulento: activa un pago automático (por ejemplo, WAP billing) o suscripciones de costo elevado.

5. Exfiltración y explotación

Los datos ingresados quedan en manos del atacante para suplantación de identidad, vaciado de cuentas o venta en el mercado negro.
El malware instalado puede interceptar SMS, grabar keystrokes o enviar información confidencial.

🛡️Recomendaciones clave para protegerte del Quishing

🔎 **1. Revisa el contexto antes de escanear**

¿Dónde apareció el QR? ¿Fue pegado encima de otro? ¿Tiene logos falsos?. ¿Lo recibiste en un mensaje inesperado?.

🌐 **2. Verifica la dirección web (URL) antes de hacer clic**

La mayoría de los lectores de QR muestran la URL. No abras enlaces acortados, raros o que no coincidan con la institución.

🛑 **3. No ingreses claves o datos personales tras escanear**

Ninguna entidad legítima te pedirá datos privados a través de un QR.

❌ **4. Nunca instales apps desde un QR**

Instala solo desde tiendas oficiales (Google Play / App Store).

🧠 **5. Detente si algo parece "demasiado bueno" o urgente**

Promesas de premios, sorteos, ayudas sociales "express" suelen ser falsos.

📱 **6. Usa apps antivirus o lectores QR con verificación de URL**

Algunos escáneres alertan si la web es sospechosa.

🔒 **7. Evita escanear QRs en lugares públicos sin verificar**

Si ves un QR en la calle o en una pantalla, consulta primero con el personal del lugar si es oficial.

Qué hacer si escaneaste un QR fraudulento

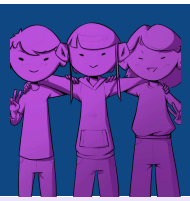
- No ingreses ningún dato.

Si ya lo hiciste:

- Cambia de inmediato tus contraseñas bancarias y de correo.
- Contacta a tu banco o entidad afectada.
- Revisa si se instaló alguna app no reconocida.
- Usa herramientas para eliminar software malicioso.
- Reporta el incidente en las entidades competentes.

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

1. Familiaridad y Comodidad Tecnológica El QR se presenta en contextos cotidianos (restaurantes, afiches, estacionamientos, campañas solidarias, etc.).	**¿Por qué caemos?** Asociamos los códigos QR con seguridad y modernidad, y los escaneamos sin sospechar porque se han vuelto parte de la vida diaria.
2. Autoridad Implícita El QR aparece junto a logos, nombres o imágenes de empresas, instituciones o marcas reconocidas.	**¿Por qué caemos?** Si el QR está junto a una marca conocida, lo validamos automáticamente y confiamos sin cuestionar.
3. Urgencia y Oportunidad Mensajes junto al QR con frases como "¡Solo por hoy!", "Paga rápido", "Oferta limitada", "Actualiza tu cuenta aquí".	**¿Por qué caemos?** La prisa por no perder un beneficio nos hace escanear el QR sin verificar su autenticidad.
4. Anonimato del Canal El QR en sí no revela a dónde llevará, ni quién lo puso, ni si fue reemplazado o alterado.	**¿Por qué caemos?** No vemos el peligro directo, así que subestimamos el riesgo y bajamos la guardia.
5.Simulación de Comunidad ("Todos lo hacen") El QR se presenta en lugares públicos o eventos, todos a tu alrededor lo usan (para menú, para pagar, para donar).	**¿Por qué caemos?** Si vemos que otros escanean, asumimos que es seguro y lo hacemos también.
6. Refuerzo Multicanal El QR llega por diferentes canales (correo, WhatsApp, afiche físico, web, etc.), reforzando la apariencia de legitimidad.	**¿Por qué caemos?** Creemos que si el mismo QR aparece en varios canales, es auténtico y no lo cuestionamos.
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