



## GET MORE INFO

[rpinfo@returnpath.net](mailto:rpinfo@returnpath.net)

1-866-362-4577

## What's Inside:

Why DKIM is vital in 2010

- See Page 2

Latest about whitelisting

- See Page 3

Subscriber engagement is key

- See Page 4

## Email Delivery Imperatives:

### Responding Successfully to Emerging Trends in 2010

As we forge ahead in 2010, Return Path's decade of experience tells us that despite the rumors, email is neither dead nor dying. In fact, faced with the market challenges of 2009, businesses increased the volume of email they sent. Some marketers added social networking to the mix, but that didn't diminish their email marketing usage – it complemented it.

We're equally sure that spammers are "alive and well" – unfortunately. The volume of spam continues to climb—accounting for almost 95% of messages sent at one point in 2009.<sup>1</sup> As a result, Internet Service Providers (ISPs) are requiring senders to jump through new and better hoops in order to keep spam out and identify legitimate mail. To remain successful, email marketers must be prepared for these changes.

Return Path takes advantage of our strong relationships with Internet Service Providers to get their insights on emerging trends and what the implications will be for email marketers in the coming year.

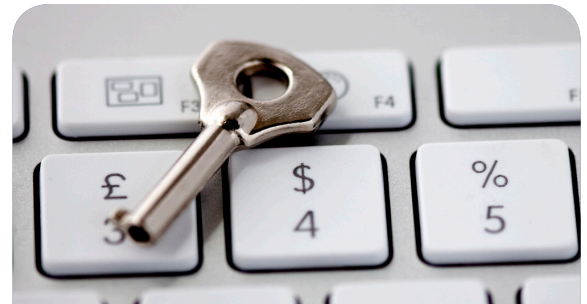
### Based on what we've gathered, we recommend that email marketers be prepared to:

- **Implement email authentication**, in particular, Domain Keys Identified Mail (DKIM), which will be increasingly important in getting your mail to the inbox. Authentication will also be key to protecting your brand from increasingly sophisticated phishing schemes.
- **Apply to get on a whitelist.** ISPs will be putting increasing emphasis on whitelists to identify mail from the "good guys" rather than screening out email from the bad actors. Whitelists may also determine which senders will be able to get access to feedback loops and other inbox benefits, such as images and links enabled by default.
- **Be ready for increasing focus by ISPs on user engagement metrics** that go beyond traditional clicks, open and conversions. Put your energy into improving new metrics such as the "not spam" rate and the rate of mailing to inactive accounts. Improve content relevancy and good mailing practices rather than increasing your email volume.

## Implement DKIM

DomainKeys Identified Mail is one more weapon for ISPs under attack from increased volumes of forged and malicious email. DKIM, one of the leading forms of email authentication, is a way of self-asserting ownership and responsibility for email sent to others. It uses public-key cryptography to authenticate the domain name that signed the message. This makes DKIM more useful than other types of authentication, where the best that can be done is to relate an email message to the IP address that sent it.

Return Path recommends that businesses use DKIM to sign their outbound email and protect their brand and domain reputation. As ISPs have to cope with more sophisticated phishing and spoofing and increasing levels of reputation hijacking and botnet attacks, they will be implementing the use of inbound DKIM verification and starting to filter mail based on domain reputation.



**Recommendation:** Use DKIM to sign your outbound email and protect your brand and domain reputation

### More Sophisticated Phishing Will Require Greater Diligence by ISPs

According to Wikipedia, phishing is “the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication”. In other words, criminals pretend to be trusted brands or senders by using the domains consumers recognize in the return address of email messages. An example is a message where a spammer impersonates a bank in order to trick the end-user into giving up account details, financial data or passwords to their account. Banks and financial institutions accounted for the majority of phishing scams in 2009, but social networks are increasingly being targeted. In 2008, there were virtually no Facebook phishing messages. Today, Facebook is on track to take the dubious distinction of the top spot in 2010.<sup>1</sup>

### DomainKeys Identified Mail (DKIM) and Domain-Based Reputation

DomainKeys Identified Mail (DKIM) is supported as one authenticity verification measure by major ISPs including Google, AOL and Yahoo!. Other ISPs have also confirmed with us that they are making big investment plans around DKIM. By using DKIM to authenticate your email, you can protect your company reputation and your customers against phishing. Since phishing depends upon the use of spoofed domain names, ISPs can easily sort out the legitimate mail sent from your domain from the forged phishing mail, since the forged mail will not be authenticated. Implementing and signing your email with DKIM ensures that an ISP can track your reputation distinctly – you get credit for your good mailing behavior and performance and the spoofed forgeries won’t count against you. ISPs may also block, throttle or otherwise interfere with other inbound messages that are not authenticated, even if they are not using spoofed names.

