

Reach the Inbox

Steps to get on the good side of ISPs and boost your e-mail deliverability

When it comes to e-mail deliverability, there is only one way to ensure success: Build a good reputation. The perception ISPs and other receivers have of the mail sent by your mail servers determines whether or not your e-mail stays clear of spam filters and gets delivered to the inbox. Unfortunately, most marketers don't have a clue where to start when it comes to determining delivery issues, much less figuring out what ISPs think of them.

There are two sides to e-mail delivery: the pre-campaign best practices that build your reputation, and the ongoing management necessary to track delivery rates and potential problems. The following five steps consider the primary factors of each. Follow these tips and you'll see more of your e-mail reach the inbox—and get higher response rates as a result.

1. Prevent Complaints

When your customers or prospects hit the “this is spam” button or report your e-mail to abuse queues, ISPs take notice. It's critical you know whether you have complaint issues—and how to fix them, if you do.

1. Prevent Complaints

When your customers or prospects hit the “this is spam” button or report your e-mail to abuse queues, ISPs take notice. It's critical you know whether you have complaint issues—and how to fix them, if you do.

The best way to prevent complaints is to take care in setting up your e-mail program from the start. Get permission—preferably by asking twice—before mailing to customers. Make it clear to subscribers what they will get from you and when. Be consistent in



your communication. And above all, make your content extremely relevant. By mailing things your customers want, you can keep your complainers to a minimum.

Following e-mail best practices, while important, still is not enough. You also need to monitor your complaints so you can see what the ISPs see. Here are three areas to monitor that will reveal if complaints are hurting your reputation.

■ **Customer support**—Your own customer support e-mail boxes and any auto-reply addresses can show you which e-mails are offending customers. A surprisingly large number of subscribers will reply to the e-mails you send with complaints about the e-mail, or in an attempt to unsubscribe—so open those replies and read them. Also, register your abuse addresses with www.abuse.net. This site is a directory of where to contact a sender about abuse

complaints. Many abuse desk administrators at ISPs and system administrators at smaller systems use this Web site to determine where to send complaints.

If you want to source more complaints—and you do—advertising where to send them on abuse.net is a helpful step.

■ **ISP feedback loops**—When people complain about your e-mail to their ISPs, that data often is captured in a “feedback loop.” AOL, Microsoft, United Online (including NetZero and Juno), EarthLink and others currently provide that information to marketers. Several of these ISPs do so in the new “Abuse Reporting Format,” or ARF, which standardizes the data elements in feedback loops, making it easier to machine parse.

■ **Reputation scoring**—An e-mail reputation management system can help you track complaints and report complaint rates by major ISPs and at the campaign level.

By looking at your complaints, you can see who is complaining and what content drives complaints. By running a complaint analysis, you specifically can determine what drives complaints, i.e., co-registration partners, creative. By fixing those things, complaint rates lower and response rates rise.

By looking at your complaints, you can see who is complaining and what content drives complaints. By running a complaint analysis, you specifically can determine what drives complaints, i.e., co-registration partners, creative. By fixing those things, complaint rates lower and response rates rise.

2. Get Authenticated

Many marketers' eyes gloss over when talk turns to the technical side

(continued on page 42)

(continued from page 41)

of e-mail. It's OK to let your technical team worry about much of it, but it's vital that your program uses an authentication protocol.

Most ISPs now require e-mail senders to use some form of authentication to ensure delivery—think of it as caller ID for e-mail. If an ISP knows you are who you say you are, you're more likely to get delivered. E-mail authentication has two primary benefits: it prevents the forgery of e-mail messages and allows senders to build a positive reputation with receivers based on their mailing behavior.

If you're not using an e-mail authentication protocol, you need to research which tool is right for you and get started. You can find detailed information about the three dominant schemes on the following Web sites:

■ **SPF:** www.openspf.org/wizard.html.

■ **SenderID:** www.microsoft.com/senderid.

■ **DomainKeys:** <http://antispam.yahoo.com/domainkeys>.

Make sure that when you implement authentication, you do so for all of your corporate e-mail—consider e-mail you send internally, through third parties, transactional e-mail, marketing e-mail, etc. Once you have all your e-mail sources authenticated, test your records to make sure they are set up correctly.

Some easy-to-use e-mail authentication testing resources include:

■ **Return Path's SPF/Sender ID Validator:** Visit senderid.returnpath.net.

■ **Port25's e-mail Relay:** E-mail

■ **Return Path's SPF/Sender ID Validator:** Visit senderid.returnpath.net.

■ **Port25's e-mail Relay:** E-mail check-auth@verifier.port25.com.

■ **DNSstuff.com SPF Tester:** Visit www.dnsstuff.com/pages/spf.htm.

■ **The SPF Project:** Visit www.openspf.org/why.html.

■ **Gmail:** Send e-mail to a Gmail account, login, view message, and view the header. Look for the "Received-SPF:" line for the result of its SPF check on your e-mail. Visit www.gmail.com.

