LexisNexis® RISK SOLUTIONS

Tendencias claves que moldean el panorama de fraude e identidad

Las transacciones digitales dominaron el mercado global a medida que la tendencia de interacciones en línea impulsada por la pandemia se convirtió en una práctica generalizada entre los consumidores.

Los desafíos de hacer negocios con consumidores altamente digitalizados que son objeto de redes de fraude industrializadas evolucionan constantemente. Las formas en que un defraudador puede interactuar con un negocio son infinitas. Estas redes de fraude altamente profesionalizadas llevan un ritmo perfecto y rentable al monetizar una serie de esquemas de fraude e identidad.

Estas son nuestras predicciones de las 7 principales tendencias en el campo de fraude e identidad de las cuales hay que estar pendientes, ya que son las que tienen mayor probabilidad de impactar su negocio.

1 LAS ECONOMÍAS DIGITALES EN EXPANSIÓN ESTÁN CREANDO OPORTUNIDADES EXPONENCIALES PARA EL FRAUDE

Datos de la red LexisNexis® Digital Identity Network® revelan un aumento en el volumen global de transacciones digitales.

ENERO A JUNIO 2022[1]

+27 % más

39,400 M transacciones

El incremento de transacciones digitales corresponde a un crecimiento casi igual de ataques de fraude.

Los canales digitales representan el **61 %** de todas las pérdidas globales por fraude[2]

Tasa de ataques iniciados por humanos **+33 % año contra año**

Ataques de bots **+38 % año contra año**[3]

A medida que las interacciones digitales se convierten en la norma y se incrementa la conectividad global, las empresas deben estar preparadas para intentos de fraude cada vez más complejos.

2 MERCADOS GLOBALES COMPLEJOS Y VECTORES DE AMENAZA INTERCONECTADOS EXIGEN UNA RESPUESTA COLECTIVA

Los defraudadores trabajan en redes complejas: cada dato utilizado está vinculado al siguiente dato valioso a escala mundial.

Por lo tanto, las empresas y las industrias necesitan una mayor colaboración a nivel mundial para combatir la red de fraude, pero también para entender quiénes son los consumidores de confianza. Tener visibilidad de los consumidores de confianza permite a las empresas abrir nuevos canales de ingresos y hacer ventas adicionales a una base de clientes leales.

3 ESQUEMAS COMPLEJOS DE INGENIERÍA SOCIAL MASIVA Y ESPECÍFICA DISTRIBUIDOS A TRAVÉS DE MÚLTIPLES GEOGRAFÍAS E INDUSTRIAS

Los ataques de ingeniería social están entre las amenazas de ciberseguridad de más rápido crecimiento en mercados tanto desarrollados como emergentes y continúan desafiando a las compañías ya que son uno de los tipos de fraude más difíciles de detectar.

Hay numerosas razones por las cuales los delincuentes están apuntando a los consumidores finales para cometer crímenes:

- Rápida digitalización global y disponibilidad de datos
- Crecimiento de banca abierta, transferencias más rápidas y pagos instantáneos
- Aumento de automatización e interacciones remotas
- Mejores controles de fraude están exponiendo el punto más vulnerable de la cadena: el consumidor

4 LA MIGRACIÓN A TRANSACCIONES MÓVILES Y EL PARADIGMA DE PAGOS DIGITALES ESTÁN DESAFIANDO EL RECONOCIMIENTO DE CONFIANZA Y LA GESTIÓN DE RIESGO

76 %

El volumen de transacciones móviles en la red Digital Identity Network® llegó a **76 % de todas las transacciones en el primer semestre de 2022**[1].

24 %

Métodos de pago alternos, entre ellos billeteras electrónicas y criptomonedas, representan el 24 % del volumen global de transacciones, un porcentaje similar al de métodos de pago tradicionales como tarjetas de crédito y débito. Las pérdidas por fraude atribuibles a estos métodos representan el 29 % de todas las pérdidas por fraude[1].

5 HALLAR EL EQUILIBRIO JUSTO ENTRE RIESGO Y FRICCIÓN ES IMPERATIVO CUANDO LAS COMPAÑÍAS BUSCAN PROTEGER A LOS CONSUMIDORES SIN INTERRUMPIR SU EXPERIENCIA

Los consumidores esperan experiencias altamente personalizadas que ofrezcan conveniencia en tiempo real y medidas de seguridad relevantes, las cuales son respaldadas por regulaciones emergentes que fortalecen aspectos de protección relacionados con cuentas y pagos.

