



Every day more than **260 million** fraudulent emails are sent to customers pretending to be from a trusted company.

GET MORE INFO

rpinfo@returnpath.net

1-866-362-4577

Phishing destroys trust in the email channel. *Fight Back and Protect Your Brand.*

Domain Assurance offers financial services marketers a new way to create a trusted customer email channel.

You spend a lot of time marketing to new clients, nurturing existing clients and building a strong brand image in the marketplace. Your main communication channel is email. Yet, customers do not trust that the email you send is actually coming from you, and for good reason. According to the Anti-Phishing Working Group, approximately 72% of all phishing attacks target financial institutions and payment services. The attacks are designed to imitate your legitimate emails and your website in order to lure your customers into giving up that personal information they think they are giving to you.

As phishing attacks target thousands of customers at financial institutions, the costs of these attacks can be high resulting in brand damage, customer attrition, loss of trust in the email channel, absorption of fraud costs, the reissuing of new credit cards and passwords, unwanted media exposure, and so on.

With 260 million fraudulent emails being sent to customers every day, how do you fight back?

Introducing Domain Assurance, a new anti-phishing service from Return Path designed to help financial institutions fight phishing on the front line of the attack – by blocking emails at the ISP gateway.

Protect your email channel. Protect your brand. Protect your customers.

Domain Assurance

Domain Assurance is a unique anti-spoofing and anti-phishing service that facilitates the **blocking of emails** pretending to come from your brand at the gateway of participating ISPs and mailbox providers around the world. Domain Assurance allows banks, financial institutions and payment services for the first time to proactively fight against this malicious activity and provide customers with a trusted channel for email communication.

Domain Assurance consists of two key components – the Domain Assurance Dashboard and the Domain Assurance Registry.

- **The Domain Assurance Dashboard:** The Domain Assurance Dashboard provides a holistic view into all email streams to ensure they are properly

authenticating. Although authentication – SPF and DKIM – unto itself is nothing new, organizations have difficulty monitoring all email streams going out from a particular domain and identifying whether or not these email streams are authenticating correctly. In addition, the dashboard provides visibility into possible phishing and spoofing attacks on your brand. Domain Assurance quickly and easily identifies any problem areas and allows you to protect your brand and ensure all emails being sent from your domains are authenticated.

- **The Domain Assurance Registry:** Once you are confident that all of your mail is set up correctly, you can request that your domain be published to the Registry to protect your brand from spoofing and phishing scams. The Domain Assurance Registry provides global ISPs with a trusted registry of authenticated domains for the primary purpose of blocking fraudulent messages and protecting customers from being phished. Emails purporting to come from your brand that fail to pass authentication checks are blocked at the gateway, which means they never reach the inbox or any other folder at participating ISPs. The Domain Assurance Registry helps to secure the email channel and protect your customer communication from malicious activity.

Domain Assurance allows you to:

- **Protect your email channel.** Stop fraudulent email activity on the front line of the attack by blocking phishing emails from ever reaching your customers.
- **Protect your brand.** Proactively protect your company against brand damage and fraud costs caused by spoofing and phishing attacks.
- **Protect your customers.** Maintain customer trust and loyalty by providing a trusted form of communication between you and your customer.

The Bottom Line

According to data from the Anti-Phishing Working Group, more than 300 brands are hijacked and over 30,000 unique phishing attacks are reported every month. Don't let fraudsters use your brand. Allow us to help you protect your customers and secure the email channel against fraudulent email activity at ISPs around the world.

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 increase inbox placement, improve industry 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 get your email delivered, engage with your customers and protect your brand against phishing. Call 866-362-4577 or email info@returnpath.net to get started today.

