L'entité sécurité d'IBM empêche les cybercriminels d'ouvrir des comptes frauduleux

La technologie d'IBM Trusteer pour lutter contre la fraude aux nouveaux comptes protège à la fois les consommateurs et les banques

CAMBRIDGE, MA - 31 oct. 2017: L'entité sécurité d'IBM a annoncé aujourd'hui une nouvelle fonctionnalité d'IBM Trusteer qui aide les banques à identifier les comptes frauduleux avant leur ouverture. La technologie protège également les consommateurs même s'ils ne sont pas clients de la banque ciblée par le faux compte.

La fraude sur l'identité continue à représenter un défi mondial qui est coûteux pour les banques et les institutions financières. Au cours des six dernières années, [112 milliards de dollars](#) ont été volés par le biais de moyens frauduleux, ce qui équivaut à 35 600 dollars perdus chaque minute. Ces tendances devraient se poursuivre alors qu'elles seront associées aux vols historiques de données d'identification personnelles telles que les adresses, les numéros de sécurité sociale et les dates de naissance.

L'entité sécurité d'IBM aide les banques et les autres fournisseurs de services financiers à protéger les consommateurs en facilitant l'identification des comptes frauduleux grâce à son offre de détection de fraude aux nouveaux comptes [IBM Trusteer New Account Fraud](#). Cette nouvelle technologie, qui fait partie du portefeuille Trusteer Pinpoint Detect d'IBM, aide les institutions financières à tirer parti du machine learning afin d'associer d'un côté les informations sur les terminaux et les réseaux utilisés pour ouvrir un nouveau compte et de l'autre les analyses permettant de détecter la fraude.

La solution IBM Trusteer New Account Fraud (fraude aux nouveaux comptes d'IBM Trusteer) aide les banques à différencier les utilisateurs frauduleux des utilisateurs « légitimes », en examinant non seulement les informations positives qu'ils fournissent, mais aussi en les comparant aux indicateurs négatifs associés à la transaction. L'outil examine également les étapes critiques du processus de création de compte et utilise l'analyse comportementale afin d'aider à vérifier l'identité et les schémas de fraude potentiels.

Par exemple, des détails tels que l'adresse IP du lieu de création du compte, la géolocalisation / le fuseau horaire et l'état de santé de l'appareil utilisé peuvent être utiles pour détecter une activité frauduleuse. Si ces détails diffèrent de ceux de l'utilisateur habituel, cela peut être le signe qu'un nouveau compte peut être frauduleux.

Pour en savoir plus sur la technologie d'IBM Trusteer pour lutter contre la fraude aux nouveaux comptes : <http://www.ibm.com/us-en/marketplace/trusteer-new-account-fraud>

La solution New Account Fraud (fraude aux nouveaux comptes) sera un service additionnel à l'offre IBM Security Trusteer Pinpoint Detect, qui protège des centaines d'institutions financières et de sites web bancaires contre les prises de contrôle sur les comptes et les transactions frauduleuses et aide à la détection des machines des utilisateurs infectées par des logiciels malveillants à haut risque.

A propos d'IBM Security

IBM Security offre l'une des gammes de produits et services de sécurité pour entreprises les plus performantes du marché. Ce portefeuille, qui repose sur les recherches du mondialement célèbre IBM X-Force®, permet aux organisations de gérer efficacement les risques et de se défendre face aux menaces émergentes. IBM compte parmi les plus grandes organisations mondiales dédiées à la recherche, au développement et à la conception de solutions de sécurité, gère 35 milliards d'évènements de sécurité par jour dans plus de 130 pays, et possède plus de 3000 brevets dans le domaine de la sécurité. Pour de plus amples informations, rendez-vous sur <https://www-03.ibm.com/security/fr-fr/>, suivez [@IBMSecurity](#) sur Twitter ou consultez le blog [IBM Security Intelligence](#).

Pour en savoir plus, vous pouvez lire les deux billets de blog suivants :

Billet de blog de Jason Keenaghan : <https://securityintelligence.com/dont-be-catfished-protecting-yourself-from-new-account-fraud>

Billet de blog de Limor Kessem : <https://securityintelligence.com/massive-identity-data-exposure-leads-to-rising-tides-of-new-account-fraud-whats-next>

Vous trouverez [ici](#), une vidéo explicative de la nouvelle fonctionnalité IBM Trusteer

Pour en savoir plus sur l'offre IBM Trusteer :

<https://www-03.ibm.com/software/products/fr/category/advanced-fraud-protection>

Contact(s) relations externes

IBM

Gaëlle Dussutour Tél. : + 33 (0)1 58 75 17 96 DUSGA@fr.ibm.com

Text100 pour IBM

Amélie Chipaux Tél. : + 33 (0) 6 62 49 20 50 amelie.chipaux@text100.fr

---