■ **Yahoo!:** Send e-mail to a Yahoo!

account to check DomainKeys signatures. Yahoo! also will display to the recipient in the user interface when the signature is valid. For more information on DomainKeys at Sourceforge, visit <http://domainkeys.sourceforge.net>.

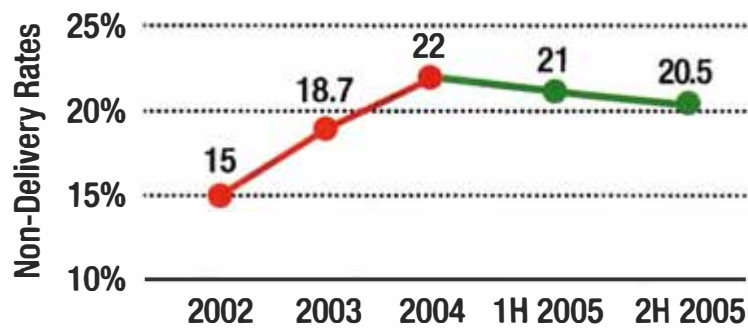
In addition, there are a wide variety of other infrastructure tests ISPs use to determine whether to accept mail from your outbound mailer server. The most common is to check whether the mail server has what is known as a reverse domain namesystem or "reverse DNS." This can be used to determine if the e-mail message is coming from

tool, this will help you see how your e-mail will look to readers, what links are broken, and whether your creative is likely to get filtered. By seeing these things up front, you can fix problems before they reach your customers—or their junk folder.

4. Keep Your List Clean

One of the simplest ways to improve your e-mail deliverability is to make sure you have a clean e-mail file. With 40 percent or more of your list degrading each year with e-mail changes and data entry errors, your list can be one of the more detrimental elements of

Email Non-Delivery Trends, 2002-2005



Source: Return Path

The percentage of e-mail that has been erroneously blocked by spam filters has declined slightly since 2004, largely because of marketer awareness of deliverability issues and better filtering by ISPs.

the domain name indicated in the message header. A good test tool for reverse DNS can be found at www.dnsstuff.com.

message header. A good test tool for reverse DNS can be found at www.dnsstuff.com.

3. Conduct Pre-campaign Creative and Delivery Testing

By testing your campaigns before you send them, you can dramatically improve response rates. Everyone knows this, but instead of only conducting creative testing to gauge customer preferences, consider doing tests that gauge your delivery potential. Whether you do so manually, or by running your campaign through a pre-campaign

your campaign when viewed by ISPs. When you have high unknown user rates—meaning, a high percentage of your file comes back as non-deliverable because the accounts are non-existent. When you have high unknown user rates—meaning, a high percentage of your file comes back as non-deliverable because the accounts are non-existent at the ISP—you look like a spammer.

To ensure your files are clean:

■ Use consistent bounce algorithms to make sure you remove bad e-mails from your file regularly.

■ Run your file through an e-mail change of address service to ensure you have the most current e-mail addresses for your customers.

■ Process your file through a list hygiene service to make sure your list is free from common data entry

errors that render e-mail addresses incorrect.

- Require double entry of addresses for accuracy.

- Make sure addresses comply with ISP standards.

- Send a welcome message and pull bounces off immediately.

When your list is dirty, you also open yourself up for “spam trap” filtering. A spam trap address is one that has never belonged to a real person, so e-mail that goes to it is assumed to be unsolicited. Some ISPs are now using abandoned e-mail addresses as spam traps, as well. By sending e-mail to customers at ancient addresses, you open yourself up for trouble. To avoid this problem, purge your list of people who have not responded to your e-mails in a realistic amount of time. You’re not losing a valued customer—and you will mitigate the risk of being blocked by key ISPs.

5. Monitor, Monitor, Monitor

The more information you know about how your campaigns perform, the more likely you are to make the continual improvements that result in higher delivery and response rates. You can set up your own tracking system, or you can use one that is readily available.

Ideally, your delivery monitoring should track:

- Rates of e-mail to the inbox, spam folder or missing outright across the primary ISPs (domestic and international, if you have international customers);

- Filtering rates in B-to-B environments; and

- Delivery rates by campaigns sent.

Delivery today hinges on your reputation, and every e-mail you send helps build—or break—that reputation.

Make sure everyone in your company who sends e-mail understands the importance of following best practices and taking the high road. Your response rates will be all the evidence you need to convince them. ■

George Bilbrey is the general manager of delivery assurance for New York City-based e-mail delivery assurance and whitelisting services provider Return Path Inc. He can be reached at (212) 905-5500.

Looking for more on E-mail Marketing?

For more resources on e-mail marketing—including an article on multivariate e-mail testing by E-Dialog’s Michael Wexler—visit the E-mail Marketing Online Community at www.targetmarketingmag.com.