BioCatch

Prevención de Fraudes en el Siglo XXI: La Importancia de la Biometría Conductual

El fraude ha evolucionado

Los humanos se han convertido en la herramienta favorita de los estafadores

BOTs

Mules

Mobile Malware

Phishing

RATs

Scams

Los sofisticados ataques fraudulentos están haciendo que las políticas de device ID y direcciones IP de los dispositivos heredados sean ineficaces.

Gartner

ÚLTIMAS TENDENCIAS EN ESTAFAS : LOS FRAUDADORES VS. SUS CLIENTES

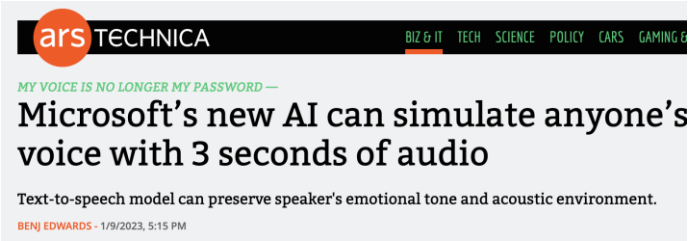
- Los defraudadores "atacan" a sus clientes fuera del perímetro del banco
- El perfil de comportamiento de la parte remitente sólo nos lleva hasta cierto punto con algunos tipos de estafa (por ejemplo, romántica, de compra, BEC).

- Están surgiendo métodos más sofisticados
- Los estafadores utilizan herramientas GenAI / Deep Fake

- Los bancos son cada vez más responsables de las estafas
- Presión normativa, modelos de responsabilidad compartida, reembolsos fraudulentos, etc.

MarketPlace

ebay



PSR Payment Systems Regulator

2023 Fraude Global Tendencias

EMEA

Las estafas ahora representan más del **50%** de todos los casos de fraude.

El **70%** de las estafas de herramientas de acceso remoto se originan a través de una llamada telefónica.

Las estafas de Pago Push Autorizado (APP) son la causa **#1** de pérdidas

APAC

Las estafas de voz han aumentado un **200%** interanual

El **54%** de todos los fraudes son ahora estafas.

El malware móvil está aumentando drásticamente con nuevos ataques como FluHorse y Nexus

LATAM

Aumento del 90% en dispositivos robados para facilitar la toma de control de cuentas

100% en cuentas mulas

Aumento del 20% en las estafas de ingeniería social.

NAM

El **61%** del fraude en 2023 provino de un dispositivo móvil, un aumento del **30%**
Los nuevos comportamientos de BOT han crecido un **72%.**
1 millón de casos de fraude de depósitos en lo que va de 2023.

Account Opening Protection

Account Takeover Protection

Social Engineering Scam Detection

Mule Attack Detection

Strong Customer Authentication

Tendencias del fraude en la banca digital en América Latina en 2023

Bienvenido(a) a la primera línea de la seguridad financiera. BioCatch, el líder mundial en inteligencia biométrica conductual, le ofrece un informe esclarecedor sobre las tendencias de fraude bancario digital en LATAM. Esta lectura esencial revela la dura realidad de los delitos cibernéticos que afectan a la industria financiera actual.

En este informe descubrirá:

- **El alarmante aumento de los ataques de ingeniería social:** un asombroso 33% de todos los casos en 2023 están relacionados con estos ataques, con picos notables en México, Brasil, Chile y Argentina.
- **El sorprendente crecimiento de los casos de dispositivos robados:** sea testigo de un aumento del 90 % en estos casos en la primera mitad de 2023 en comparación con la primera mitad de 2022.
- **Cuentas mula en aumento:** Un aumento significativo del 100 % en las cuentas mula reportadas, lo que pone de relieve los crecientes desafíos que enfrentan los bancos.
- **Diversos métodos de estafa en LATAM:** desde la insidiosa estafa de la "familia WhatsApp" hasta el atractivo engañoso de las "estafas de inversión", ármate de conocimiento sobre las últimas tácticas fraudulentas que causan estragos en la región.
- **Técnicas más allá del simple robo:** conozca métodos como "Shoulder Surfing", "SIM Swapping" y "Facial Recognition Bypass" que los delincuentes emplean para violar las medidas de seguridad y acceder a las cuentas bancarias de las víctimas.
- **El llamado a la seguridad avanzada:** Dado que las víctimas a menudo responsabilizan a los bancos por sus pérdidas, profundice en cómo las instituciones financieras en LATAM están implementando soluciones avanzadas como el aprendizaje automático y la inteligencia biométrica del comportamiento para salvaguardar a sus clientes y preservar la reputación de su marca.

Las defensas tradicionales están fallando a usted y a sus clientes

BOTs

Mules

Mobile Malwar e

Phishing

RATs

Scams

Análisis de datos estáticos

Proteja las defensas bancarias

Los comportamientos son elementos de datos

Altos falsos positivos

TRADITIONAL FRAUD ALERTING

APPLICATION	600	ACTION REQUIRED
DEVICE	800	ACTION REQUIRED
BEHAVIOR	400	ACTION REQUIRED
NETWORK	900	ACTION REQUIRED
TRANSACTION	500	ACTION REQUIRED

Estafas de Voz

Datos no Conductuales

Los indicadores proporcionan indicios tempranos de que esto puede haber sido una estafa; Sin embargo, la fricción asociada a este tipo de normas es muy alta.

Dispositivo consistente

El usuario está usando un dispositivo conocido

Ubicación geográfica coherente

La actividad de los usuarios se concentra en una región específica

Cambio en el valor del pago

La cantidad de pagos realizados difiere significativamente del comportamiento normal del usuario

Nuevo beneficiario

Los detalles del beneficiario son nuevos para un usuario que normalmente usa los mismos beneficiarios

El desafío de las reglas.

