

As principais tendências do cenário de fraudes e de identidades

As operações digitais dominaram o mercado global, à medida que as tendências das interações online, impulsionadas pela pandemia, tornaram-se um comportamento normal dos consumidores.



Realizar negócios com consumidores altamente digitalizados e que são ativamente visados por redes fraudulentas mostram que os desafios estão em constante evolução, uma vez que os caminhos para um fraudador interagir com uma empresa são infinitos. Essas redes de fraudes altamente profissionalizadas possuem um ritmo perfeito e lucrativo, monetizando uma série de golpes de fraude de identidade.

Veja a seguir as nossas previsões para as 7 principais tendências a serem observadas para o cenário de fraudes e identidade, pois apresentam grande probabilidade de impactar os seus negócios.

1 ECONOMIAS DIGITAIS EM EXPANSÃO ESTÃO CRIANDO OPORTUNIDADES EXPONENCIAIS DE FRAUDES

Dados da LexisNexis® Digital Identity Network® revelaram alta no volume global de operações digitais



O aumento das operações digitais é acompanhado por um crescimento semelhante dos ataques de fraudes



À medida que as interações digitais se tornam o padrão e a conectividade global aumenta, as empresas precisam estar preparadas para enfrentar tentativas de fraudes cada vez mais complexas.

2 A COMPLEXIDADE DOS MERCADOS GLOBAIS E A INTERCONECTIVIDADE DAS AMEAÇAS EXIGEM UMA RESPOSTA COLETIVA

Por meio de redes complexas, os fraudadores atuam massivamente e em escala global. Todo dado usado é vinculado ao próximo dado valioso.



Por consequência, as empresas e os setores precisam de uma maior colaboração global para entender quem são os clientes de confiança e combater às redes de fraudes. Ter certeza dos consumidores confiáveis permite que as empresas abram novos canais de receita e vendam mais para uma base fiel de consumidores.

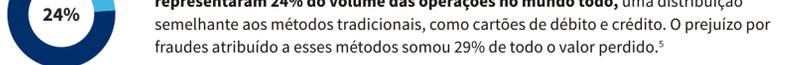
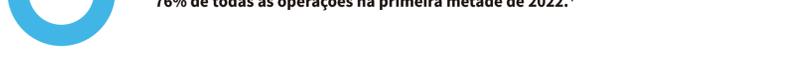
3 GOLPES EM MASSA DE ENGENHARIA SOCIAL SÃO DIRECIONADOS E DISTRIBUÍDOS POR DIVERSOS SETORES E ÁREAS

Ataques de engenharia social são os que apresentam crescimento acelerado dentre as ameaças de segurança cibernética, tanto nos mercados desenvolvidos, como nos emergentes. E continuam desafiando empresas, uma vez que representam uma das formas de fraudes mais difíceis de serem detectadas.

Há diversos motivos pelos quais os criminosos têm os consumidores finais como alvos de seus crimes:



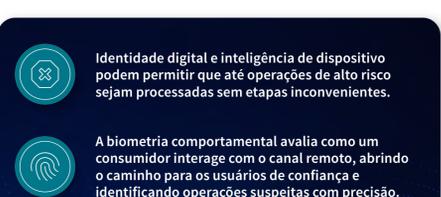
4 O PARADIGMA DA MIGRAÇÃO PARA AS OPERAÇÕES MÓVEIS E DE PAGAMENTOS DIGITAIS DESAFIAM O RECONHECIMENTO DE CONFIANÇA E A GESTÃO DE RISCO



5 DETECTAR O RISCO CORRETO PARA O EQUILÍBRIO DO ATRITO É PRIMORDIAL, JÁ QUE AS EMPRESAS TÊM COMO OBJETIVO PROTEGER OS CONSUMIDORES SEM INTERROMPER A EXPERIÊNCIA

Os consumidores esperam experiências altamente personalizadas, que ofereçam conveniência em tempo real, medidas de segurança relevantes e que são apoiadas por regulamentações emergentes que protegem questões de proteção de contas e pagamentos.

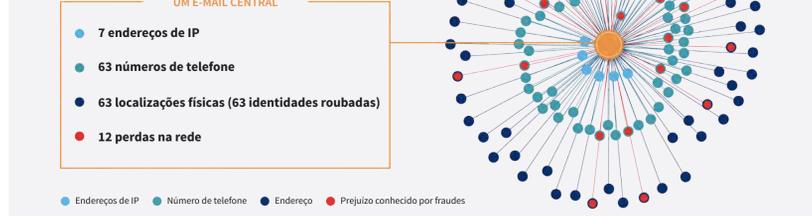
As soluções mais recentes de identidade e autenticação adotam uma visão holística de identificação e risco, combinando verificação de identidade física com evidências digitais baseadas no dispositivo utilizado, na localização geográfica e no comportamento do consumidor.



6 MAIOR CONECTIVIDADE GLOBAL LEVA AO AUMENTO DA COMPLEXIDADE DOS GOLPES POR PARTE DAS REDES FRAUDULENTAS

Em escala global, identidades roubadas e sintéticas são mais difíceis de serem identificadas quando as empresas carecem do contexto e das informações que vinculam os consumidores às dimensões de identidade digital, física e comportamental. As diferentes dimensões de uma identidade precisam ser analisadas para que complexos golpes fraudulentos sejam detectados e expostos.