Las últimas soluciones de identidad y autenticación adoptan una visión holística de la identidad y el riesgo, al combinar verificación de identidad física con evidencia de identidad digital asociada con el dispositivo que se está utilizando, ubicación geográfica y comportamiento del consumidor.

La inteligencia de identidad digital y de dispositivos puede permitir que aún las transacciones de alto riesgo procedan sin el inconveniente de pasos adicionales.

La biometría del comportamiento evalúa la manera en que un consumidor interactúa con el canal remoto, despejando así el camino para usuarios confiables e identificando con precisión transacciones sospechosas.

6 EL AUMENTO DE LA CONECTIVIDAD GLOBAL LLEVA A LAS REDES DE FRAUDE A AMPLIAR LA COMPLEJIDAD DE LOS ESQUEMAS DE FRAUDE

Las identidades sintéticas y robadas se vuelven más difíciles de descubrir cuando las empresas carecen de contexto y perspectivas que conecten a los consumidores a través de las dimensiones de identidad digital, física y de comportamiento a nivel global. Las diferentes dimensiones de una identidad deben ser analizadas para detectar y revelar esquemas de fraude complejos.

LOS CIBERDELINCUENTES APROVECHAN 63 NÚMEROS TELEFÓNICOS Y UBICACIONES FÍSICAS ÚNICAS ASOCIADAS CON UN SOLO CORREO ELECTRÓNICO[4]

UN CORREO ELECTRÓNICO CENTRALIZADO

- 7 direcciones IP
- 63 números telefónicos
- 63 ubicaciones físicas (63 identidades robadas)
- 12 pérdidas al interior de la red

Direcciones IP · Números telefónicos · Dirección · Pérdida detectada por fraude

7 LAS IDENTIDADES MULTIDIMENSIONALES DE LOS CONSUMIDORES EXIGEN UNA RESPUESTA MÁS DINÁMICA EN CADA PASO DE LA JORNADA DIGITAL[5]

1 de cada 12 creaciones de cuentas nuevas representa un intento de fraude

1 de cada 20 restablecimientos de contraseña es un ataque

Los enfoques estáticos contra el fraude no son sostenibles para operar en forma exitosa y segura en el mundo interconectado de hoy.

La jornada digital de los clientes dejó de ser simplemente lineal y a menudo se dan a través de varios canales digitales, híbridos y presenciales[5].

Promedio global

ESTABLECER CONFIANZA, MEJORAR LA EXPERIENCIA E IDENTIFICAR EL RIESGO: LAS 5 MEJORES ESTRATEGIAS PARA EL ÉXITO.

- Prepárese para cambios en procesos de gestión de riesgo a medida que se globalizan los pagos en tiempo real
- Priorice soluciones con aprendizaje automático avanzado a medida que este progresa significativamente
- Revise las ideas sobre compartir datos a medida que cambia la economía interconectada
- Adopte un enfoque multicapa hacia la prevención de fraude
- Invierta en educación ya que los humanos continúan siendo el eslabón más débil

El informe de LexisNexis® Risk Solutions sobre el estado global de fraude e identidad presenta nuestros más recientes hallazgos y perspectivas sobre tendencias de identidad, vectores de amenaza y tecnologías que más impactan su estrategia de defensa contra el fraude en este momento.

Para más perspectivas sobre cada tendencia, **Descargue el informe sobre el estado global de fraude e identidad 2022 (informe en inglés)**

Descárguelo ya >>

1. Análisis de datos de la red LexisNexis® Digital Identity Network®, enero-junio 2022.
2. LexisNexis® Risk Solutions *El verdadero costo del fraude™*, 2021-2022
3. Análisis de datos de la red LexisNexis® Digital Identity Network®, enero-junio 2022
4. Análisis de datos de la red LexisNexis® Digital Identity Network®, enero-junio 2022
5. Encuesta global de LexisNexis® Risk Solutions, 2022
6. LexisNexis® Risk Solutions: Análisis de datos de nuevas solicitudes de tarjetas de crédito de octubre y noviembre de 2021
7. Análisis de datos de la red LexisNexis® Digital Identity Network®, enero-junio 2022
8. LexisNexis® Risk Solutions *El verdadero costo del fraude™*, 2021-2022