¡Hablemos de FRAUDES!

¿Qué hacer para evitarlos?

¿Sabías que un fraude financiero es cualquier acción realizada con la intención de engañar a una persona o institución para obtener beneficios económicos de manera ilícita?

Las personas delincuentes emplean diversas estrategias, desde simples engaños hasta sofisticados esquemas tecnológicos para acceder a información sensible, como números de cuenta, contraseñas o datos de tarjetas.

Estos fraudes pueden ocurrir tanto en entornos físicos como digitales, y las consecuencias para las víctimas incluyen pérdidas económicas, robo de identidad y problemas legales.

Por ello, es fundamental conocer las medidas de prevención y actuar de forma inteligente en el manejo de nuestras finanzas.

¿qué hacer?

Como ya lo expusimos, la prevención de un fraude es fundamental y aquí te damos algunos condutips:

Activa alertas de seguridad:
Solicita a tu Banco notificaciones para transacciones realizadas con tus cuentas y tarjetas. Esto te permitirá detectar movimientos sospechosos de inmediato.

Cambia tus contraseñas regularmente:
Utiliza claves seguras con combinaciones de letras, números y símbolos. Evita fechas de nacimiento o datos fáciles de adivinar.

Verifica la autenticidad de los sitios web:
Asegúrate de que las páginas donde introduces datos bancarios tengan una URL que comience con https://, revisa que el dominio sea correcto y checa que el ícono del candado esté cerrado.

Protege tus dispositivos:
Mantén actualizado tu sistema operativo, antivirus y aplicaciones bancarias. Configura el bloqueo automático de pantalla en tu celular.

Consulta directamente con tu Banco:
Si recibes un correo o mensaje sospechoso, llama al número oficial de tu Banco para confirmar. No confíes en números telefónicos proporcionados en mensajes dudosos.

Destruye documentos sensibles:
Tritura o quema tus recibos bancarios, estados de cuenta o cualquier papel con información personal, no lo tires a la basura.

Usa redes seguras:
Realiza operaciones bancarias únicamente en redes de Wi-Fi privadas o desde tu red móvil. Evita las redes públicas para tus transacciones.

¿qué no hacer?

- **No compartas tus datos personales:**
Nunca des tus números de cuenta, contraseñas, códigos de seguridad o claves dinámicas a través de llamadas, mensajes o correos electrónicos.
- **No confíes en ofertas demasiado buenas para ser verdad:**
Si algo parece demasiado atractivo, como un premio en el que no recuerdas haber participado, es probable que sea un intento de fraude.
- **No accedas a enlaces sospechosos:**
Evita hacer clic en links enviados por correos o mensajes que no esperabas, especialmente si prometen recompensas o advierten de problemas con tu cuenta.
- **No uses contraseñas repetidas:**
No utilices la misma contraseña para tus cuentas bancarias y otros servicios en línea.
- **No dejes tu tarjeta sin supervisión:**
Si estás en un establecimiento, mantén siempre tu tarjeta a la vista al momento de pagar.
- **No respondas mensajes de "urgencia":**
Los Bancos no solicitan información personal ni financiera por correo, SMS o WhatsApp. Desconfía de mensajes alarmantes.
- **No compartas fotos de tus tarjetas:**
Evita tomar fotografías o compartir imágenes de tus tarjetas de débito o crédito, incluso con personas de confianza.

ejemplos de fraudes financieros

***Phishing* (fraude por correo electrónico):**
Los delincuentes envían correos electrónicos que aparentan ser de tu Banco, solicitando que confirmes información personal o accedas a un enlace para "actualizar" tu cuenta. Al hacer clic, te redirigen a una página falsa donde roban tus datos.

***Smishing* (fraude por SMS):**
Similar al *phishing*, pero realizado a través de mensajes de texto. El SMS puede incluir un enlace o un número telefónico falso donde intentan obtener información confidencial.

Llamadas fraudulentas:
Alguien se hace pasar por un representante del Banco y te pide información como números de cuenta, claves de seguridad o códigos enviados por SMS, argumentando que hay un problema urgente con tu cuenta.

***Skimming* (clonación de tarjetas):**
En cajeros automáticos o terminales de pago, las o los delincuentes instalan dispositivos que copian la información de tu tarjeta al insertarla. También suelen colocar cámaras para obtener tu PIN.

Fraudes en redes sociales:
Publicaciones o mensajes privados que ofrecen promociones, préstamos inmediatos o premios a cambio de proporcionar información bancaria o realizar un pequeño depósito inicial.

Falsas aplicaciones móviles:
Aplicaciones que imitan las oficiales de los Bancos y que, al instalarse, solicitan tus contraseñas o accesos para robar tus datos.

Robo de identidad:
Usan información obtenida de documentos personales, redes sociales o bases de datos comprometidas para hacerse pasar por ti y abrir cuentas, solicitar créditos o realizar compras.

Fraude en plataformas de compra-venta:
Las personas estafadoras envían comprobantes de pago falsos para adquirir productos o servicios, o venden artículos que nunca envían tras recibir el pago.

Ingeniería social:
El delincuente manipula a la víctima psicológicamente, ganando su confianza para obtener información sensible o acceso a cuentas bancarias.

Cajeros automáticos alterados:
Además del *skimming*, algunos cajeros son manipulados para quedarse con tu tarjeta o para que no entreguen el dinero retirado, mientras los delincuentes aprovechan para robarlo.