42.634.215.112.710

100 variables organizadas en grupos de 10 sin repetir.

Las nuevas casuísticas son emocionalmente devastadoras.

40%

de las víctimas de fraude nunca lo denuncian porque les da vergüenza.

Proteger a los clientes de ahora y lo que viene

Biometría conductual de 1a generación

COLECCIÓN Datos

INTELIGENCIA Conductual

MODELING de Sesión

Toma de decisiones basada en reglas y análisis de perfiles

SCORING de Riesgo (Ejemplo)

SCORE de RIESGO

515

Los datos y la actividad no no identificar el riesgo.

Inteligencia de Biometría Conductual

Behavioral Insights

Cognitive Intent Analysis

Rules-Based Decisioning & Profile Analysis

Risk Decision Intelligence

SCORE de RIESGO

925

Recomendación de acción dirigida

Pausar la transacción y requerir más autenticación y reconocimiento del usuario antes de permitir que la transacción se reanude o se procese.

BioCatch CONNECT

Fraud Telemetry Collection

3,000+ application, behavioral, device and network data signals collected from 7+ billion users sessions a month

- Applications
- Devices
- Transactional
- Browsers
- Networks

Continuous Behavioral Sequencing

Behavioral data science analyzes more than 300 unique user actions and cognitive patterns

- Age Analysis
- Being Guided
- Distractions
- Hesitation
- Active Phone Call
- Selection

Predictive Intelligence

Intent signals inform AI models that validate user motivation and identify risk of potential fraud

- Risk Score
- Risk & Genuine Factors
- Data Points
- Threat Indicators

La inteligencia para mirar lo que sigue

FRAUDE TRADITIONAL ALERTAS

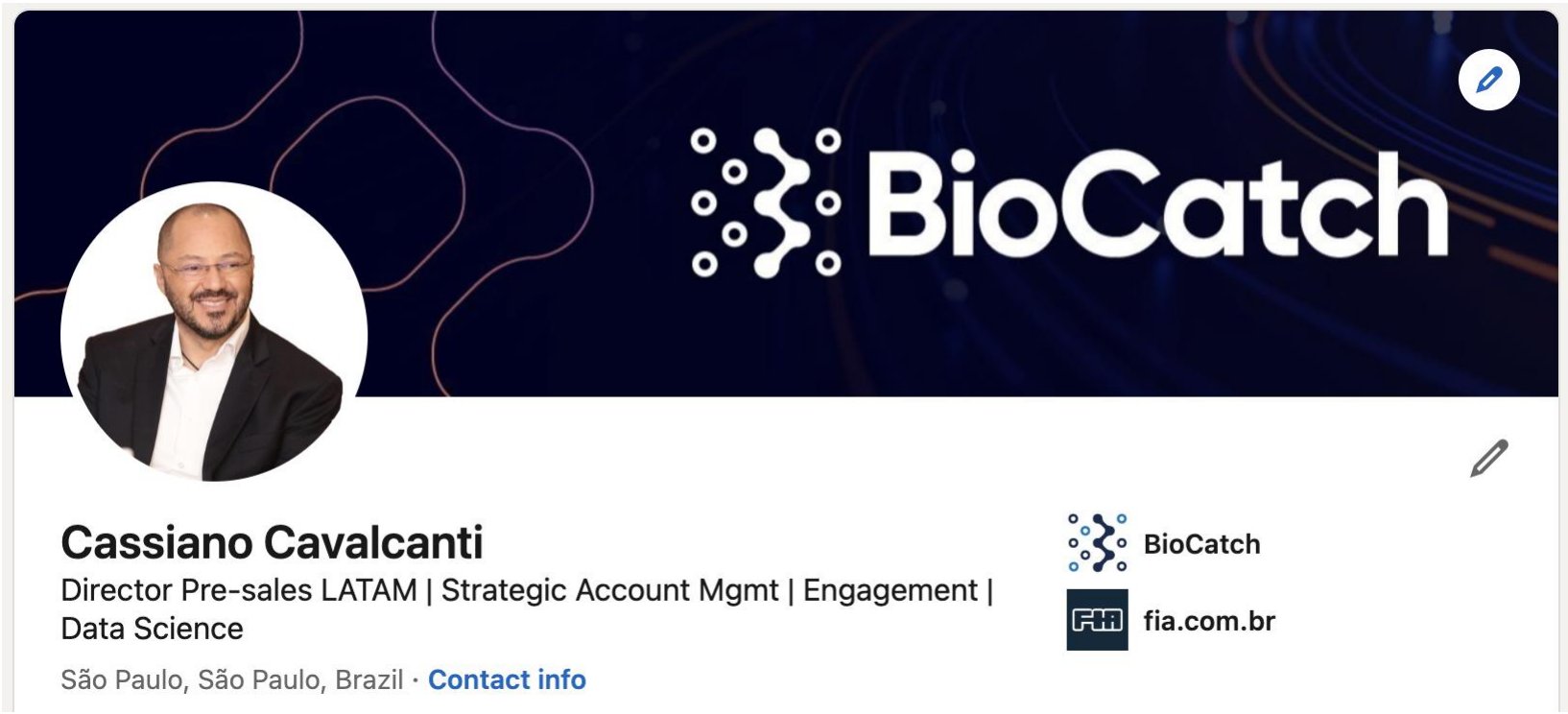
VS.

COMPORTAMIENTO CONTINUO SECUENCIACIÓN

Como comunidad tenemos la oportunidad, capacidad y deber para luchar contra el fraude.

¿Cómo podemos ayudarte a ser el héroe de la historia de tu cliente?

Detección de BOT *Acceso remoto* *Malware* *Emuladores Móviles* *Robo de credenciales* *Mulas* *Estafas*



Muchas Gracias