

ICBC MÉXICO



CONSEJOS DE SEGURIDAD PARA PROTEGERTE DEL FRAUDE

La información proporcionada en el presente material por Industrial and Commercial Bank of China México, S.A., Institución de Banca Múltiple ("ICBC México") es solo para fines informativos generales. El contenido de este documento se basa en información procedente de diversas fuentes de información públicas, las cuales no han sido corroboradas por ICBC México. Toda la información se proporciona de buena fe, no hacemos ninguna representación o garantía de ningún tipo, expresa o implícita, con respecto a la precisión, adecuación, validez, confiabilidad, disponibilidad o integridad de cualquier información presentada. ICBC México, su controladora, filiales, consejeros, funcionarios o empleados no se considerarán responsables frente a sus clientes ni a ningún tercero, ni asumirán responsabilidad alguna por cualquier pérdida directa o indirecta que pueda derivarse del uso del contenido del presente material. El presente documento está sujeto a cambios sin previo aviso. Lo anterior, en el entendido que, ICBC México no tendrá ninguna obligación de actualizar o modificar cualquier información contenida en este documento. La información y opiniones presentadas en el presente documento son únicamente de carácter informativo y cualquier uso de la información contenida en el mismo se hace bajo responsabilidad y riesgo de quien la utilice.

¿QUÉ ES EL FRAUDE FINANCIERO?

Son aquellos comportamientos o conjunto de acciones realizadas por una persona o conjunto de personas en contra de los usuarios de los servicios financieros con la finalidad de obtener un lucro indebido para sí o para una tercera persona.

CONDUCTAS DE FRAUDE

USURPACIÓN DE IDENTIDAD

Cuando una persona obtiene, transfiere, utiliza o se apropia de manera indebida, de los datos personales de otra sin la autorización de ésta última, usualmente para cometer un fraude o delito.

CONSEJOS PARA PREVENIR LA USURPACIÓN DE IDENTIDAD:

- Al deshacerte de los documentos que contengan información personal o financiera, destrúyelos perfectamente.
- Verifica constantemente tu estado de cuenta o consulta de movimientos para identificar movimientos que no realizaste y reporta inmediatamente al Banco si ves movimientos sospechosos.
- Utiliza contraseñas que no se relacionen con datos personales como fechas de nacimiento, números telefónicos o nombres de familiares; utiliza letras mayúsculas, minúsculas, números combinados y caracteres especiales.
- Nunca compartas tus contraseñas.
- Todos los documentos personales o archivos electrónicos, así como NIP, contraseñas y claves dinámicas deben conservarse en lugar seguro para evitar que personas extrañas tengan acceso a ellos.
- No utilices equipos públicos para realizar operaciones bancarias o compras por internet.
- Verifica la seguridad de los sitios web que utilizas.
- No hagas clic en enlaces sospechosos de correos o mensajes

ROBO DE DATOS PERSONALES E INFORMACIÓN FINANCIERA

Cuando una persona obtiene, utiliza o se apropia de manera indebida, de los datos personales y la información financiera de otra sin la autorización de ésta última, con la finalidad de obtener un lucro indebido para sí o para tercera persona.

CONSEJOS PARA PREVENIR EL ROBO DE DATOS PERSONALES E INFORMACIÓN FINANCIERA:

- Al deshacerte de los documentos que contengan información personal o financiera, destrúyelos perfectamente.
- Habilita autenticación multifactorial (MFA).
- Actualiza tu software y antivirus.
- Usa contraseñas seguras, deben ser largas, únicas y combinando letras, números y símbolos.
- No utilices equipos públicos para realizar operaciones bancarias o compras por internet.
- Verifica la seguridad de los sitios web que utilizas.
- No hacer clic en correos o mensajes que pidan información sensible.
- No realices transacciones en redes no seguras sin el uso de una VPN.

SUPLANTACIÓN DE IDENTIDAD DE INSTITUCIONES FINANCIERAS

Técnica fraudulenta en la que terceros malintencionados se hacen pasar por una organización legítima para engañar a empleados, clientes o socios, con el fin de obtener información confidencial, realizar fraudes o dañar su reputación.

CONSEJOS PARA PREVENIR SER VÍCTIMA:

- Verifica la dirección web, ingresando manualmente la URL en el navegador en lugar de hacer clic en enlaces de correos.
- Confirma con la institución directamente en los canales de comunicación oficiales.
- No confíes en mensajes alarmistas, ICBC México no solicita información personal a través de correos electrónicos, llamadas, ni SMS.

COMPROMISO DE MEDIOS ELECTRÓNICOS Y MALWARE

Ataques cibernéticos mediante software malicioso en los dispositivos de los usuarios, con el objetivo de robar información, interrumpir operaciones o causar daño a los usuarios .

CONSEJOS PARA PREVENIR EL COMPROMISO DE MEDIOS ELECTRÓNICOS Y MALWARE:

- Instala en tus dispositivos antivirus y antimalware.
- Manten el software de tus dispositivos actualizados.
- Usa contraseñas complejas y diferentes para cada cuenta.
- Instala firewalls.
- Realiza una copia de seguridad periódica de los datos importantes para restaurarlos en caso de un ataque.

FALSIFICACIÓN DE CHEQUES

Conducta que consiste en la creación, alteración o uso indebido de cheques con el propósito de engañar y obtener beneficios económicos de manera ilícita.

CONSEJOS PARA PREVENIR FRAUDES RELACIONADOS CON LA FALSIFICACIÓN DE CHEQUES:

- Utiliza cheques con medidas de seguridad como marcas de agua, tintas especiales y microimpresiones.
- Verifica la autenticidad de los datos en el cheque.
- Evita dejar espacios en blanco en los cheques para evitar alteraciones.
- Verifica la autenticidad de los cheques con luz ultravioleta si es posible.
- Asegúrate de que los números y letras coincidan y que no haya signos de alteración.