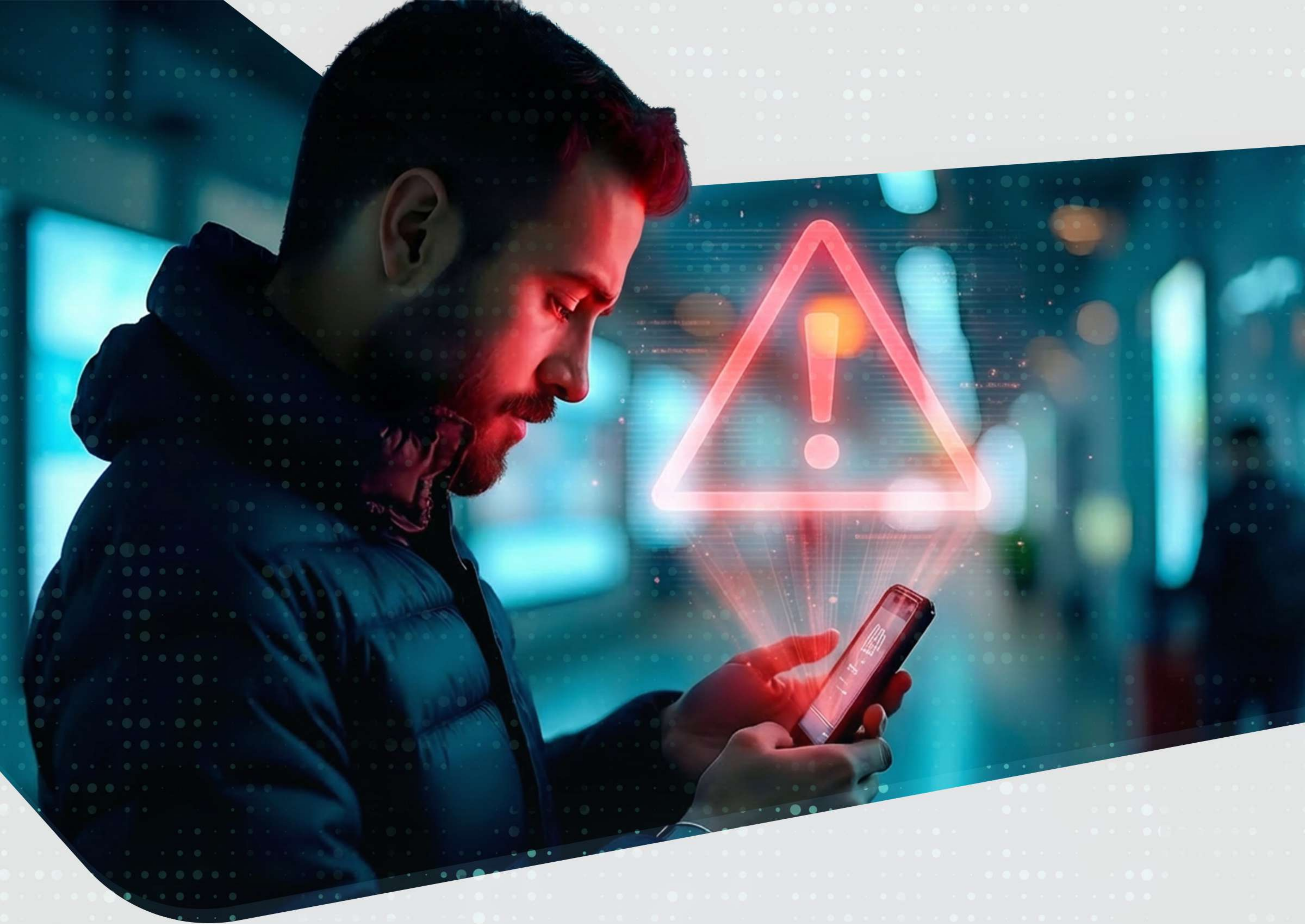


Afiliado prevenido, futuro protegido

Ponte un paso adelante del fraude





El fraude es una realidad y un temor de los colombianos

¿Sabías que el **Fondo Nacional del Ahorro** reveló en una encuesta qué tan seguros se sienten los consumidores al realizar compras o trámites en línea? Los resultados dejan un panorama preocupante: el **47 % afirma sentirse poco seguro** y otro **14 % nada seguro**. En otras palabras, el **61 % de las personas no se siente tranquilo al realizar este tipo de acciones digitales**.

A esto se suma que el **35 % de los encuestados admite no conocer términos o modalidades de fraude**, como el *phishing*, lo que evidencia la **necesidad de informar y educar a los usuarios sobre los riesgos y la prevención del fraude digital**.

Cuida tus datos, protege tu futuro

Usa contraseñas fuertes y únicas



- Combina mayúsculas, minúsculas, números y símbolos.
- Evita usar la misma contraseña para todo
- Activa siempre el doble factor de autenticación (2FA).

