360 fraud protection by AppGate

PREVENCIÓN DE FRAUDE EN LA NUEVA ERA DE LA BANCA DIGITAL

Evolucionar la estrategia frente al fraude digital es una prioridad en Venezuela

Resumen ejecutivo

El fraude digital evoluciona más rápido que las arquitecturas de seguridad de la mayoría de los bancos. En América Latina los atacantes combinan phishing, suplantación de identidad, ingeniería social y fraude multicanal para comprometer clientes y ejecutar transacciones fraudulentas. Sin embargo, muchas instituciones financieras continúan abordando el fraude mediante tecnologías aisladas y tradicionales de autenticación, biometría o monitoreo transaccional.

Estas soluciones analizan eventos individuales, pero no comprenden el contexto completo del ataque. Como resultado, los bancos suelen detectar el fraude después de que el daño ya ocurrió.

La tormenta perfecta del fraude digital en Venezuela

Venezuela fue el país de América Latina con más crecimiento de ataques comparando 2024 y 2025. Según cifras del Guardian Fusion Center de AppGate, el incremento fue del 228%. Esto se debe a factores como:

- Crecimiento acelerado de la banca digital
- Dolarización de las transacciones
- Infraestructura tecnológica heredada y tradicional
- Escasez de talento especializado en ciberseguridad
- Mayor sofisticación del fraude digital en la región

El fraude ya no comienza en la transacción

Los ataques modernos se desarrollan en múltiples etapas: compromiso de identidad, acceso a la cuenta, manipulación de la sesión y ejecución de la transacción fraudulenta. En muchos casos, el ataque comienza antes de que el cliente siquiera inicie sesión.

El problema estructural: silos de seguridad

Muchas instituciones financieras utilizan plataformas aisladas y variadas para un mismo propósito, para autenticación, monitoreo de transacciones y análisis de comportamiento. Esta fragmentación impide comprender el contexto completo del cliente y del ataque.

Limitaciones de la autenticación basada en el riesgo tradicional

Las soluciones de autenticación basada en el riesgo (RBA) suelen analizar el riesgo del login, utilizando señales como dispositivo, IP o geolocalización. Sin embargo, muchas de estas soluciones no analizan el riesgo de la transacción posterior. Esto significa que un usuario puede autenticarse correctamente y aun así ejecutar una transacción fraudulenta.

Una nueva arquitectura de prevención de fraude

Las estrategias modernas de prevención de fraude requieren analizar continuamente tres dimensiones del riesgo en tiempo real:

- Riesgo de identidad
- Riesgo de sesión
- Riesgo de transacción

Cómo 360 Fraud Protection by AppGate cambia el modelo

- Análisis integral del recorrido digital del cliente
- Correlación de señales de identidad, comportamiento y transacción
- Detección temprana de fraude antes del login
- Autenticación adaptativa basada en riesgo
- Uso de analítica avanzada e inteligencia artificial para detectar fraude

Impacto para las instituciones financieras

- Reducción significativa de pérdidas por fraude
- Mayor adopción de canales digitales
- Menor fricción para clientes legítimos
- Mejor visibilidad operativa del fraude
- Mayor confianza del cliente en los canales digitales

EL IMPACTO DE LA IA EN EL FRAUDE DIGITAL

La inteligencia artificial está transformando radicalmente el panorama del fraude digital. Por primera vez, tanto los atacantes como las instituciones financieras utilizan tecnologías de IA para escalar sus capacidades, por tanto, tener estas capacidades es indispensable del lado de la banca.

Cómo utilizan la IA los atacantes

Generación de campañas de phishing mucho más creíbles utilizando modelos generativos

Creación de deepfakes de voz y video para suplantar ejecutivos o clientes

Automatización de ataques a gran escala contra plataformas digitales

Generación de malware y herramientas de fraude más sofisticadas

Uso de IA para identificar vulnerabilidades en procesos digitales

Esto permite a los atacantes aumentar dramáticamente el volumen, velocidad y sofisticación de los ataques.

Cómo utilizan la IA las instituciones financieras

Modelos de machine learning para detectar patrones anómalos de comportamiento

Análisis de comportamiento del cliente en tiempo real

Identificación temprana de ataques antes de que se ejecuten las transacciones

Correlación de señales de riesgo a lo largo del recorrido digital del cliente

Automatización de respuestas de seguridad basadas en riesgo

Cuando se utiliza correctamente, la inteligencia artificial permite a los bancos pasar de un modelo reactivo a uno predictivo de prevención de fraude.

Para conocer cómo Bancamiga protege su banca digital con las soluciones 360 Fraud Protection by AppGate, haz clic aquí.