ORGANIZAÇÕES FRAUDULENTAS USUFRUÍRAM DE 63 NÚMEROS ÚNICOS DE TELEFONE E LOCALIZAÇÕES FÍSICAS LIGADOS A UM E-MAIL⁶

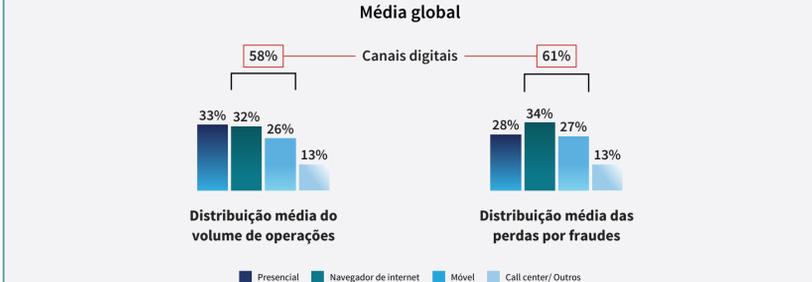


7 IDENTIDADES MULTIDIMENSIONAIS DE CONSUMIDORES EXIGEM UMA RESPOSTA MAIS DINÂMICA EM TODAS AS ETAPAS DA JORNADA⁷



No mundo interconectado de hoje, as abordagens estatísticas às fraudes não são sustentáveis para alcançar interações bem-sucedidas e seguras.

As jornadas dos consumidores deixaram de ser exclusivamente lineares e costumam ocorrer em vários canais digitais, híbridos e presenciais.⁸



ESTABELEÇA CONFIANÇA, APRIMORE A EXPERIÊNCIA E IDENTIFIQUE RISCOS: AS 5 PRINCIPAIS ESTRATÉGIAS PARA O SUCESSO

- Esteja preparado para mudanças nos processos de gestão de fraudes, à medida que os pagamentos em tempo real se tornam globais
- Priorize as soluções com machine learning avançado, pois estes programem de maneira significativa
- Reveja as opiniões sobre compartilhamento de dados conforme a economia interconectada apresenta mudanças
- Adote uma abordagem de inteligência para prevenir fraudes
- Invista em capacitação, uma vez que os humanos continuam sendo o ponto mais sensível



O relatório "O estado global das fraudes" da LexisNexis® Risk Solutions disponibiliza as mais recentes informações e pesquisa sobre as tendências de identidade, os vetores de ameaça e as tecnologias que mais influenciam a sua estratégia de defesa contra fraudes.

Para saber informações mais detalhadas sobre cada tendência, baixe o relatório em inglês: "Global State of Fraud and Identity".⁹

Baixe agora >>

Sobre a LexisNexis Risk Solutions

A LexisNexis® Risk Solutions aproveita o poder dos dados e das análises avançadas para fornecer informações que ajudam empresas e governos a reduzir risco e melhorar a tomada de decisões, beneficiando pessoas no mundo todo. Fornecemos soluções de dados e de tecnologia para uma grande variedade de setores, inclusive de seguros, serviços financeiros, assistência médica e governos. Com sede na região metropolitana de Atlanta, estado da Geórgia, Estados Unidos, contamos com escritórios por todo o planeta e fazemos parte do RELX Inc. (LSE: REL/NYSE: RELX), fornecedor global de análises baseadas em informações e ferramentas de tomada de decisão para clientes profissionais e empresas. Para mais informações, acesse www.risk.lexisnexis.com e www.rlx.com.

Este documento tem somente fins educativos e não garante a funcionalidade e nem os recursos dos produtos identificados da LexisNexis. A LexisNexis® Risk Solutions não garante que este documento esteja completo e sem erros. Se escrito por terceiros, as opiniões podem não refletir as da LexisNexis. A LexisNexis, a logomarca Knowledge Burst e a LexID são marcas comerciais registradas da RELX Inc. A LexisNexis é uma marca comercial registrada da RELX Inc. A Digital Identity Network é uma marca comercial registrada da ThreatMetrix, Inc. A LexID é uma marca comercial registrada da RELX Inc. Outros produtos e serviços podem ser marcas comerciais ou marcas comerciais registradas de suas respectivas empresas. Copyright © 2022 LexisNexis Risk Solutions. NXRI1528-00-0123-PT-LA

1. Data analysis from the LexisNexis® Digital Identity Network®, January-June 2022
2. LexisNexis® Risk Solutions True Cost of Fraud™ Survey, 2021-2022
3. Data analysis from the LexisNexis® Digital Identity Network®, January-June 2022
4. Data analysis from the LexisNexis® Digital Identity Network®, January-June 2022
5. LexisNexis® Risk Solutions True Cost of Fraud™ Survey, 2021-2022
6. LexisNexis® Risk Solutions: Data analysis from new credit card applications from October and November 2021
7. Data analysis from the LexisNexis® Digital Identity Network®, January-June 2022
8. LexisNexis® Risk Solutions True Cost of Fraud™ Survey, 2021-2022
9. risk.lexisnexis.com/global/en/insights-resources/research/global-state-of-fraud-and-identity