¡Cuidado con lo que compartes en redes sociales!



- No publiques documentos, dirección, número de identificación o datos sensibles.
- Revisa la configuración de privacidad de tus cuentas al menos cada seis meses.

Protege dispositivos y apps



- Actualízalos ya que cuando los sistemas no lo están son más vulnerables.
- Procura instalar solo apps de tiendas oficiales (Google Play, App Store, Microsoft Store, o de este tipo).

Desconfía de enlaces y archivos sospechosos



- Nunca abras archivos adjuntos que no esperabas.
- Verifica siempre la dirección del remitente.
- Ante la duda, no des clic, mejor contacta a la entidad para verificar.

Cuidado con redes Wi-Fi públicas



- No hagas compras, transacciones o ingresos a cuentas en Wi-Fi abiertas o gratuitas.

Información financiera, ultrasensible

Nunca compartas claves o códigos OTP. Ningún banco pide claves, códigos SMS o token por teléfono, correo o WhatsApp.

Activa las notificaciones de movimientos para detectar cualquier transacción no autorizada.

Accede desde la app o sitio oficial y no ingreses a través de enlaces enviados por terceros.

Revisa tus estados de cuenta regularmente y podrás detectar anomalías, lo que facilita el bloqueo de operaciones fraudulentas.



Aprende a identificar fraude o phishing

Señales de mensajes sospechosos (correo, SMS o WhatsApp)

1. Errores ortográficos.
2. Ninguna entidad legítima pide: claves, códigos OTP, token o fotos de documentos.
3. Archivos adjuntos inesperados: .zip, .exe, .html, .bat.

¿Cómo identificar llamadas fraudulentas?

1. Dicen ser del banco, pero te piden datos confidenciales, lo cual nunca debe ser así.
2. Tienen un tono de presión, miedo o promesas, por ejemplo: "su tarjeta está siendo usada ahora mismo, necesito su clave para bloquearla".
3. Imitan voces automatizadas del banco: los estafadores utilizan audios muy similares a los oficiales, si te piden datos sensibles, cuelga de inmediato.

Reconoce los enlaces falsos

1. Revisa el enlace antes de hacer clic: asegúrate que no sea un dominio extraño: ban-co.com, usualmente es banco.com. Además, que las URL no estén acortadas por desconocidos: bit.ly/.
2. Si no tiene el HTTPS, también es sospechoso.
3. Presta atención a detalles, si el sitio web luce parecido, pero no es igual (logo pixelado, diseño distinto del original o solicita datos que normalmente no pide la entidad) es un llamado de alerta.

Aplica estas estrategias para verificar si es real

1. Contacta directamente a la entidad: usa la app, consulta la web oficial, escríbela manualmente y no mediante un enlace.
2. Busca inconsistencias, por ejemplo:
 - ¿Te llaman por un trámite que no hiciste?
 - ¿Te escriben desde un correo corporativo extraño?
 - ¿El mensaje no coincide con tus movimientos recientes?
3. Siempre consulta un canal oficial: chat de la entidad, línea de atención o sitio oficial de la entidad.



Los fraudes más usuales



Phishing y smishing (mensajes falsos)

Por lo general, los delincuentes emplean correos, SMS o mensajes con:

- Falsas promociones.
- Alertas sobre entregas, bloqueos de cuentas o premios.
- Enlaces que llevan a sitios fraudulentos.



Páginas web falsas “clonadas”

Existen sitios que imitan tiendas reconocidas usando logos, colores y diseños reales, pero que dirigen el pago hacia cuentas ilegítimas.



