RiskIQ Anti-Phishing Technology

Get Fewer False Positives to Combat Phishing at Scale

Companies are facing brand new challenges from a problem as old as the Internet itself. Phishing has evolved from the primitive tactics of its infancy into a sophisticated form of attack that combines new technology with a mature ecosystem of specialized criminals. Today, trillions of email abuse messages circulate on the Internet daily. To detect instances of phishing, anti-phishing providers must process tens of millions of URLs per day—something most are simply unable to do effectively.

RiskIQ's Anti-Phishing detects phishing attacks, automates alerts and analysis, and combats phishing at scale to allow security, eCrime, and incident-response teams to mitigate phishing's impact on a company dramatically.

Features and Benefits

Comprehensive Phish Detection and Unique Intelligence

RiskIQ Anti-Phishing continuously scans web pages for evidence of phishing. Our proprietary machine-learning classification algorithm finds and confirms unreported phishing pages at an industry-leading 95% accuracy rate.

By tracking against a wide range of sources—social media, digital ads, known phish events within the RiskIQ index, Domain-based Message Authentication, Reporting and Conformance (DMARC), abuse box and referrer log integrations for known phishing signatures, and 15 reputational list sources—we provide accurate, comprehensive coverage against rapidly growing phishing threats. With more than 30 million phishing pages scanned, we understand how best to identify quickly evolving phishing attempts at scale.

Virtual User Technology

Our proprietary virtual user crawl technology, invisible to anti-phishing countermeasures, experiences phish as targets would. By emulating user behavior while evaluating and analyzing phishing pages, RiskIQ can detect anomalies in behavior that indicate fraudulent activity more accurately than general methods such as checking the email or URL structure—while simultaneously bypassing techniques criminals use to evade detection.

RiskIQ's vast virtual user network includes:

- A diversified bank of IP addresses from more than 100 geographic locations
- All major browsers, both desktop and mobile
- Algorithms that initiate crawlers on specific pages and follow links to simulate referred traffic
- Algorithms that simulate user browsing behaviors and page and click-throughs, evading IP blacklists

Unparalleled Accuracy

With more than 95% accuracy in identifying phish, companies using RiskIQ won't waste time with false positives while live phish await verification. RiskIQ eliminates the need for large-scale manual reviews associated with alternative solutions with single-digit accuracy percentage rates. RiskIQ's Anti-Phishing dramatically shortens not only time to mitigation per phish but also overall phish uptime.

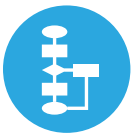
Scales With Your Needs

With the commercialization of phishing, companies are increasingly challenged to deal with larger scale and more sophisticated phishing campaigns. The volume and impact of these phish are rapidly outpacing legacy tools, which slow down identification and remediation efforts, and ultimately extend the lifetime of true phish and increase the impact of each attack on the organization.

RiskIQ Anti-Phishing Technology

Get Fewer False Positives to Combat Phishing at Scale

Only RiskIQ enables your security team to stay several steps ahead of these phishing campaigns. By empowering your organization to act on accurately identified phish without the distraction of false positives, you can find, block, and initiate takedowns of phish sites better than ever before.



Workflow

RiskIQ's user-friendly dashboard offers companies and security analysts full details on phishing events upfront for easy review and investigation. Analysts have four actions they can take for each incident:

- Confirm
- Dismiss
- Resolve
- Assign for Further Review

Analysts may also apply custom tags, annotate events with notes, and email event details to team members for feedback.

Remediation

RiskIQ empowers companies to disrupt phish attacks as they happen in the most effective way, by blocking customers' end users from visiting confirmed phish URLs. As follow-up, RiskIQ sends out notices to the ISP hosting the phish requesting a takedown of the phish URL.
Continuous monitoring lets customers know when enforced threats have been remediated successfully, and RiskIQ's post-resolution monitoring re-opens events and informs users of any tenacious threats posing a recurring risk to the organization.

Reporting

RiskIQ provides a sleek web user interface for clients to monitor the service and investigate specific incidents. Highlights include:

- A dashboard of all events across all products with event state and origin across a global map
- 'Screen Captures' show the web page as the virtual user session rendered it both on the first crawl and the most recent crawl to confirm the latest status
- 'Link Attributes' show the characteristics of the link, including its online status, the source, associated redirects, the domain, and country of origin
- 'Incident History' tracks the history of how the incident has been actioned by the support team
- 'WhoIs Data' aids in investigating the site associated with an incident
- 'Site-Crawl Data' including both the original response, fully rendered Document Object Model (DOM), extracted links, and file details

RISKIQ PROTECTS CORPORATE BRANDS AND THEIR CUSTOMERS ON THE INTERNET. The company combines a worldwide proxy network with synthetic clients that emulate real users to monitor, detect and take down malicious and copycat apps, drive by malware and malvertisements. RiskIQ is being used by leading financial institutions and brands in the US to protect their web assets, visitors, employees, and customers from security threats and fraud. To learn more about RiskIQ, visit www.riskiq.com.