New Account Fraud

Stopping identity theft and new account fraud

Highlights

- Uniquely identify users' devices via device ID and complex device fingerprinting
- Detect device/user/session risks by using multiple technologies to determine if account access is anomalous (including proxy detection, device spoofing, etc.)
- Use a global criminal device database to stop access based on device reputation
- Address online, mobile and cross channel attacks by correlating device risk and account credentials compromise history across all channels

Establishing a new account creates a trust relationship between organizations and their customers. This is also a critical stage where criminals use personally identifiable information (PII) stolen from victims via malware, phishing and other attacks to establish fake accounts. Various regulations, such as Red Flags Rule, require organizations to detect and prevent such attempts.

Detecting new account fraud requires an extensive view of device risks associated with the new account opening. IBM® tracks devices that access multiple accounts within the same organization and across IBM-protected organizations – a key risk factor at new account creation.

Traditional device ID systems lack the full visibility to today’s cross channel and multi-vector attacks and cannot uniquely identify most mobile devices. In contrast, IBM uses multiple technologies to determine if account access is anomalous, including device fingerprinting, device spoofing detection, proxy detection, geo-location, user behavior analysis, persistent mobile device ID, and more. By leveraging a massive global database of criminal devices, previously identified at any one of our hundreds of customers, IBM can flag devices that represent a high risk at account opening.

IBM further extends new account fraud detection with a holistic view of the fraud life cycle. In addition to device reputation and risk factors, IBM detects account credentials compromise history via malware and phishing to more accurately flag high risk account creation. IBM’s broad visibility, from identity theft to account creation, enables organizations to mitigate new account fraud risk and protect their customers’ funds and personal information.

.

For more information

To learn more about the IBM Security Trusteer portfolio of fraud prevention solutions, contact your IBM representative or IBM Business Partner, or visit: ibm.com/security

© Copyright IBM Corporation 2014

IBM Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

September 2014

IBM, the IBM logo, ibm.com, are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

Please Recycle