RISKIQ®

RiskIQ for Financial Services

RiskIQ empowers financial services security teams to respond quickly to external threats targeted at their employees, customers, and brand that use their own assets against them. RiskIQ illuminates unknown attack vectors that include phishing websites, shadow IT, rogue mobile apps, fake social media profiles, and domain infringement.

Financial Services Organizations Use RiskIQ to Reduce Their Digital Attack Surface and Solve Problems Associated With:

To provide a continuously updated inventory of external-facing digital assets, RiskIQ's proprietary discovery technology automatically identifies and indexes company-owned digital assets—including shadow IT, third-party code, and component relationships and dependencies between assets. With this view, organizations know:

Compliance with Industry Regulations and Policy

Information Security in a New Age of Financial Services

To comply with regulatory requirements, financial institutions must perform periodic risk assessments considering changes in the internal and external threat environment. RiskIQ uncovers unknown digital assets and, once discovered, adds them to the asset inventory of the organization and continuously monitors them for compromise and compliance. With a complete list of external-facing digital assets, a bank's security team can ensure an up-to-date asset inventory, complete with ownership information and status, and provide required compliance documentation.

Phishing

RiskIQ found and took down a domain hosting 240 different phishing sites targeting a single major bank

Financial services organizations are some of the largest targets for phishing schemes since they're the closest to a threat actor's primary goal—money. RiskIQ scans the internet for evidence of phishing, looking for unofficial sites that use an organization's logo, branding, and copied phrasing and marketing language. RiskIQ virtual-user technology experiences websites like a real user would, and can provide information about what would happen if a customer were to be tricked into visiting the site. RiskIQ can also open suspected phishing emails that are submitted by users and customers, follow the links, and analyze their impact.

RiskIQ automates the discovery and analysis processes around phishing investigations and allows security and incident response teams to mitigate its impact faster than ever before.

Mobile App Security

RiskIQ eliminated 16 rogue mobile application threats for a major bank in Q1 2016

RiskIQ continuously scans mobile app stores and apps to safeguard brand reputation and customers by detecting malware, application tampering, and brand impersonation. For each financial organization, we create a complete inventory of mobile assets to map the bank's mobile footprint across the global mobile app ecosystem. This includes monitoring for new apps, existing apps, app updates, and rogue or fraudulent apps.

By using RiskIQ, financial organizations have access to a robust, real-time footprint of its mobile app presence so it can continue to find and analyze threats and vulnerabilities.

Social

RiskIQ found multiple profiles impersonating a CEO for a major financial services firm

Recently, threat actors impersonated a large bank's customer service Twitter handle saying it was the secondary support profile setup to take on overflow from the primary one. Its tweets included a link for the user to click to "solve" their issue, which directed them to a phishing site masquerading as the official site.

With RiskIQ's virtual-user technology, organizations can find and shut down social impersonators like this by continuously discovering and monitoring social media profiles—both legitimate and fraudulent. They can then detect and eliminate social media-based threats against the organization, its employees, and its customers.

Domain Infringement

RiskIQ discovered and took down multiple infringing domains being used in tech support scams and browser locker attacks on customers of a major bank

Threat actors can register domains using trusted financial services brand names to drive monetizable traffic to other sites, phish for login credentials or payment card data, and distribute malware. RiskIQ searches DNS zone files for both exact matches to branded terms and close spelling variants (typosquatting) within domain names not belonging to an organization.

Our virtual-user technology automatically maps out an organization's websites and infrastructure and more accurately distinguishes legitimate sites from third-party registrations—even those falsely claiming brand association in their WHOIS data.

Threat Investigation

In a matter of minutes, security analysts can use RiskIQ's PassiveTotal® to build additional context and indicators related to financial fraudsters. Looking at a fraudulent URL in PassiveTotal, an analyst can see several unique data points:

- A historical view of the IP resolution for this domain
- Correlated web and analytics trackers to a particular domain
- WHOIS registrant/registrar information related to the domain
- Tags associated to the indicator that show that the domain is in RiskIQ's blacklist and that it is active

Teams leveraging RiskIQ can identify large portions of threat actors' infrastructure, which they can block and report, impacting their ability to monetize—and deterring them from targeting more victims.

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com