¡Cuida tu patrimonio!

Evita fraudes bancarios

Nuestro patrimonio, además de estar compuesto por todos aquellos bienes de carácter propio o heredado como pueden ser: autos, casas, joyería, obras de arte, acciones del mercado de valores, muebles y otros, también está formado por nuestro dinero. Es por esta razón que, en una época en la que los fraudes bancarios han ido en aumento, es necesario que estemos atentos y pongamos manos a la obra para protegerlo.

De acuerdo con la Condusef, de 2020 a finales de 2022,
se registraron un total de

391 mil 182

controversias por posible fraude.

Además, se encontró un **incremento en el fraude cibernético,** que podría deberse al aumento del **comercio electrónico** y las **transferencias vía electrónica.**

Esto resulta aterrador, pero no te preocupes, cuidar tu dinero es muy fácil. A continuación, te compartimos algunos tipos de fraudes para que logres identificarlos y que tu información no caiga en las manos equivocadas.

Tipos de fraude

SPAM o correo basura

Es un mensaje enviado a distintas personas que suele estar disfrazado de un anuncio publicitario o comercial y te invita a visitar una página o descargar algún archivo. Si encuentras algunos elementos sospechosos o poco comunes, **evita hacer clic** porque, en lo general, es un virus para robar información de tu dispositivo electrónico. Por esta razón, si descargas aplicaciones, **hazlo mediante páginas oficiales.** Asimismo, para estar aún más seguros, te recomendamos **instalar un antivirus.**

¡Cuida tu patrimonio!
Evita fraudes bancarios

Smishing

Este fraude, tiene el mismo modo de operar que el punto anterior, pero se presenta mediante mensajes de texto. Así que ya sabes, no caigas en la tentación de abrir hipervínculos de fuentes desconocidas, porque puede ser fraude y darte muchos dolores de cabeza.

Phishing

Esta es una de las estafas más comunes y es el caso en el que las personas caen con mayor facilidad debido a que su objetivo es hacerse pasar por una institución financiera, indicando vía mensaje de texto o llamada telefónica que hay un error en tu cuenta bancaria, por lo que te solicitan ingresar o compartir tus datos personales. Este método es uno de los más peligrosos porque con tus datos, pueden hacer compras, solicitar créditos a tu nombre, realizar transferencias e incluso vaciar tus cuentas. En caso de que recibas una llamada o mensaje solicitando este tipo de información, **comunícate directamente con tu banco** para reportarlo. Recuerda que **los bancos no hacen este tipo de solicitudes.** Es mejor que entres directo a tu banca electrónica o acudas a tu sucursal.

Pharming

Este cibercrimen es muy parecido al phishing, pero su principal diferencia es que el ataque se hace aprovechando las páginas web. Es decir, no tienes necesariamente que dar clic en algún hipervínculo o recibir un mensaje o llamada. Los ciberdelincuentes se encargan de redirigir a los usuarios a una página web falsa cuyo nombre es el dominio oficial y robarles su información personal. Así que pon atención especial al nombre de la página web para evitar confusiones.

Seguro en este momento te estás preguntando, ¿cómo sé que la página web es real? No te preocupes, es muy sencillo. Solo verifica que exista un **candado** en la barra de direcciones y haz clic en él para asegurar que el sitio web tiene un **certificado de confianza actualizado.**

Asimismo, te recomendamos estar siempre alerta y revisar si la página tiene el más mínimo detalle diferente a las páginas que sueles visitar. De igual manera, si te solicitan información que llame tu atención mejor evita proporcionarla.

Como te mencionamos anteriormente, protegernos de estos ataques cibernéticos es muy sencillo y está a tu alcance. Estar atentos nos puede ayudar a prevenir que nuestra información personal caiga en las manos equivocadas y evitarnos un mal rato.