PROTEGE TU CARTERA DE LOS FRAUDES

Nadie está exento

Uno de los temas que constantemente está en boca de todas las personas,, por lo común, es el de fraudes financieros. Si eres de las y los que piensan que jamás caerá en uno, checa el siguiente artículo, ya que nadie está exento de ser una víctima más.

Quienes realizan este tipo de actividades actúan de diversas formas, por lo que es necesario que implementes acciones para proteger eso que tanto trabajo te cuesta obtener: tu dinero y patrimonio.

En este artículo de la revista *Proteja su Dinero* te decimos cuáles son los tipos de fraude más comunes y las medidas que puedes adoptar para protegerte.

Conocemos como fraudes financieros a todas aquellas acciones que una persona realiza de forma ilegal para obtener un beneficio propio y perjudicar la economía de otra.

POR TELÉFONO

Este medio es uno de los primeros que utilizaron los estafadores para obtener tu información personal y financiera. Ten mucha precaución si alguien se comunica contigo para confirmar tu información personal: nombre, dirección, RFC o CURP, número cuenta o tarjeta, NIP, contraseñas, códigos de seguridad, etcétera. Escucha detenidamente y si dudas de la finalidad de la llamada no entregues tus datos.

¿CÓMO DEBES ACTUAR?

- Contacta a tu institución financiera y confirma la información obtenida de la llamada.
- Si proporcionaste los datos que te solicitaron, no dudes en cancelar tus tarjetas y revisar si no tienes gastos que no reconozcas.

De enero a junio de 2021, el 70% del total de las reclamaciones del sector bancos, se deben a un Posible Fraude. BEF

POR TELÉFONO CELULAR A TRAVÉS DE MENSAJES SMS (SMISHING)

También conocido como *smishing,* en este tipo de fraude por lo general te envían un mensaje SMS a tu teléfono celular, con la finalidad de que visites una página web fraudulenta. Lo anterior con el objetivo de tener tu información bancaria para realizar transacciones a tu nombre.

¿CÓMO DEBES ACTUAR?

- Evita abrir vínculos a sitios sospechosos.
- En caso de descargar alguna aplicación, hazlo por medio de las tiendas oficiales.

CLONACIÓN, ROBO Y ALTERACIÓN DE INFORMACIÓN

Generalmente, este tipo de fraudes se realizan en cajeros automáticos, sucursales bancarias, gasolineras, restaurantes, entre otros. La forma en que operan es variada, sin embargo, la información que requieren conocer es tu número de NIP y tarjeta.

¿CÓMO DEBES ACTUAR?

- Antes de utilizar el cajero automático verifica si detectas piezas sueltas, bandas o redes en las ranuras, si es así repórtalo y no lo uses.
- Cuando pagues con tu tarjeta de crédito o débito, no la pierdas de vista, pide que te lleven la terminal y cubre el teclado al ingresar el NIP.
- No aceptes ayuda de extraños para ningún tipo de transacción, si requieres que alguien te auxilie acude con el personal del banco.
- Contrata servicios de alertas para recibir notificaciones de tus movimientos y conoce al instante lo que sucede con tus finanzas, consulta con tu institución financiera los costos y funcionamiento.

Fraudes

SITIOS FALSOS EN INTERNET (PHISING)

Igual que en los otros tipos de fraude, los creadores de estos sitios buscan obtener tu información bancaria. Este fraude también es conocido como *phishing,* en el cual, los estafadores crean una página falsa para hacerse pasar por una institución financiera, ya sea indicándote que existe un error en tu cuenta bancaria y con alguna otra situación alarmista te convencen para dar los datos que necesitan.

¿CÓMO DEBES ACTUAR?

- Evita acceder a sitios web que no reconozcas o parezcan inseguros.
- Si requieres entrar a un sitio web, escribe directamente en la barra de direcciones la página a la que deseas entrar.
- Nunca abras archivos adjuntos supuestamente provenientes de tu banco o descargados de internet.

El total de reclamaciones del sector bancos sumaron 27 mil 706 por posible Robo de Identidad (el 0.9% del total). Enero a junio 2021 BEF.

POR CORREO ELECTRÓNICO Y REDES SOCIALES

¡Acabas de ganar el premio mayor: 1 millón de pesos!, ¿te suena conocido? Correos con mensajes como el anterior son utilizados para cometer fraude. Otro nombre que se le da es el de spam o correo basura, se trata de un mensaje enviado a varios destinatarios que, usualmente no lo solicitaron y están disfrazados de fines publicitarios o comerciales.

La información de dicho correo te invita a visitar una página o descargar algún archivo que por lo general es un virus, a través del cual se roban los datos de tu dispositivo.

Los bancos con más reclamaciones por posible robo de identidad son Banco Azteca y Banamex con el 68% de las reclamaciones. Enero a junio 2021 BEF.

Por redes sociales, los defraudadores mandan mensajes privados solicitando tus datos personales y bancarios. Si recibiste un mensaje de este tipo, duda inmediatamente de su procedencia; no proporciones nada y verifica la situación con tu banco.

También el fraude se puede cometer por medio de ventanas emergentes o ligas en páginas falsas; a este se le conoce como ***pharming.*** ¡No caigas en el engaño!, asegúrate de ver la palomita de verificación marcada en color azul en todas las plataformas oficiales o un candado cerrado en la barra de navegación.

Recuerda que el incremento en fraudes financieros se debe principalmente a la falta de información y la forma en cómo tienes tu información en la red. ¡Maneja tus datos bancarios o personales con sumo cuidado!