Email Fraud Protection Services

Email Fraud is dominating security headlines

While email remains highly valuable to consumers and businesses worldwide, it is also vulnerable to abuse and is a leading attack vector used by malicious actors. Sending identities are often spoofed, making it difficult for ISPs and users to differentiate between legitimate and fraudulent email. Criminals exploit these technical and social vulnerabilities to achieve their commercial or political objectives by targeting a company's subscribers and employees with phishing, malware and other email-borne threats.

Through June 2014, phishing campaigns increased 146% year over year according to the Anti-Phishing Working Group. This is prominently displayed in the growing number of companies being targeted by email-based attacks that subsequently dominate the security and mainstream headlines. While fraud losses, investigation and remediation costs are key drivers in justifying the investment in a solution, the more significant damage is the lost trust in the brand.

Two things are certain: email fraud is a growing problem and traditional solutions have failed to address the situation. Brands need a holistic solution to block threats from reaching the inbox and reduce the impact from email-based threats. Return Path's real time threat intelligence supports a dynamic solution to protect your brand from the potential harm done by the wide array of threats that exist in today's ecosystem.

Types of spoofing include

Domain-based threats mimic the precise sending domain of the brand (e.g support@mybank.com).

Cousin domain threats are sent from addresses with domains that closely resemble the sending domain of the brand (e.g support@my-bank.com).

Display name spoofing mimics the brand in the header from label which most email clients render (entirely unrelated to the header-from email address itself).

Subject line spoofing mimics the brand in the subject line (independent of domain/ display name) in order to get the recipient to open the malicious message.

Designing a better solution

Traditional solutions operate downstream of the attack: they are reactive and focus on shutting fraudulent sites down after the malicious messages have already been sent. Meanwhile, the damage may already have been done. A more ideal solution is multi-layered and is achievable through closer cooperation with receivers of email:

1. Impact eliminated with DMARC implementation: block email fraud from reaching inboxes.
2. Expedited threat mitigation: mitigate email threats that did get through more quickly.
3. Real time threat intelligence: provide greater intelligence regarding the nature, size and impact of the threat.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

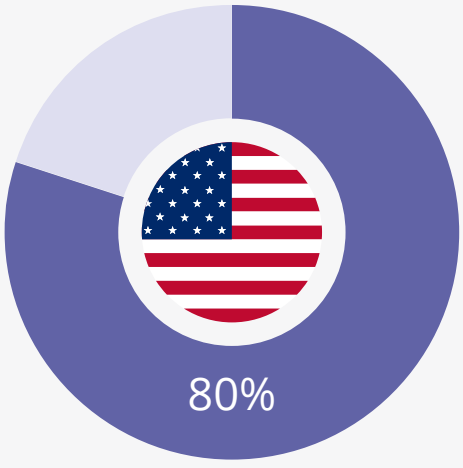
Prevents domain-based spoofing (specifically, spoofing of the "header from" or RFC5322.From domain) for domains owned by a brand.

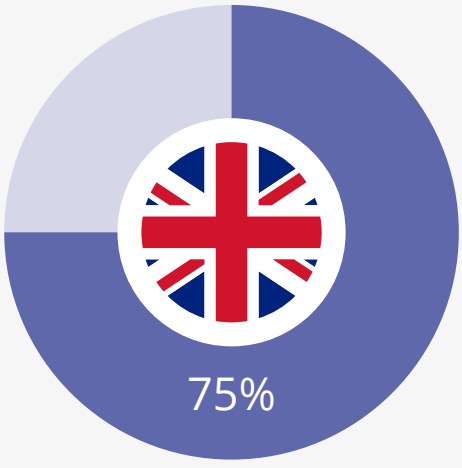
Provides threat reporting mechanism (aggregate and forensic data).

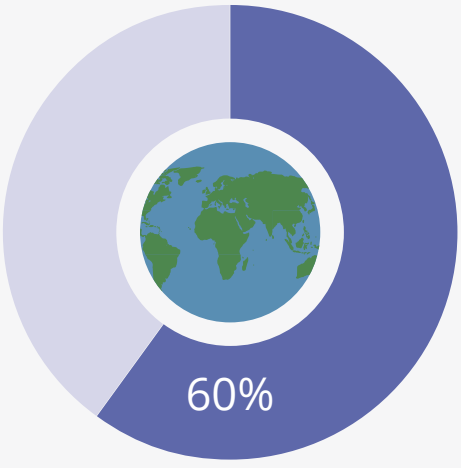
Leverages existing internet protocols: DNS, Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKM).

Supported by Gmail, Outlook.com, Yahoo! and other ISPs representing 60% of world's consumer mailboxes.

Percentage of mailboxes covered with DMARC:







The benefit of working with ISPs

Since 1999, Return Path has been a trusted partner of ISPs around the world to help them make better decisions regarding the differentiation between emails sent from legitimate senders that should be delivered, and fraudulent emails that should be blocked. Employed by ISPs in their filtering processes, Return Path's proprietary data services help protect over 2.5 billion mailboxes worldwide every day.

The data exchanged in its relationships with ISPs, combined with data from its other services, have enabled Return Path to build the world's largest database of email threat intelligence, which it makes available to its customers for expedited mitigation and investigation purposes. No other email security provider analyzes more terabytes of email data, at a faster rate, to identify and take action against phishing attacks.

