¿Cómo protegerse del fraude por apropiación de cuentas?

Recopilado por el Staff de El Inversionista

Latinoamérica vive una aceleración sin precedentes en la adopción del comercio digital y los pagos en línea. Sin embargo, este avance también ha traído consigo nuevos desafíos. Según el estudio "Pagos en Latinoamérica en 2025: De la inclusión a la sofisticación", elaborado por Kushki en conjunto con Payments and Commerce Market Intelligence (PCMI), la inteligencia artificial se ha convertido en una poderosa aliada para combatir el fraude… pero también en una herramienta sofisticada para cometerlo.
Las tecnologías basadas en IA permiten identificar patrones anómalos en tiempo real, automatizar procesos y reducir los falsos positivos, generando así una detección de fraude más eficaz y menos costosa para los comercios. Además, la adopción de soluciones abiertas y accesibles como DeepSeek promete democratizar aún más estas capacidades en la región.
Sin embargo, el informe también advierte sobre el surgimiento de nuevos tipos de fraude impulsados por IA generativa, como el fraude de apropiación de cuentas (mejor conocido como account take over fraud) o los ataques mediante deepfakes, que están afectando a cualquier empresa que gestione cuentas de usuario.

Entendiendo el account take over fraud

Este tipo de fraude ocurre cuando un tercero malicioso obtiene acceso no autorizado a una cuenta legítima (por ejemplo, de banco, correo, redes sociales, etc.) para cometer fraudes, robar datos o realizar transacciones ilícitas. Para esto, los atacantes utilizan diferentes técnicas:
Phishing: correos o mensajes falsos que engañan al usuario para que entregue sus credenciales.
Fugas de datos: robo de información en plataformas que luego se vende en la dark web.
Credenciales reutilizadas: usar el mismo usuario y contraseña en múltiples sitios facilita el acceso masivo.
Malware: programas espía que registran las pulsaciones del teclado o capturan contraseñas guardadas.
Con esto, los grupos criminales acceden a información personal y/o financiera, con la cual pueden realizar compras, transferencias y retiros. Además, pueden hacer fraudes en nombre del titular y suplantar la identidad de la persona para acceder a otras redes, marketplaces, etc.

Recomendaciones para prevenir el account takeover fraud

Este tipo de fraude ya no es exclusivo de la banca o las fintech. Hoy cualquier comercio —desde un marketplace hasta un gimnasio o un restaurante— puede ser blanco de estos ataques. Por tanto, es importante que las empresas se preparen y ajusten sus protocolos de seguridad, para evitar este tipo de ataques y así mantener la confianza de los usuarios.
Así, la paytech brinda estas recomendaciones:
Autenticación multifactor (MFA) obligatoria: Implementa siempre al menos dos factores de autenticación en accesos sensibles (como correo electrónico, contraseña más un código OTP o biometría). Es una barrera efectiva contra accesos fraudulentos, incluso si se han filtrado contraseñas.
Supervisión de comportamiento transaccional con IA: Utiliza motores de detección basados en aprendizaje automático para identificar patrones de comportamiento anómalos en tiempo real (ubicaciones inusuales, frecuencia de transacciones, cambios repentinos en credenciales o dispositivos).
Tokenización de datos sensibles: Sustituye la información real de tarjetas por tokens seguros, evitando que los datos reales estén expuestos en caso de una apropiación de cuenta.
Protección de credenciales en el front-end: Cifra toda la información que se transmite desde el navegador o app móvil.
Evita almacenar contraseñas de forma insegura y usa siempre hash con algoritmos actualizados (como bcrypt o Argon2).
Alertas en tiempo real para los usuarios: Notifica inmediatamente al cliente cuando se detecten actividades clave: cambios de contraseña, nuevos dispositivos conectados o intentos de acceso desde ubicaciones desconocidas.
Revisión constante de accesos privilegiados y permisos: Asegúrate de que los administradores del sistema no tengan acceso innecesario a datos sensibles de usuarios, y aplica políticas de «menor privilegio» por defecto.
Promueve prácticas seguras entre tus usuarios: Comunica de forma constante a tus clientes cómo detectar intentos de phishing o suplantación, y fomenta el uso de contraseñas fuertes y únicas para cada servicio.
Trabajar con aliados especializados en prevención de fraude: Busca empresas aliadas que integren la detección de fraude nativa con IA, análisis en tiempo real y sistemas antifraude actualizados en tus procesos de pago.