ASOCIACIÓN DE BANCOS DE MÉXICO

CONDUSEF
COMISIÓN NACIONAL PARA LA PROTECCIÓN Y DEFENSA DE LOS USUARIOS DE SERVICIOS FINANCIEROS

COMUNICADO DE PRENSA

Ciudad de México, 10 de septiembre 2026

ALERTA PREVENTIVA SOBRE DESCARGA DE PROGRAMAS MALICIOSOS (MALWARE); CONOCIMIENTO Y PREVENCIÓN, LA MEJOR DEFENSA DEL USUARIO

- ***Los fraudes no inician o están vinculados necesariamente a apps bancarias.***
- ***El malware es un programa diseñado para infiltrarse sin permiso en los dispositivos y hacer fraudes bancarios robando credenciales o manipulando transferencias, tomando en algunos casos el control del dispositivo.***
- ***Desconfiar y verificar correos o mensajes con sentido de urgencia o de remitentes dudosos, entre las recomendaciones básicas a los usuarios.***

Ante la identificación reciente de intentos de fraude financiero relacionados con programas maliciosos, conocidos como *malware*, que se instalan en dispositivos móviles y buscan capturar claves, interceptar códigos de verificación o tomar control de éstos para intentar realizar transacciones no autorizadas, la Asociación de Bancos de México y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) exhortan a los usuarios de los servicios financieros y a los ciudadanos en general, a tomar medidas de prevención ante estos riesgos.

La prevención y mitigación de este tipo de fraude es prioritario para las instituciones bancarias, ya que el *malware* permite que el atacante opere desde el propio dispositivo o entorno digital del cliente al utilizar credenciales legítimas y mecanismos de autenticación previamente comprometidos; lo que a su vez dificulta la identificación inmediata de una operación fraudulenta y la forma en que se originó y ejecutó la transacción.

Por las distintas modalidades en que opera, como el control remoto, superposición de pantallas, extensiones maliciosas o instalación de archivos y aplicaciones comprometidas, las instituciones bancarias han fortalecido sus medidas preventivas, la comunicación con sus clientes y la coordinación interinstitucional con las autoridades financieras.

Cabe precisar que este tipo de fraude no inicia necesariamente dentro de la aplicación bancaria; en muchos casos, comienza cuando se recibe un mensaje SMS, un correo electrónico, una llamada o enlace falso engañoso que solicita se descargue una aplicación, abrir un archivo o compartir información confidencial. Con ese acceso, los delincuentes intentan obtener claves, códigos de seguridad o controlar el equipo para realizar operaciones no autorizadas.

En este contexto, tanto la ABM, organismo cúpula de la banca en el país, así como la CONDUSEF, institución que protege los derechos de los usuarios de los servicios financieros, comparten recomendaciones preventivas básicas que evitarán caer en engaños:

- Instalar una herramienta anti-malware-antivirus y mantenerla activa y actualizada.
- Evitar abrir enlaces recibidos por mensajes inesperados.
- Descargar aplicaciones únicamente desde tiendas oficiales.
- Mantener actualizado el sistema operativo, navegador y aplicaciones.
- No compartir contraseñas, NIP ni códigos de verificación.
- No instalar herramientas de control remoto por indicación de terceros.
- Verificar en toda operación, monto, beneficiario y cuenta destino antes de autorizarla.
- Activar alertas de movimientos para detectar operaciones no reconocidas.
- Abrir directamente la app oficial del banco y revisar desde ahí los movimientos.
- No descargar aplicaciones o archivos de mensajes sospechosos; de notarlo, bloquearlo y reportarlo.
- Ante dudas, llamar al número telefónico que aparece al reverso de la tarjeta o sitio oficial de la institución.

Entre las principales señales de alerta están los mensajes que generan urgencia, las solicitudes de contraseñas, NIP, códigos de verificación o datos de tarjetas, instrucciones para instalar aplicaciones o permitir acceso remoto, así como enlaces o páginas sospechosas y cambios inusuales en el funcionamiento del celular.

Si sospecha que su dispositivo fue comprometido o detecta una operación no reconocida, detenga la transacción, desconecte el equipo de internet y contacte de inmediato a su institución financiera por sus canales oficiales. Cambie también sus contraseñas desde un dispositivo seguro.

La implementación de medidas como la actualización de dispositivos, la cautela ante enlaces sospechosos, evitar instalaciones no oficiales y la verificación minuciosa de autorizaciones, contribuirá a reducir significativamente el riesgo de fraudes bancarios.

La Asociación de Bancos y la CONDUSEF refrendan su compromiso, desde el ámbito de sus responsabilidades, por trabajar en conjunto por un sistema financiero eficaz y útil para los ciudadanos, con la convicción de que la seguridad es una responsabilidad compartida.

---00---

Contacto para medios:

ABM
comunicacion@abm.org.mx

CONDUSEF
comsoc@condusef.gob.mx