Suplantación de identidad en bancos y comercios

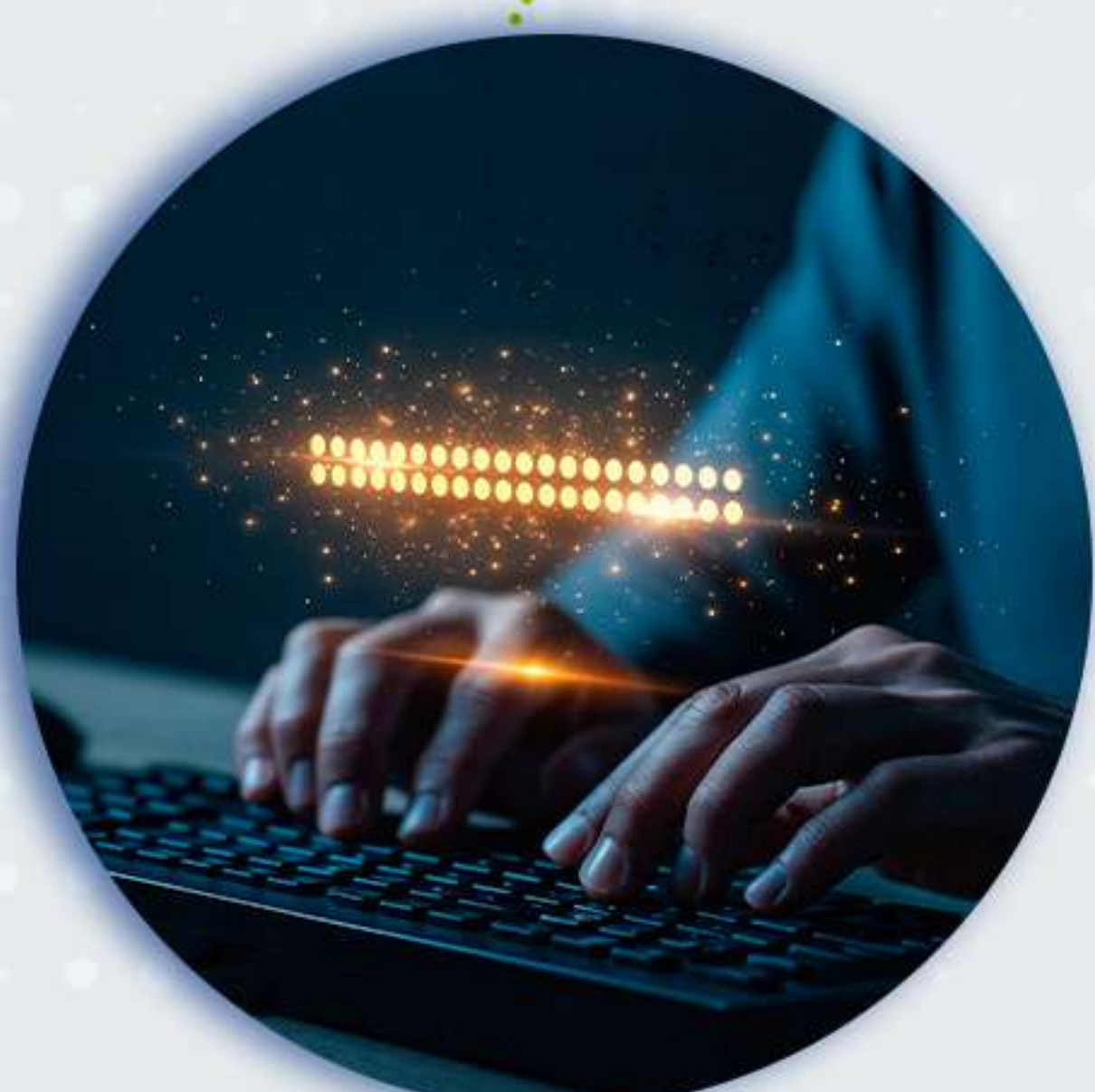
- Los delincuentes realizan llamadas falsas haciéndose pasar por bancos.
- Envían solicitudes de códigos, claves o datos sensibles.



Ventas falsas a través de redes sociales

Los delincuentes crean cuentas falsas y solicitan

- Pago anticipado vía transferencias, PSE o billeteras digitales.
- Luego desaparecen o bloquean al comprador.



Pagos inseguros o sin pasarelas certificadas

Las entidades y plataformas recomiendan evitar:

- Pagos por enlaces desconocidos.
- Transferencias directas a cuentas personales.
- Pasarelas sin protocolos de seguridad como HTTPS o certificados SSL.



¿Qué hacer en caso de ser víctima o intento de fraude?

Bloquea y protege tus cuentas de inmediato

Comunícate de inmediato con tu entidad financiera para bloquear movimientos.

Cambia contraseñas y activa doble factor de autenticación en: correo, redes sociales y app financieras.

Reporta el caso ante la entidad y Policía Nacional

Avisa por los canales oficiales de la entidad.

La Policía Nacional dispone del sistema **¡A Denunciar!**, donde se puede reportar fraude, estafa, suplantación y otros delitos informáticos.

¿Qué hacer en caso de ser víctima o intento de fraude?

Reporta ante la Superintendencia Financiera (en caso de que se tengan productos financieros involucrados)

La SFC permite reportar: fraudes bancarios y suplantación.

Al presentar una denuncia se debe aportar: capturas de pantalla, correos, mensajes y números desde donde te contactaron, enlaces sospechosos, extractos o movimientos irregulares, comprobantes de pago o transferencias.

Se puede realizar mediante CAI virtual, redes sociales, plataformas o tiendas donde haya ocurrido el incidente o intento de fraude.



Si perdiste dinero, sigue estas rutas:



Reporta de inmediato a tu entidad financiera.



Presenta un derecho de petición si no hay solución.



Acude a la Superintendencia Financiera para exigir respuesta.



Denuncia ante la Fiscalía el fraude.

