LexisNexis®
RISK SOLUTIONS

ÉTUDE DE CAS

LexisNexis® Risk Solutions bloque les attaques par test des identifiants sur l'application mobile d'une chaîne de restaurants

Les renseignements dynamiques sur l'identité numérique assurent une protection de bout en bout contre la fraude et l'exploitation abusive des avantages offerts pour l'inscription et la connexion à l'application mobile

EN BREF

SOCIÉTÉ

Grande chaîne de restaurants américaine

CAHIER DES CHARGES

- Détecter l'exploitation abusive des avantages offerts lors de la création d'un compte sur l'application mobile.
- Lutter contre un problème récemment identifié d'usurpations de comptes frauduleuses.
- Assurer à tous les utilisateurs une expérience fluide sur l'application mobile.

SOLUTION

Grâce aux renseignements dynamiques sur l'identité numérique fournis par LexisNexis Risk Solutions, cette chaîne de restaurants peut détecter et stopper efficacement les pratiques abusives et frauduleuses en temps réel, sans créer de contretemps pour les utilisateurs légitimes.

CE QU'IL FAUT RETENIR

- Réduction significative des usurpations de comptes frauduleuses.
- Forte diminution du nombre de rejets de débit.

ÉTUDE DE CAS

Grâce aux renseignements dynamiques sur l'identité numérique fournis par LexisNexis® Risk Solutions, cette chaîne de restaurants peut détecter et stopper efficacement les pratiques abusives et frauduleuses en temps réel, sans créer de contretemps pour les utilisateurs légitimes.

Présentation

Lorsque cette grande chaîne de restaurants a lancé son application mobile pour éviter aux clients de faire la queue en commandant et en payant leurs commandes sur leurs appareils mobiles, elle tenait à ce que sa philosophie simple et centrée sur le client soit reflétée en ligne. Elle devait cependant s'assurer que les avantages incitatifs et les récompenses ne fassent pas l'objet d'abus, et que l'introduction d'un système de paiement en ligne ne l'expose pas à la fraude.

Grâce à LexisNexis Risk Solutions, la société peut :

- Identifier avec précision les réseaux de fraude organisée qui tentent de tester les identifiants ou les informations de carte bancaire avant de compromettre les comptes des utilisateurs de confiance.
- Modifier les règles au sein du moteur de stratégies LexisNexis Risk Solutions de manière simple et rapide pour faire face à l'évolution constante des modèles de fraude.
- Maintenir l'intégrité de la plate-forme d'application mobile pour les utilisateurs de confiance réguliers.
- Continuer à proposer en toute confiance des offres et des avantages pour la création de compte.

Enjeu commercial

En guise d'incitation à la création d'un compte en ligne, cette chaîne de restaurants offrait un mets gratuit pour toute nouvelle inscription à l'application. Le nombre de comptes par utilisateur était limité, mais la société a vite constaté des abus, les clients créant plusieurs comptes à partir de leur appareil pour profiter de mets gratuits.

Ces pratiques ont affecté les résultats de la société, mais un problème plus important est rapidement apparu suite à l'introduction du paiement en ligne à partir de l'application mobile. La société a commencé à enregistrer un grand nombre de rejets de débit et de tentatives d'usurpations de comptes, ce qui semblait indiquer l'infiltration de cybercriminels organisés essayant de se connecter aux comptes des clients avec des identifiants usurpés ou volés, et de tester des informations de carte bancaire volées.

La chaîne de restaurants avait besoin d'une solution de protection contre la fraude performante, capable de détecter avec précision les comportements anormaux ou à haut risque au moment de la connexion, et d'offrir une meilleure visibilité sur la véritable identité numérique d'un utilisateur afin de détecter l'exploitation abusive des offres incitatives gratuites.

La puissance des renseignements partagés à l'échelle mondiale pour une détection en temps réel des événements à haut risque

La meilleure façon de lutter contre le problème complexe du cybercrime organisé est d'exploiter la puissance d'un réseau mondial partagé. Le réseau d'identités numériques Digital Identity Network® de LexisNexis® collecte et traite les renseignements partagés à l'échelle mondiale provenant de millions d'interactions client quotidiennes, dont les connexions, les paiements et les demandes de nouveau compte. Grâce à ces informations, LexisNexis® Risk Solutions crée une identité numérique unique pour chaque utilisateur en analysant les innombrables liens entre les appareils, les lieux et les informations personnelles anonymisées.