Many of the larger ISPs (including Yahoo!, Gmail and AOL) have already added domain-based reputation systems to their anti-spam systems. In addition to tying measures of sender reputation (e.g. “this is spam” complaints, spam trap hits, unknown user rates, “not spam” votes) to the Internet Protocol (IP) address, they now also tie them to the sending domain. Getting your mail through to the inbox for these ISPs will thus depend on having good emailing practices across all of the IP addresses from which you send email. With domain-based reputation, a single bad sending IP in your domain could tar the reputation of all of your IPs.

Some ISPs have not yet made the investment to add domain-based reputation into their spam filtering. In 2010 we expect more receivers and filtering companies will begin to accrue reputation at the domain level as increasing numbers of senders start using DKIM signing.

The use of domain-based reputation will have three primary advantages for senders:

- Senders can change IP addresses, add IP addresses or move to a new Email Service Provider (ESP), while still preserving their domain-based reputation.
- If a sender has had to change ESPs and is working to rebuild their IP reputation, domain-based reputation appears to be reducing that build-up period.
- Senders now sending from shared IP addresses will be less likely to “catch” a negative reputation from those with whom they share an address.

However, domain reputation systems won't be universal, nor will they all operate identically, so senders will still need to closely monitor their IP reputations as ISPs will be using both methods.

A good domain-based reputation, like a good IP-based reputation, comes from maintaining good sending practices: sending email that is wanted, expected, respectful and above all, relevant to your subscribers. Without good sending practices, your carefully authenticated domain reputation will suffer, and that battered reputation will interfere with the deliverability of all email you send.

## Get on a Whitelist

By getting on a whitelist, email senders can maximize their ability to get legitimate, permission-based email to the inbox of those who have requested it. ISPs are starting to emphasize methods for positively identifying “legitimate mail” and good senders rather than filtering out spam and passing the rest through. To do this, they are increasingly relying on whitelists, such as the Return Path Certification program.

Whitelists of IP addresses, email addresses or domain names tell an email blocking program or ISP “it’s okay to accept messages from these guys; you don’t need to filter them.” By using a whitelist, the ISP can avoid spam false positives that block emails the recipient wants to receive.

One of the most beneficial things about being on a whitelist is increased functionality for trusted senders. For example, in Return Path’s Certification program, images and links are automatically enabled by default at Yahoo! and Hotmail. There are also fewer restrictions and throttling limits so that senders can send email when and how they want it. Being on a whitelist doesn’t mean you can become complacent about your sending practices. The increasing emphasis on whitelists means that senders who do the right thing will be able to get more of their mail through to the inbox, but you need to continue your positive email practices to stay on the whitelist.



**Recommendation:** Get whitelisted and let ISPs know your “one of the good guys”

## Whitelisting May Become Important in Maintaining Access to Feedback Loops

Feedback loops let commercial senders monitor when users report their emails as spam. This powerful real-time feedback gives commercial email senders the ability to identify the messages users are complaining about, better understand why recipients are marking their mail as spam and fix the problems that are causing the complaints.

Right now feedback loops are generally available to all senders, which is somewhat problematic. Spammers with access to feedback loops are a nightmare for ISPs. They can verify legitimate addresses by dissecting the complaint data they receive, and continue to spam or sell lists of confirmed addresses. Alternatively, they can “list wash”, removing the complaining addresses from their lists and reducing their spam complaints. This gives the impression of a cleaner list, which drives ISPs to focus more on engagement to separate the good from the bad mailers.

Watch for ISPs to create stricter requirements for senders seeking to be on a feedback loop, so that only senders with good sending reputations will get the benefit of feedback data and reports. Because whitelists are the ultimate mark of good sending practices, being on a whitelist eventually could make it easier to get on, or stay on, a feedback loop. If you're not yet on a whitelist, it's time to seriously consider applying to the Return Path Certification program. The program grew significantly across the globe in 2009, and we expect to see continued growth as more ISPs implement the list in 2010.

