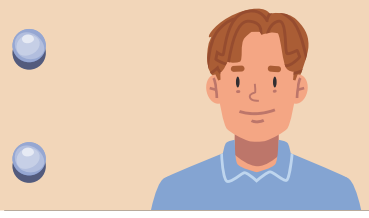
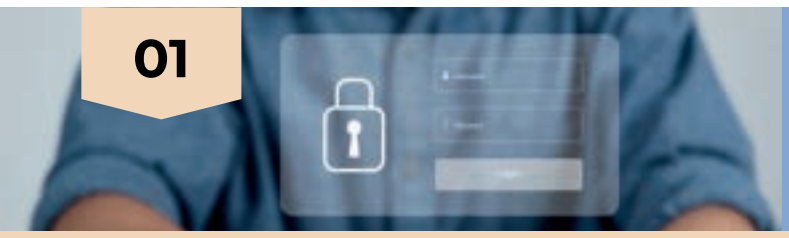


10 reglas básicas
para no caer en fraudes

ASOCIACIÓN DE BANCOS DE MÉXICO

Acciones simples que marcan la diferencia.

01



- No compartas NIP, token ni contraseñas.
- Son datos personales y nunca deben compartirse con nadie.
- Ni el banco, ni un familiar, ni un ejecutivo deben pedirlos.

02

- No hagas clic en enlaces sospechosos
- Un mensaje con un enlace inesperado puede llevar a:

Un sitio falso.

Una descarga peligrosa.

Un robo de tus datos.

03

Verifica que el sitio o app sea oficial

- Hay sitios web y apps que se parecen al banco, pero son falsos.
- Estas páginas roban tu usuario y contraseña.

¿Cómo verificar?

- Sitio web debe comenzar con https://
- La app debe estar en App Store, APP Gallery o Play Store.
- Verifica que el desarrollador sea el banco oficial.

No aceptes ayuda de extraños en cajeros

Algunas personas se hacen pasar por clientes amables o personal del banco para ayudarte, pero quieren robarte tu tarjeta o NIP.

04

05

No des ni teclees datos personales por teléfono

Aunque suene profesional o diga que es del banco, nunca compartas.

Nombre completo.

Fecha de nacimiento.

Número de cuenta o tarjeta.

Token o códigos SMS.

Teléfono y correo electrónico.

06

Activa las notificaciones de tu app bancaria

Las alertas por SMS, correo o dentro de la app te informan en tiempo real si se hace un movimiento con tu cuenta.

Cambia tus contraseñas regularmente

- Una contraseña segura no debe repetirse, ni ser predecible.
- Cambiarla con frecuencia reduce el riesgo de acceso no autorizado.

Evita Wi-Fi públicas para operaciones

Las redes gratuitas en aeropuertos, cafés o plazas no son seguras.

Un delincuente podría estar “espiando” la red para robar datos.

07

08

Reporta de inmediato transacciones que no reconozcas

Si ves un cargo que no hiciste o un movimiento raro:

No esperes. Reporta de inmediato.

Puede ser una señal de fraude en curso.

09

Desconfía de lo demasiado bueno para ser verdad

Premios sorpresa, préstamos milagrosos, regalos de dinero, sorteos que no recuerdas haber participado...

10

Valida todo antes de actuar

Antes de hacer cualquier movimiento, valida siempre:

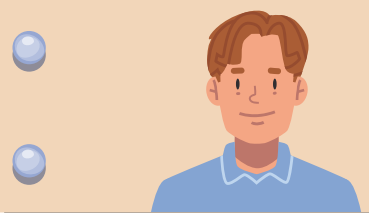
¿Es realmente el banco quien me contactó?

¿Estoy en el sitio oficial?

¿Reconozco esta compra o transferencia?

¿Estoy entregando información a alguien autorizado?

La mejor defensa contra el fraude está en tus manos.

