

Evolución del fraude financiero en México: Un nuevo desafío

Recopilado por Amalia Beltrán

El sector bancario en México se enfrenta a una nueva generación de fraudes digitales altamente organizados por grupos criminales que están utilizando plataformas tecnológicas avanzadas que se alquilan como un servicio, permitiendo a estafadores comunes, operar ataques complejos de manera masiva y automatizada. Puede comenzar por algo cotidiano como una llamada, un mensaje de WhatsApp, un SMS, un correo electrónico o incluso una publicidad en redes sociales.

La principal amenaza radica en que estos ataques logran burlar las medidas de seguridad tradicionales, como los códigos de verificación enviados por SMS, al combinar páginas web falsas casi idénticas a las de los bancos, llamadas telefónicas engañosas generadas por Inteligencia artificial, y programas espías en teléfonos móviles, los delincuentes consiguen que sean los propios clientes quienes entreguen las llaves de sus cuentas bancarias sin darse cuenta.

¿Cómo engañan a los clientes?

El fraude se ejecuta mediante una manipulación psicológica muy refinada, apoyada en herramientas tecnológicas que operan de la siguiente manera:

El Anzuelo: Los clientes reciben mensajes alarmantes por WhatsApp, SMS, llamadas o correo (ej. «cargo retenido» o «cuenta bloqueada»), supuestamente de su banco, instándolos a actuar de inmediato a través de un enlace.

La Pantalla Falsa: Al hacer clic, el cliente entra a una página web que

copia a la perfección el diseño del banco. Mientras el cliente escribe su usuario y contraseña en el sitio apócrifo, un criminal está viendo esos mismos datos en vivo.

La Llamada Tecnológica: Si se requiere un código de seguridad, los criminales utilizan sistemas que imitan la voz humana para llamar al cliente. Estos sistemas automatizados suenan como asesores bancarios reales y convencen a la víctima de que les proporcione el código de seguridad que acaba de recibir en su celular.

El Robo: Con el usuario, contraseña y el código de seguridad (proporcionado voluntariamente por la víctima engañada), los delincuentes ingresan al portal real del banco y vacían las cuentas.

El punto crítico de inflexión: Ya no se necesitan grandes equipos de personas (Call Centers falsos) para hacer estas llamadas. Ahora, programas de computadora pueden hacer docenas de llamadas simultáneas, con voces que suenan completamente reales y profesionales, convenciendo a los clientes de entregar sus códigos de seguridad. Actualmente la IA puede ayudar a los atacantes a crear mensajes mejor redactados, con un lenguaje adaptado al contexto de la víctima y generar contenido falso cada vez más creíble, tal como: Correos y mensajes convincentes imitando tonos de comunicación bancarias, incluso generar audios que imiten voz de otras personas que sean utilizados para

solicitar información.

Mayor personalización: Por medio de la información que se encuentra disponible en internet, personalizar sus mensajes incluyendo nombres, cargos, empresas o datos que pueden parecer legítimos.

Imágenes y/o videos manipulados: Los deepfakes pueden utilizarse para reforzar una historia falsa o hacerse pasar por una persona.

La prevención ante este tipo de estafas automatizadas requiere adoptar hábitos estrictos de verificación al interactuar con cualquier notificación de la banca digital.

Jamás compartir códigos de seguridad por teléfono: Si se recibe una llamada solicitando este tipo de información —incluso si la voz suena profesional o automatizada—, se debe colgar de inmediato.

Evitar abrir enlaces en mensajes de texto o chat: Cualquier trámite debe realizarse escribiendo manualmente la dirección oficial en el navegador o

abriendo la aplicación oficial.

Ignorar llamadas de alerta urgente: Si una llamada notifica sobre una transferencia sospechosa en proceso y pide realizar pasos inmediatos en el teléfono, no se deben seguir las instrucciones. Es necesario colgar y marcar al número oficial que aparece al reverso de la tarjeta bancaria. Verificar la barra de dirección en el navegador antes de ingresar el usuario o la contraseña.

Privilegiar el uso de biometría: Habilitar el uso de huella dactilar o reconocimiento facial para movimientos bancarios.

Actuar con rapidez en caso de engaño: Si por error se ingresaron credenciales en un sitio web sospechoso o se proporcionó un código durante una llamada, se debe contactar de inmediato al banco por sus canales oficiales para realizar las medidas necesarias.

La tecnología puede hacer más sofisticado el engaño. Recuerda siempre verificar antes de actuar, esta acción continúa siendo una de las mejores defensas.

