



Internet Service Providers can leverage our solution to strengthen their authentication efforts, in order to fully mitigate phishing threats and protect their customers from fraudulent emails.

GET MORE INFO

rpinfo@returnpath.net

1-866-362-4577

Anti-Phishing Solution for Internet Service Providers

Domain Assurance offers ISPs an anti-phishing solution that enables you to readily detect phishing and spoofing attacks to protect your customers from malicious email.

Every day your customers are targeted by innumerable fraudulent emails pretending to be from a trusted company. Although spam filters can help you capture many of them, filters are not foolproof, and a significant amount of phishing email continues to slip through.

In order to address the problem, major email providers like Yahoo!, Hotmail and Gmail have adopted two primary methods of email authentication, SPF and DKIM. They utilize SPF to prevent address spoofing and DKIM to validate the authenticity of a message. Nevertheless, the absence of authentication does not necessarily denote that an email is illegitimate, as few senders are authenticating their email or they are doing it incorrectly. For this reason, ISPs are reluctant to block unauthenticated email.

To make authentication work effectively, you would still need a registry of senders who can assure you that all their mail is being authenticated. This enables you to block unauthenticated mail at the gateway, protecting your network and your customers from phishing and fraud. You also need a communication mechanism to enable senders to ascertain which domains are signing all of their outbound mail to prevent sender authentication mistakes.

Introducing Domain Assurance, a new anti-phishing service from Return Path

Domain Assurance is a unique anti-phishing service that enables you to block unauthenticated email at the gateway to protect your customers' mailboxes from phishing attacks. The Domain Assurance solution allows senders to monitor and manage their authentication profile and confirm to ISPs that they are authenticating the email streams originating from their domains, thereby allowing you to reject all email that fails authentication checks.



Once participating senders are confident their mail is properly authenticated, they publish their domains and sub-domains to the Domain Assurance Registry. The Domain Assurance Registry provides the following benefits to ISPs:

- A trusted record of authenticated domains. This empowers you to enforce your authentication policies with confidence, rejecting email from domains in the Registry that fails both SPF and DKIM authentication checks, and treating other email according to your local policies.
- Increased efficiency in preventing delivery of malicious email to user inboxes. The ability to block unauthenticated messages, without having to perform expensive scanning of the content, enables you to better utilize the resources of your overworked servers.
- Decreased customer service issues sent to Postmaster teams by reducing malicious email traffic in the inbox. Your staff can focus on managing your network rather than on spoofing attacks.
- Improved inbox protection from illegitimate email that originates from frequently spoofed brands. Return Path works with the top brands in the Financial Services, Social Networking, Online Gaming and Online Coupon markets to ensure that their email streams are properly authenticated to keep pretenders out.

Domain Assurance allows you to:

Optimize your authentication policy. By integrating the Domain Assurance Registry with your email security solutions, you will be able to optimize your authentication policy and protect your network against phishing attacks at the gateway.

Proactively prevent phishing attacks. By contributing your authentication results data to the Domain Assurance Authentication Data Cooperative, you can provide comprehensive intelligence to legitimate senders, to help them audit their email authentication efforts and authorize you to block all unauthenticated messages.

The Bottom Line

In exchange for providing email authentication data, our ISP partners have free access to the Domain Assurance Registry and Audit List. The authentication results data that you contribute to the Domain Assurance Authentication Data Cooperative provides comprehensive intelligence to help legitimate senders audit their email authentication efforts. Domain Assurance provides statistical reports to ISPs that include the number of phishing attacks blocked and the effectiveness of the authentication policy. It also provides authorization from participating senders to block unauthenticated email without repercussion. This will enable you to prevent delivery of phishing or spoofed mails to your customers' mailboxes.

Why Return Path

We know email. As experts in email deliverability, we have built a solid reputation in the industry for helping legitimate email get into the inbox and keeping malicious email out. Our deliverability solutions are used by thousands of senders around the world to improve sending practices and protect the email channel from spam and other email abuse. Our receiver solutions are trusted by an extensive global network of receiver partners utilizing our data every day to improve their inbox filtering decisions.

Since 1999, Return Path has been setting email standards and protecting the inbox from malicious activity. We certify 16 billion emails every month and protect two billion users every day. Make sure your email and your email programs are trusted by both subscribers and mailbox providers. Let Return Path help you to block customer phishing emails, secure the email channel, protect your brand and mitigate fraud costs. Call 866-362-4577 or email info@returnpath.net to get started today.



If you have questions or would like to hear how Return Path can help, please call 1-866-362-4577, or email rinfo@returnpath.net. © 2011 Return Path, Inc. www.returnpath.net v033011