RiskIQ and Email Security

IDENTIFY AND BLOCK PHISHING ATTEMPTS

Every day, threat actors send millions of malicious emails to their targets. Attackers target employees of enterprises to gain access to internal systems, as well as customers to fool them into handing over payment card info or login credentials. Subjects of their attack emails range from ad campaigns soliciting views of a particular product to deliberately stealing system credentials or financial information.

By tracking against a wide range of sources, RiskIQ provides accurate, comprehensive coverage against rapidly growing phishing threats. With more than 30 million phishing pages scanned, RiskIQ can identify quickly evolving phishing attempts directed at your organization, customers, and partners at scale.

EMAIL THREATS

Diving into the Data

$2.3B

Estimated cost to organizations due to CEO email scams over the past three years, according to the FBI

250%

Increase in number of phishing websites detected since October 2015, according to the APWG

100K-230K

Jump in number of unique phishing campaigns between January 2016 to February 2016

PHISH DETECTION AND ABUSE BOX MONITORING

Enterprise security programs often utilize automated, internal phishing detection systems to detect phish targeting employees, but these systems don't see or protect against phishing threats to customers and partners. RiskIQ can scan emails from your internal phishing systems as well as suspected emails submitted by customers through an external-facing abuse box. RiskIQ then applies intelligence to find, confirm, and take down phish.

BE SMARTER ABOUT FINDING PHISH

The RiskIQ External Threat Management platform continuously scans web pages from Domain-based Message Authentication, Reporting and Conformance (DMARC), blacklists, threat intelligence vendors, email abuse boxes, and referrer log integrations for known phishing signatures. Meanwhile, our machine-learning classification algorithm and virtual user technology finds and confirms unreported phishing pages.

For security analysts, emails are an immense source of information—particularly infrastructure data. RiskIQ's PassiveTotal harnesses the power of big data analytics to surface the footprint of an attacker using elements found in an email, making threat investigations and incident response quicker and more efficient than ever before.

WITH RISKIQ FOR EMAIL:

AUTOMATE your workflow to shorten the mean time to mitigation per phish. RiskIQ crawls URLs on demand, automating URL investigations from Proxy, Email, DNS, and HTTP referrers and enriching internal logs with real-time intelligence.

KNOW where the phish are. RiskIQ detects phish with data beyond that found in an email—social media, digital ads, and known phish events within the RiskIQ index compiled from over 30 million phishing pages scanned.

SCAN your Abuse Box. Suspicious emails sent to employees and customers can be forwarded to an abuse box, and RiskIQ will scan emails and follow links with our virtual user technology, automating the phishing detection and confirmation process.

MANAGE the phish lifecycle. From detection to takedown, RiskIQ can automate the phish detection and confirmation process. The platform allows you to submit pages directly to Google Safe Browsing and Microsoft to block the attacker's campaign.

BENEFITS

Reduce your mean time to remediation

Reduce your security team's time to detection and phish remediation by utilizing RiskIQ to automatically analyze emails from your DMARC platform, spam filters, and abuse box. RiskIQ's virtual user technology will crawl all of the links in emails, checking for matching blacklisted URLs, known phishing pages, or pages hosting malware.

Uncover additional phishing infrastructure

Investigate confirmed phishing infrastructure using PassiveTotal to uncover additional sources for phish or malicious campaigns against your users and brand. Utilizing terabytes of passive DNS, WHOIS, and web tracker data, RiskIQ provides investigation capability to find other sites and attack infrastructure and proactively block your users from accessing themv.

Accelerate phish response

RiskIQ provides in-platform remediation capabilities to submit confirmed phish directly to Google Safe Browsing and Microsoft. This process alone can block 95% of all web traffic from accessing the phishing pages within 10 minutes of discovery. In addition to submitting malicious pages to Google and Microsoft, you can submit takedown requests directly to ISPs and hosting providers in three clicks.