Les comportements s'écartant de cette identité numérique de confiance sont détectés avec précision et en temps réel, alertant la chaîne de restaurants d'une utilisation abusive des avantages incitatifs et d'une possible tentative de fraude.

Les comportements suspects sont identifiés et signalés pour vérification, authentification renforcée ou rejet avant le traitement de la transaction, ce qui crée une expérience fluide pour les utilisateurs de confiance.

Des empreintes numériques des appareils sont créées par validation croisée, permettant une détection complète de la fraude sur l'ensemble des transactions de l'application mobile.

Principales fonctionnalités de la solution LexisNexis® ThreatMetrix®

- **Smart ID** identifie les utilisateurs récurrents qui effacent les cookies, se servent de la navigation privée et modifient d'autres paramètres pour contourner la prise d'empreintes numériques des appareils. Cela améliore la détection des utilisateurs récurrents et réduit les faux positifs. À partir de l'analyse des caractéristiques d'un grand nombre de navigateurs, plug-ins et connexions TCP/IP, Smart ID détecte les tentatives de connexion multiples des utilisateurs cherchant à profiter des offres incitatives gratuites, ainsi que des fraudeurs tentant d'usurper des comptes existants.
- Les **technologies d'analyse approfondie des connexions** offrent un aperçu plus précis des événements suspects. Les fraudeurs tentent souvent de se cacher derrière des services de dissimulation de l'identité et de l'emplacement géographique, tels que des proxies cachés, des VPN et le navigateur TOR. Grâce à la technologie de perçage de proxy, LexisNexis® Risk Solutions examine les informations d'en-tête des paquets TCP/IP pour dévoiler à la fois l'adresse IP de proxy et la véritable adresse IP.

ÉTUDE DE CAS

Le réseau d'identités numériques Digital Identity Network® de LexisNexis® collecte et traite les renseignements partagés à l'échelle mondiale provenant de millions d'interactions client quotidiennes, dont les connexions, les paiements et les demandes de nouveau compte. Grâce à ces informations, LexisNexis® Risk Solutions crée une identité numérique unique pour chaque utilisateur en analysant les innombrables liens entre les appareils, les lieux et les informations personnelles anonymisées.

LexisNexis® RISK SOLUTIONS

Pour plus d'informations, appelez le 866.528.0780
ou rendez-vous sur risk.lexisnexis.com/FIM-EN

À propos de LexisNexis Risk Solutions

LexisNexis Risk Solutions exploite tout le potentiel des données et de l'analyse avancée pour fournir des informations qui aident les entreprises et les pouvoirs publics à réduire les risques et à prendre des décisions plus éclairées visant à rendre le monde plus sûr. Nous proposons des solutions technologiques et des données dans de nombreux secteurs d'activité, notamment les assurances, les services financiers, la santé et le service public. Basée à Atlanta, Géorgie, la société est implantée dans le monde entier et fait partie de RELX Group (LSE : REL/NYSE : RELX), fournisseur mondial de solutions d'information et d'outils d'analyse pour les professionnels dans tous les secteurs d'activité. Membre du FTSE 100, RELX est basé à Londres. Pour plus d'informations, rendez-vous sur www.risk.lexisnexis.com et www.relx.com

À propos de ThreatMetrix

ThreatMetrix®, société de LexisNexis® Risk Solutions, permet à l'économie mondiale de connaître une croissance rentable et sûre, sans compromis. Grâce à une vision complète sur 1,4 milliard d'identités numériques tokenisées, LexID® Digital fournit des renseignements sur lesquels s'appuient 110 millions de décisions quotidiennes d'authentification et de confiance afin de distinguer en temps réel les clients légitimes des fraudeurs. Dans l'étude Forrester Wave™ de 2017, ThreatMetrix est reconnu comme l'unique leader du marché de l'authentification basée sur les risques.

Pour en savoir plus, rendez-vous sur www.threatmetrix.com.