



Cómo protegerte de fraudes digitales y llamadas falsas para cuidar tu dinero e información

La tecnología ha transformado la forma en la que manejamos nuestro dinero. Hoy es posible hacer transferencias, pagar servicios, comprar en línea y realizar trámites desde el celular en cuestión de minutos. Sin embargo, esta facilidad también ha creado nuevas oportunidades para los delincuentes, quienes utilizan diferentes métodos para intentar obtener información personal, datos bancarios o acceso a cuentas.

Tanto los fraudes digitales como las llamadas falsas son cada vez más comunes y pueden afectar a cualquier persona, sin importar su edad o experiencia con la tecnología. Por eso, aprender a identificar señales de alerta y adoptar hábitos de seguridad digital es una parte importante de cuidar nuestras finanzas.

¿Qué son los fraudes digitales?

Los fraudes digitales son intentos de engaño realizados mediante herramientas tecnológicas con el objetivo de obtener información personal o financiera.

En México, instituciones como la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF) han alertado sobre modalidades como el phishing, llamadas falsas de supuestos bancos y mensajes fraudulentos que buscan obtener información de usuarios.

Algunos de los métodos más utilizados son:

- Phishing: mensajes o correos falsos que imitan a bancos, empresas o instituciones para robar datos.
- Smishing: fraudes realizados mediante mensajes SMS o aplicaciones de mensajería.

- Vishing: llamadas telefónicas en las que alguien intenta hacerse pasar por una empresa o institución legítima.
- Sitios web falsos: páginas que imitan tiendas, bancos o servicios conocidos.
- Aplicaciones maliciosas: programas que buscan obtener información del dispositivo.

El objetivo suele ser conseguir datos como contraseñas, números de tarjeta, códigos de seguridad, datos personales y acceso a cuentas, ya sea bancarias o de servicios digitales.

¿Por qué los fraudes funcionan?

Los delincuentes suelen aprovechar emociones y situaciones comunes para generar presión.

Algunas estrategias frecuentes son:

- Crear urgencia a través de frases que infunden temor como “tu cuenta será bloqueada si no actúas ahora”.
- Ofrecer premios o beneficios inesperados y, comúnmente, difíciles de creer.
- Alertar sobre supuestos cargos no reconocidos.
- Fingir ser familiares o personas conocidas que necesitan dinero con urgencia.
- Prometer oportunidades demasiado buenas para ser verdad.

La intención es que la persona actúe rápida e impulsivamente, sin tener oportunidad de analizar la situación.

Señales de alerta en llamadas falsas

Una llamada puede ser sospechosa si te piden datos confidenciales, si solicitan contraseñas o códigos enviados por SMS, o si te piden realizar una transferencia. También si te presionan para tomar una decisión inmediata y amenazan con bloquear tu cuenta, o si aseguran que ganaste un premio por el que ni siquiera has participado.



bancodonde.com

Recuerda que los bancos y otras instituciones legítimas normalmente no solicitan información sensible (como contraseñas, pines o claves enviadas a tu correo o número celular) por llamada para “verificar” tu identidad.

Nunca compartas códigos de seguridad

Uno de los fraudes más comunes consiste en que alguien solicita un código enviado por mensaje de texto o aplicación. Estos códigos suelen funcionar como una llave de acceso temporal, por lo tanto, si los proporcionas estarás dando acceso a quien te lo pide a tus servicios bancarios u otras aplicaciones con información personal o financiera.

Así que, aunque la persona diga ser del banco, soporte técnico o una empresa conocida, evita compartir códigos enviados por SMS, números de autenticación, contraseñas, NIP y los datos completos de tus tarjetas.

Si alguien te solicita esta información, es una señal importante de alerta y lo mejor es cortar la comunicación para llamar directamente al banco, la institución o empresa que supuestamente te está contactando.

Recomendaciones para proteger tus finanzas digitales

1. Activa medidas de seguridad. Aprovecha las herramientas disponibles y usa contraseñas diferentes para cada cuenta, activa la autenticación de dos factores, mantén actualizados tu celular y aplicaciones, y utiliza bloqueos de pantalla seguros. Estas medidas agregan capas de protección.
2. Verifica antes de hacer clic. Antes de abrir un enlace recibido por mensaje o correo, revisa si el remitente es confiable y verifica si el enlace corresponde al sitio oficial. Evita entrar a páginas bancarias desde enlaces recibidos por mensajes sospechosos. Lo recomendable es ingresar directamente desde la aplicación oficial o escribir la dirección manualmente.
3. No descargues aplicaciones desconocidas. Algunos intentos de fraude buscan que instales aplicaciones para supuestamente recibir ayuda, mejorar la seguridad o resolver un problema. Antes de descargar cualquier aplicación revisa quién la creó, consulta las reseñas y opiniones, y sobre todo, descarga solo desde tiendas oficiales.



bancodonde.com

4. Revisa tus movimientos financieros. Detectar un problema rápidamente puede reducir riesgos. Para ello, revisa periódicamente tus estados de cuenta, movimientos bancarios, compras con tarjeta y transferencias. Si identificas algo extraño, repórtalo de inmediato a tu institución financiera.

5. Cuida la información que compartes en internet. La información que publicamos puede ser utilizada para intentar engañarnos. Evita compartir públicamente tus datos personales completos, información financiera, fotografías de documentos y ubicaciones o rutinas detalladas. Los delincuentes pueden usar pequeños datos para crear engaños más creíbles.

Si sospechas que compartiste información o realizaste una operación fraudulenta, contacta inmediatamente a tu banco mediante canales oficiales y reporta el incidente ante las autoridades correspondientes. Activa medidas adicionales de seguridad al bloquear tarjetas o accesos comprometidos y cambiar contraseñas. Actuar rápido puede ayudar a reducir el impacto.

Muchas veces pensamos que los fraudes solo les ocurren a otras personas, pero los métodos de engaño cambian constantemente y pueden ser cada vez más sofisticados. Recuerda que la seguridad financiera también implica proteger nuestra identidad digital y la información que utilizamos todos los días.



bancodonde.com