

**PRIMER**  
plano



FRAUDES FINANCIEROS

# EL TERROR DE TU CARTERA

Aprende a reconocerlos y no caigas en sus garras

**H**emos llegado al mes de noviembre, el penúltimo del año y en el cual las personas comienzan a recibir algunos adelantos de dinero que reciben a final de año, como la primera parte de su aguinaldo o algunas otras prestaciones adicionales a su sueldo.

Es por tal flujo de efectivo que debes cuidar muy bien tu dinero y tu cartera, esto con la finalidad de que las garras de los fraudes financieros no amenacen la seguridad de tu dinero. Sabemos que actualmente son muchos los tipos de fraudes financieros que se realizan, pero para facilitarte un poco las cosas, en esta edición de la revista Proteja su Dinero te daremos a conocer todos los detalles al respecto. Así que toma nota de cada uno de los tipos de fraudes financieros que existen, no expongas tu dinero ante el terror que representan y aprende a identificar el modus operandi de cada uno de ellos.

## ¿Qué son los fraudes financieros?

Debes saber que los fraudes financieros son acciones que una persona realiza con el fin de obtener un beneficio propio a costa de dañar la economía de otra. La mayoría de los defraudadores buscan conseguir tus datos para sacar un beneficio económico ilícito.

## ¿Cuáles son los fraudes más comunes?

Ahora que ya sabes cuál es la importante de tener identificados y estar siempre alerta de los fraudes financieros, te invitamos a que conozcas cuáles son los que existen, para mejor entendimiento, los dividimos en fraudes de persona a persona, fraudes cibernéticos o por internet, fraudes telefónicos y fraudes con tarjetas.

### Fraudes de persona a persona

- **Créditos exprés:**

son estafas en donde falsas empresas que se hacen pasar por gestoras de crédito, ofrecen préstamos con mínimos requisitos e inclusive sin consultar tu historial crediticio, y con tasas de interés por debajo de las que se ofrecen.

Usualmente piden un depósito anticipado, argumentando que son gastos de solicitud y comisión por apertura. Una vez que realizas el depósito, la empresa te informa tiempo después que el crédito no fue aprobado, pero no te devuelven tu dinero y desaparecen.

- **Pirámides:** son cadenas de ahorro que ofrecen ganancias elevadas, existen varios tipos, también usan mucho las redes sociales para llegar a más personas.

- **Ahorro informal:** las conocidas tandas pueden ser un medio para que se realice un fraude. La persona que administra la tanda, puede dejarte sin dinero en cualquier momento.



• **Trashing:** consiste en buscar información valiosa en la basura, como estados de cuenta, copias de identificaciones oficiales u otro documento que contenga datos importantes, con los cuales se pueda realizar un fraude, por ejemplo, robar tu identidad y/o realizar transacciones bancarias a tu nombre.

• **Alteración de cheque:** una persona se acerca cuando estás en la fila del Banco y ofrece cambiar tu cheque para que no pierdas tiempo esperando en la fila. Ya que el delincuente tiene el cheque, se retira y procede a alterar algunas de sus partes como: cambiar el nombre del portador, aumentar el monto a cobrar y endosarlo a su nombre.

• **Tallado de tarjetas:** este tipo de fraude se realiza en cajeros automáticos, y operan en grupos. Alteran la ranura donde introduces la tarjeta para que veas que el cajero está fallando, una persona que es parte de este grupo delictivo, te ofrece ayuda para limpiar tu tarjeta y aprovecha ese momento para cambiártela.

Un segundo cómplice observa cuando tecleas el NIP al momento de intentar retirar dinero por segunda vez y espera a que te retires para meter tu verdadera tarjeta y disponer de tu dinero.

• **Extorsión a domicilio:** los delincuentes acuden a tu domicilio y simulan ser empleados de algún Banco para conseguir tus datos, generalmente te convencen al decirte que tus cuentas están registrando cargos irregulares o que van a borrar tu historial crediticio.

## Fraude cibernético (internet)

• **Correo basura:** también conocido como SPAM, se trata de un mensaje, enviado a varios destinatarios que usualmente no lo solicitaron, con fines publicitarios o comerciales. La información de dicho correo te invita a visitar una página o descargar algún archivo que por que roba la información de tu dispositivo.

• **Smishing:** en este tipo de fraude, te envían mensajes SMS a tu teléfono móvil con la finalidad de que visites una página web fraudulenta. Esto con el fin de obtener tu información bancaria, para realizar transacciones en tu nombre.

• **Phishing:** también conocido como suplantación de identidad, aquí el defraudador se hace pasar por una institución financiera, para que al enviar un mensaje indicándote un error en tu cuenta bancaria, ingreses tus datos y así obtener tu información confidencial.

• **Pharming:** consiste en redirigirte a una página de internet falsa mediante ventanas emergentes, para robar tu información.

• **Fraude en comercio electrónico:** en este fraude sustraen tus datos personales, bancarios y contraseñas, mediante páginas de tiendas en línea falsas.

## Fraudes por teléfono:

- **Vishing:** mediante una llamada, en este fraude los delincuentes simulan ser empleados de alguna institución para obtener tu información personal y bancaria. Te convencen al decirte que tus cuentas están registrando cargos irregulares o que requieren alguna información.

## Fraudes con tarjetas:

- **Clonación de tarjetas con skimmer:** se trata de un dispositivo pequeño que se coloca en la ranura donde se desliza la banda magnética de tu tarjeta para hacer una clonación de tus datos bancarios.

## Fui víctima de fraude... ¿y ahora qué hago?

Ahora bien, si por mala suerte ya has caído en algún tipo de fraude y no sabes qué es lo que debes de hacer, acá te damos una breve guía de los pasos a seguir:



Contacta a tu Institución financiera o a los establecimientos comerciales implicados para solicitar la cancelación del medio intervenido y que en su caso se genere la emisión de una "alerta de fraude".



Reclama ante la CONDUSEF: Si se trata de algún problema en productos de Servicios Financieros (cuentas bancarias, tarjetas de crédito, créditos, etc.). En caso de que se trate de problemas con establecimientos de comercio o de prestación de servicios (no financieros) presenta tu reclamación ante la PROFECO. Si es posible, solicita el bloqueo de tu Reporte Especial de Crédito (Burós de Crédito) para evitar que los delincuentes obtengan más información sensible y así notificar a las Sociedades de Información Crediticia (Burós de Crédito) de las inconformidades que hayan surgido. Si no sabes cómo, acércate a la CONDUSEF para solicitar asesoría.



Denuncia ante la Policía Federal o la Policía Cibernética, para evitar futuras consecuencias legales. En caso de haber extraviado alguna identificación, levanta un acta ante el Ministerio Público inmediatamente sin esperar que seas víctima de algún fraude.



Mantente alerta y solicita tu Reporte Especial de Crédito En caso de identificar algo anormal, (por ejemplo, un crédito que no tramitaste) notifícalo de inmediato tu Institución o acércate ante la CONDUSEF.



Monitorea regularmente tus cuentas bancarias Cambia tus contraseñas de manera regular alternando mayúsculas, minúsculas y números. Recuerda que es necesario tener una contraseña diferente para cada cuenta, aunque parezca complicado.