## Keep Your Subscribers Engaged

Sending more email won't help you reach the inbox, but sending email with more relevant content will. It's a recurring theme in Return Path recommendations, and it hasn't changed: make sure you are sending your subscribers mail that they want to read.

As ISPs feel the weight of billions of non-legitimate messages, they are increasingly using engagement metrics to find the legitimate needles in the haystack. The new engagement metrics in use by ISPs go beyond the opens, clicks and conversions that marketers regularly rely upon for evaluating email campaign performance. For example, Yahoo! is tracking the time the email stays in the inbox before it is deleted. AOL has already announced enhancements to their whitelist to give greater benefit to those senders that maintain high engagement and low complaints. The metrics used are intended to measure overall subscriber engagement by looking at how much mail the client gets from you, whether subscribers are responding and how often the subscriber goes to their email account.

Be aware of the statistical measures, but focus on relevancy. Each ISP will have its own methods for collecting and interpreting engagement data, so a narrow focus on specific statistics may create problems for senders.

Other engagement metrics that the major email providers are already using to determine inbox placement, or plan to use in 2010, include:

- **“Not Spam” data.** When recipients check their spam folder and discover a message they want to receive, they can click “not spam.” That tells the ISP that the message is relevant and desired. If your subscribers really want your email, they'll vote it back to the inbox.
- **Reliability of reporter data.** It's possible for senders to game the system by setting up fake mailboxes and voting their own mail back to the inbox, but ISPs have found ways to stay ahead of this. They adjust for users who are



**Recommendation:** Engage subscribers and turn email delivered into email revenue

overzealous in voting everything as spam or everything as “Not Spam”. As a result, only the data from reliable reporters are calculated into engagement measures.

- **Panel Data.** Microsoft and Gmail use panels of real subscribers who are asked to verify the appropriateness of inbox or spam folder placement for random messages sent to them. The use of panels may grow, as it is very hard to cheat this data.
- **Inactive accounts.** Beware if you send a lot of mail to users who haven’t logged into their email account for long periods. This indicates to ISPs that you could be trying to reduce complaint rates by not removing inactive accounts, or that you have issues with list maintenance and quality. By keeping these email addresses on your list, you lower your “Not Spam” rate and reduce your chances of moving out of the spam folder. You also lower your engagement factors - to improve engagement, ensure that you are only sending email to active customers. While it is impossible to know if your subscribers have logged into their email account, you can use the open and click data available to you to remove subscribers who are not viewing your mail.

Sending more email or creating more email programs to send to the same subscribers isn’t going to increase your email ROI. Instead, shift your focus to being sure that you are sending email that is highly relevant to each subscriber, at their preferred and expected cadence. Pay increasing attention to the type of permission you have from your subscribers and the types of messages they want to receive. Bottom line – when you establish a relationship with your subscriber through opt-in, clearly set expectations on content, frequency and value, then meet that expectation!

## Conclusion

As you charge ahead in the coming year and begin a new decade, it will be more important than ever to do what it takes to become a trusted sender. Authenticate your email with DKIM, take action to get whitelisted and resolve to keep your subscribers engaged with your emails. By following best practices and continuing to create relevant messages, you will get your email delivered.

### The 2010 Email Imperatives:

- **Implement DKIM**
- **Get Whitelisted**
- **Engage Subscribers**

## About Return Path

Move your email program from ordinary to extraordinary by boosting deliverability, subscriber engagement and response. Return Path works with both ISPs and email senders to make sure consumers get the email they want. We provide data to ISPs to help them separate good email from spam and we offer commercial senders visibility into their email deliverability. Our tools and services give senders the insight and resources to diagnose and prevent email deliverability and rendering failures by improving and maintaining their email sending reputations. This paper was developed by Return Path’s Receiver Services team and based on the strong relationships with the world’s largest Internet Service Providers. For more information about how Return Path can help improve your email program, visit us at [www.returnpath.net](http://www.returnpath.net), email us at [rpinfo@returnpath.net](mailto:rpinfo@returnpath.net) or call us at 1-866-362-4577.

## Resources Cited:

1. “1 Billion Spammers Served.” Project HoneyPot. December 15, 2009 <[http://www.projecthoneypot.org/1\\_billionth\\_spam\\_message\\_stats.php](http://www.projecthoneypot.org/1_billionth_spam_message_stats.php)>