Crecen 22% quejas contra la banca por robo de identidad

El **monto reclamado llegó a mil 122 mdp** en el tercer trimestre de 2025; el sector financiero llama a usuarios a incrementar acciones de vigilancia

ANTONIO HERNÁNDEZ
—cartera@eluniversal.com.mx

Al cierre del tercer trimestre de 2025, el monto reclamado por robo de identidad al sector bancario del país llegó a mil 122 millones de pesos, 22.5% por encima de lo registrado en el mismo periodo del año previo, indican datos del Buró de Entidades Financieras de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef).

Algunas causas de reclamación consideradas son la apertura de cuenta no solicitada ni autorizada por el cliente, créditos no reconocidos u otorgados sin ser tramitados o aprobados, así como disposiciones de efectivo en ventanilla y/o sucursal no realizadas por el afectado, entre otras.

A la par, el fuerte crecimiento que han tenido los servicios financieros digitales en México ha disparado las reclamaciones por la misma causa entre las empresas financieras tecnológicas (*fintech*) que operan en el país.

De acuerdo con datos de la Condusef, en este caso las quejas por posible suplantación de identidad involucraron un monto de 5 millones 737 mil 906 pesos entre enero y septiembre del año pasado, más del doble que los 2 millones 320 mil 823 pesos reportados en el mismo lapso de 2024.

Ante el crecimiento en este tipo de fraudes, las instituciones financieras mantienen sus alertas y campañas de información para evitar que sus clientes sean víctimas.

MOODY'S

"A medida que los ataques se vuelvan más rápidos y escalables, las empresas que no inviertan en defensas basadas en IA serán (...) más vulnerables"

"La IA generativa está transformando los ataques de suplantación de identidad al permitir campañas altamente personalizadas y convincentes"

FERNANDO GUARNEROS
Director de operaciones de IQSEC

"Gobierno y educación se perfilan como los sectores con mayor exposición en el corto plazo"

De acuerdo con Scotiabank, los usuarios deben incrementar la vigilancia, principalmente en el uso de la banca móvil.

El banco agrega que, como primera línea de defensa, se recomienda activar métodos de autenticación biométrica, como huella digital o reconocimiento facial, para el acceso a aplicaciones financieras. Es crucial, además, habilitar funciones de rastreo, bloqueo y borrado remoto del dispositivo móvil para reaccionar ante extravíos o robos. Adicionalmente, los clientes deben evitar almacenar contraseñas, datos bancarios o códigos de acceso en notas o correos electrónicos.

Ante cualquier movimiento no reconocido o sospecha, la notificación inmediata a la institución financiera es vital para activar protocolos de protección, monitoreo y prevención, señala Scotiabank.

IA potencia ataques en 2026

Para Moody's, el uso de la inteligencia artificial supondrá una creciente amenaza para las empresas en 2026. La agencia recordó que, durante los últimos meses, el fuerte uso de esta tecnología ha ampliado las técnicas existentes de ciberataque en lugar de introducir otras completamente nuevas.

Lo anterior ha provocado que las campañas de suplantación de identidad sean más convincentes y ha permitido estafas de *deepfake*.

"El consenso de la industria es que aún no se ha atribuido plenamente ninguna vulneración importante a la innovación impulsada por IA, pero a medida que los ataques se vuelvan más rápidos y escalables, las empresas que no inviertan en defensas basadas en IA serán cada vez más vulnerables", destaca Moody's.

Añadió que los avances en IA sugieren que, en el transcurso de los próximos años, los atacantes podrán utilizar *malware* que reescriba su propio código, aproveche las fallas de seguridad previamente desconocidas y lance campañas automatizadas contra miles de objetivos simultáneamente.

"La IA generativa está transformando los ataques de suplantación de identidad al permitir campañas altamente personalizadas y convincentes que evaden los métodos de detección tradicionales y aumentan significativamente las tasas de éxito", advierte la agencia.

"Más allá de los correos electrónicos y los mensajes de texto, la tecnología *deepfake* basada en IA puede producir suplantaciones realistas de audio y video de personas de confianza, lo que aumenta la eficacia de la ingeniería social".

Empresas bajo presión

Ante los mayores riesgos digitales, la firma de ciberseguridad IQSEC dijo que 2026 mostrará un escenario de alta presión para las firmas mexicanas, donde se anticipa un incremento sostenido de ataques basados en contraseñas robadas y campañas de suplantación de identidad cada vez más creíbles, facilitadas por mercados clandestinos que comercializan identidades digitales a escala global.

Para la empresa especializada, de mantenerse esta tendencia, México podría incorporarse formalmente al grupo de los 10 países más afectados por *ransomware* a nivel mundial.

"Gobierno y educación se perfilan como los sectores con mayor exposición en el corto plazo, mientras que tecnologías de la información y manufactura continuarán apareciendo de forma recurrente", asegura el director de operaciones de IQSEC, Fernando Guarneros.

"La combinación de digitalización acelerada, déficit de talento especializado y restricciones presupuestales crea un entorno especialmente vulnerable para una escalada prolongada de incidentes". ●