7 Billion

Beyond DMARC, Return Path tracks data relating to 7 billion emails per day to identify bad senders.

300 Million

Return Path receives message-level data relating to 300 million potentially fraudulent emails every day.

770 Million

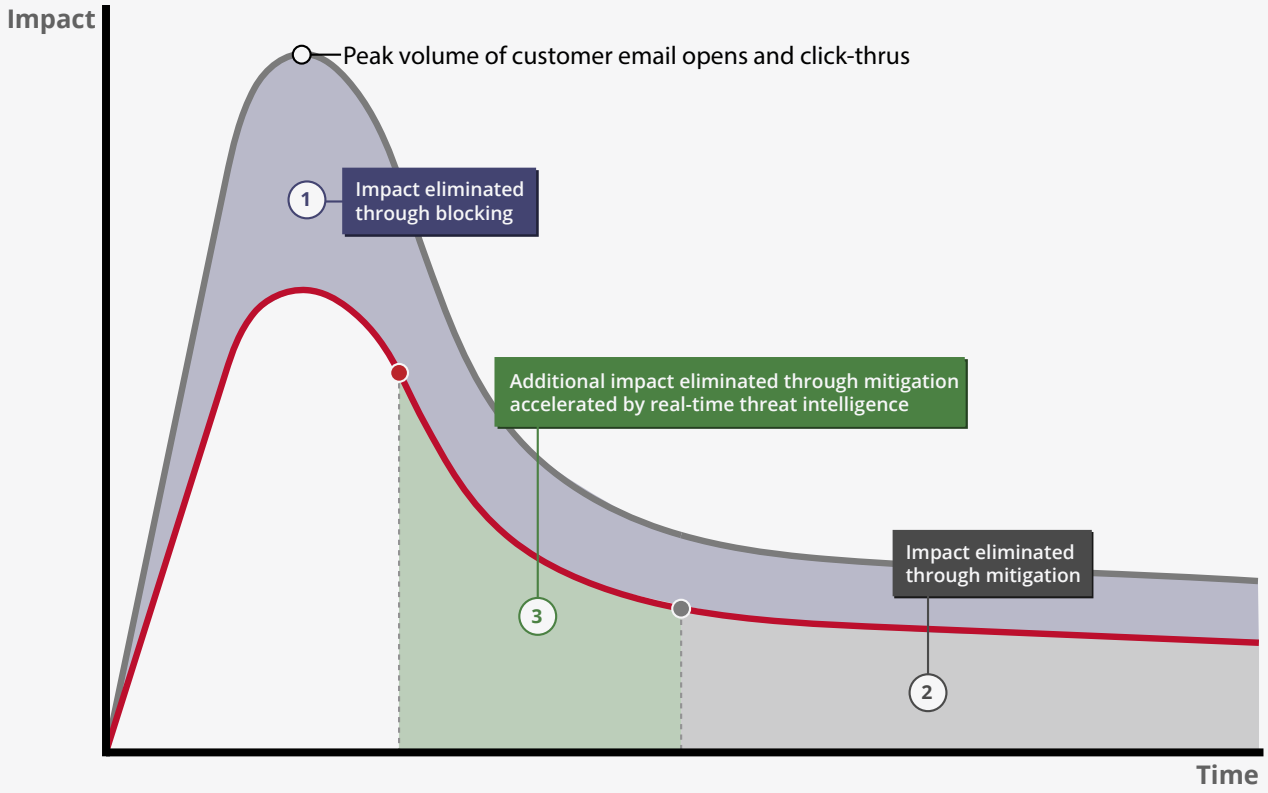
Return Path's blacklist of malicious IPs is used on a daily basis to protect 770 million consumer mailboxes.

Eliminating the impact of email fraud

Email fraud is clearly a growing problem: more verticals are being targeted with increasing regularity and sophistication. Meanwhile, traditional solutions are failing to provide companies with adequate protection. Looking at the profile of a multi-layered attack (e.g. a phishing campaign including both domain-based and cousin-domain attacks), most of the damage is done in the first four hours.

Time is money: the quicker Return Path responds to and eliminates a threat, the greater the reduction in impact. Our Email Fraud Protection services are used by top global brands, minimize the impact of email fraud, reduce fraud losses, enhance the trust in your brand and help you avoid becoming the subject of security news headlines:

1. Impact eliminated: suspicious emails that fail to meet authentication, reputation or other heuristic criteria are blocked by ISPs.
2. Impact mitigated: fraudulent URLs are published to a global network of providers who block access to the malicious site and ultimately remove the offending content.
3. Mitigation accelerated: real-time threat intelligence feeds an automated process to reduce the time to detection, thereby reducing the time to mitigation.



Contact Us

USA (Corporate Headquarters) rpinfo@returnpath.com
Australia rpinfo-australia@returnpath.com
Brazil rpinfo-brazil@returnpath.com
Canada rpinfo-canada@returnpath.com
France rpinfo-france@returnpath.com
Germany rpinfo-germany@returnpath.com
United Kingdom rpinfo-uk@returnpath.com

Return Path

returnpath.com