LOS FRAUDES CIBERNÉTICOS SE ACTUALIZAN

Evita ser un blanco fácil

Se conocen como fraudes cibernéticos a aquellas estafas que utilizan la red para realizar transacciones ilícitas. Muchas veces, los estafadores se aprovechan del desconocimiento o poco cuidado que tienen las personas al utilizar los servicios financieros en línea, convirtiéndose en un blanco fácil.

En los últimos años, el fraude cibernético se ha sofisticado cada vez más, al grado de que, hacer un depósito, cobrar un cheque, retirar dinero de un cajero automático, solicitar un crédito, pagar con la tarjeta o realizar compras en línea, se ha convertido en un riesgo y de no adoptar medidas preventivas, puede llevarnos a ser víctimas de un algún fraude.

De 2020 a finales de 2022, la CONDUSEF registró un total de 391 mil 182 controversias por posible fraude, teniendo un incremento en el fraude cibernético, el cual, podría derivarse principalmente por el aumento del comercio electrónico y las transferencias vía electrónica.

Tan solo, durante 2022, el 62.3% de las controversias correspondieron a la banca múltiple (134,433). De esa cifra, 30.5% fueron asuntos presentados por personas adultas mayores (41,051) y de éstos, el 50.5% (20,745) se originaron por un posible fraude.

Las cuatro principales causas fueron:

- Consumos no reconocidos 8,426
- Transferencia electrónica no reconocida 4,162
- Cargos no reconocidos en la cuenta 3,257
- Disposición de efectivo en cajero automático no reconocida por el usuario 2,126

Pero para los delincuentes cibernéticos todos los usuarios de servicios financieros son blanco, desarrollando para ello, distintas formas de fraude, perfeccionando algunas otras clásicas como el SPAM o correo basura; el *smishing*, cuya característica es el envío de mensajes SMS a tu teléfono móvil; el *phishing*, también conocido como suplantación de identidad, con un mensaje indicándote un error en tu cuenta bancaria.

El *pharming*, que consiste en redirigirte a una página de internet falsa mediante ventanas emergentes, para robar tu información.

A continuación, te brindamos una serie de recomendaciones sencillas para que las pongas en práctica y evites ser víctima de fraude a través de:

Wifi

- No permitas que tu móvil se conecte automáticamente a redes Wifi de libre acceso.
- Apaga tu Wifi si no lo necesitas.
- Nunca envíes información confidencial a través de redes Wifi que no sean seguras.

Apps

- Instala solo las aplicaciones desde las tiendas oficiales, NUNCA las descargues de páginas web.
- OJO con las aplicaciones con malas referencias o de desarrolladores desconocidos.
- Actualiza tus *apps*, esto permitirá que tengan lo último en seguridad.
- No otorgues muchos privilegios a las aplicaciones a menos que sean seguras.
- Si no confías en la aplicación, no otorgues permisos como acceder a tus fotos, ubicación, contactos, documentos, etc.
- Recuerda que la CONDUSEF cuenta con el SIPRES, que te ayuda a conocer si el crédito que te otorgan por *app* proviene de una institución financiera debidamente regulada y supervisada. Visítalo en www.condusef.gob.mx

Smishing (*phishing* a través de SMS)

• Nunca confíes en mensajes que intentan obtener tu información personal.
• Nunca des clic a los enlaces que te envíen por mensaje.
• No descargues aplicaciones que te soliciten por mensaje.

Vishing (*phishing* por llamada telefónica)

• Nunca respondas a llamadas donde te soliciten información financiera o personal.
• Llama directamente a tu banco, utilizando el número de teléfono que aparece en el reverso de tu tarjeta de crédito o débito.
• Solo proporciona tu información cuando seas tú quien contacta directamente al banco, recuerda que los bancos tienen un protocolo para identificarte como cliente.
• Instala un *software* en tu móvil que pueda identificar si estás navegando en una página web segura o falsa.

Explorador

• Cuidado con los anuncios, premios, concursos y ofertas que parecen demasiado buenos para ser verdad, son prácticas de *phishing* que solo quieren robar tu información personal y financiera.
• Verifica que las URL sean seguras.
• Nunca guardes tu información de inicio de sesión, al utilizar un navegador web.
• Nunca des clic en la opción ''recordar contraseña'' en las páginas web.

Bluetooth

• Deshabilita el emparejamiento automático de *Bluetooth.*
• Apágalo cuando no lo necesites.
• Desconfía de los mensajes que intentan obtener tu información personal.

También puedes ingresar a nuestra página del Portal de Fraudes Financieros, donde podrás denunciar teléfonos, páginas web, perfiles de redes sociales y correos electrónico. Visita:
https://phpapps.condusef.gob.mx/fraudes_financieros/index.php