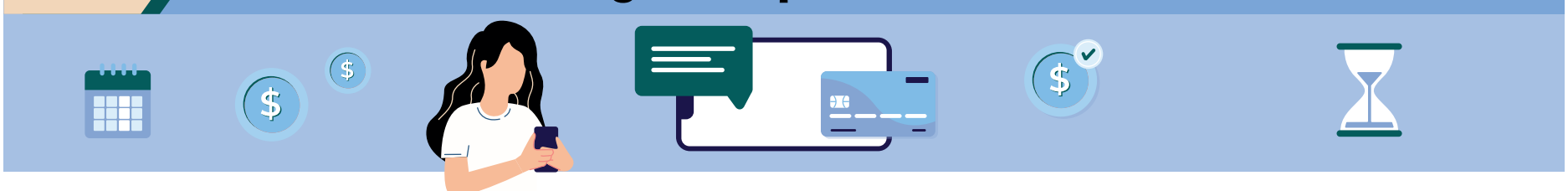


Tipos de fraudes bancarios en 2025

ASOCIACIÓN DE BANCOS DE MÉXICO

Conoce cómo se presentan y qué puedes hacer para protegerte.

01 Fraudes digitales y en redes sociales



Phishing

Son correos electrónicos que **parecen reales,** con logotipos y colores del banco, pero son **falsos.**

Te dicen que hay un problema con tu cuenta o que debes confirmar tu identidad.

Te piden que hagas clic en un **enlace peligroso** que lleva a una página falsa donde tú mismo **escribes tu usuario, NIP o token.**

Redes sociales

En Facebook, WhatsApp o Instagram pueden aparecer **publicaciones con préstamos falsos, sorteos o beneficios "urgentes".**

A veces se hacen pasar por el banco o incluso **clonan el perfil de una persona que conoces** para engañarte.

Smishing

Es como el phishing, pero **por mensaje de texto.**

Te mandan un SMS diciendo que tu cuenta fue bloqueada o que tienes un cargo extraño.

Incluye un **enlace falso** que al abrirlo puede robar tu información o instalar un virus.

Apps falsas

Hay aplicaciones que parecen reales pero no lo son.

Las apps falsas se descargan fuera de las tiendas oficiales (como Play Store, APPGallery o App Store).

Al instalarlas, **roban tus contraseñas o piden permisos para controlar tu celular.**

Vishing

Te llaman haciéndose pasar por **empleados del banco.**

Te dicen que hubo un cargo raro o que debes actualizar tu información.

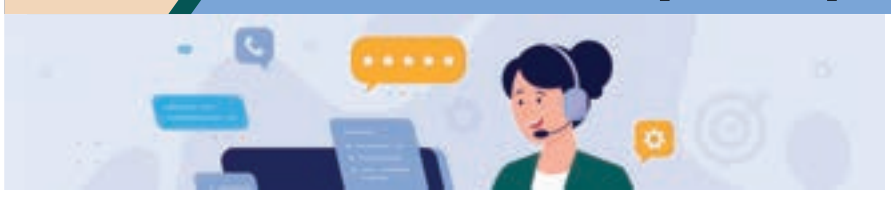
Te piden códigos, token, NIP o contraseñas, **pero en realidad quieren robarte.**

Malware bancario

Es un virus que se instala en tu celular o computadora y **espía tus movimientos.**

Algún malware incluso **copian lo que escribes** y lo envían a los delincuentes.

02 Fraudes por suplantación de identidad



Correos de suplantación

- El delincuente se hace pasar por una empresa, una persona o el banco.
- Usa correos similares a los oficiales.
- Los correos pueden tener errores ortográficos, urgencia o promesas irreales.

Solicitudes de créditos o compras sin autorización

Si tienen tus datos, pueden:

- Sacar un préstamo a tu nombre.
- Solicitar tarjetas.
- Comprar a crédito.
- Hacer compras en línea.

Robo de datos personales

- Obtención de INE, RFC, CURP, comprobantes y datos bancarios para abrir cuentas o pedir créditos.
- No compartas documentos por internet; destruye físicamente los que deseches y monitorea tu reporte de crédito, ya sea en Buró de Crédito o en Círculo de Crédito.

¿Qué hacer si alguien se hace pasar por ti?

01 **Llama de inmediato al banco** y reporta lo sucedido.

02 Pide que **bloqueen movimientos.**

03 Presenta un reporte en CONDUSEF si es necesario.

04 Denuncia el caso ante el Ministerio Público (fiscalía digital).

05 Si tienes buró de crédito, pide una alerta de protección.

Regla de oro

NO compartas tus datos personales, claves ni códigos.

Detente, piensa y verifica dos veces antes de actuar; si algo parece sospechoso, llama directamente a tu banco.