The Opt-In Email Marketer's Checklist for Inbox Delivery

1. __ Use a static IP address.

Whether you use software or a hosted/ASP solution to do your email marketing, make sure your email marketing server uses a static IP address. Unlike a dynamic IP address, a static IP address generally stays the same and is analogous to having a consistent phone number or physical address—it tells ISPs and the world at large that you're stable, that you've been around, and that you plan on being around in the future. A lot of companies still believe they can't afford static IP address, but fortunately—that's no longer true. They're very affordable these days.

2. __ Ask a few key questions.

Whether you use software or a hosted/ASP solution to do your email marketing, your delivery rates can be affected by the behavior of others around you. Even if you're adhering to the most ethical email practices in the world, it won't do you very much good if your email is sharing bandwidth with a spammer or if someone in a different department of your organization is sending out email that doesn't comply with spam laws. Here are some questions you should be asking if you really want to get your email through to the recipient's inbox:

- Does your hosted provider screen prospective customers in any way before signing them? Some type of screening process is a good sign that an ASP is being selective and making an attempt to steer clear of spammers. Questions usually relate to the type of email that will be sent, as well as the nature of the lists in use (opt-in, rented, etc.).

- Will your hosted provider provide you with a fixed IP address? If they don't, it could mean that they rotate or "round-robin" IP addresses among all their clients which can have a negative impact on delivery rates for your email. You should also ask what kind of relationships they have with major ISPs, as well as what procedures are in place to resolve delivery problems.

- How do email sending practices differ among departments within your own organization? Even if you don't use a hosted service, it's a good idea to make sure that other divisions within your organization are using best practices for sending. Make sure everyone is on the same page, so your mail doesn't get blocked as a result of another department's mistakes. To help organizations understand good sending policies as well as current spam law, Lyris has developed an email best practices guide which is available here:

  http://www.lyris.com/resources/whitepapers/bestpractices

3. __ Make sure your DNS entry is complete and correct.

Because DNS is such an important way of establishing identity on the Internet, spammers will often forge domain names or IP addresses to hide where their mail is coming from. To detect these forgeries, ISPs perform a reverse DNS lookup on incoming messages. This type of lookup takes the IP address that's trying to make the connection and checks to see if there is a registered domain associated with it. If it doesn't match, the message may be a forgery—or, the hapless sender may have an incorrect DNS entry. In either case, the ISP will most likely treat the message as spam.

You can help ISPs verify your identity by making sure that your DNS entry is complete and correct. To make sure your domain has all the correct entries, you can use a web site like the one below. If you have questions, work with the person or department responsible for your domain to understand what changes may need to be made.

http://www.dnsreport.com

4. __ Publish an SPF record for your domain.

A newer form of authenticating incoming email is SPF, or Sender Permitted Framework. In a nutshell, SPF is just a single line within your DNS entry that identifies which IP addresses are approved to send email for your domain. You may have heard a bit of buzz about SPF recently due to Microsoft's recent decision to implement Sender ID on all Hotmail accounts, so it's a good time to make sure you're all squared away on this issue. Taking the singe step of checking the existence and/or accuracy of your SPF record can have positive deliverability payoffs, both now and in the future.

Recommended steps for senders:

- Determine the IP address(es) of your email marketing server(s) by contacting the responsible IT representative within your organization.

- Make sure that the IP address(es) of your email marketing server is a published part of your public SPF record. Many senders publish the IP addresses of their own company's internal email server in their SPF record, but neglect to list the IP addresses of their email marketing server in that record. For maximum deliverability, your organization's SPF record should contain both sets of IP addresses.

- If you haven't already published a full SPF record for your organization, do so as soon as possible. The process of publishing an SPF record is relatively easy, and there are several free tools available to help you do so, like the two listed below. Again, make sure that your email marketing server's IP address(es) is also a published part of this record.

- Tool #1: http://www.spf.pobox.com/wizard.html

- Tool #2 http://www.anti-spamtools.org/SenderIDEmailPolicyTool/Default.aspx

5. __ See unsubscribes as a good thing.

Processing email to erroneous addresses uses up valuable ISP resources, so they quickly lose patience with senders who repeatedly mail to a high percentage of "dead" or non-existent addresses and may start blocking or quarantining your campaigns as a result. So if someone unsubscribes from your list or their address bounces twice, sacrifice that recipient to the cause of greater deliverability: set your software or service to automatically remove or separate the email address from your lists after a couple of failures. If a high percentage of bad addresses or unsubscribe requests seem to be coming from one ISP in particular, you can look into it further by contacting that ISP, but don't keep sending to the bad addresses until you get further clarification.

Of course, no sender ever wants to lose an address, but when one turns bad or a recipient asks to stop receiving mail, it can actually be a blessing in disguise. By removing bad and unsubscribing addresses quickly, your lists are kept populated with recipients who actually want to receive your mail, which isn't just great for delivery rates—it's great for response rates too.

6. __ Keep an eye on delivery rates at individual ISPs.

If a domain with previously high deliverability rates suddenly shows a large number of non-existent users, it could be that the ISP has started to see you as a spammer for some reason and is trying to make you go away. Some ISPs try to do this with deceptive transactional messages that say recipients no longer exist—even when they do. Whether or not this is an effective tactic on the part of ISPs (do spammers really remove inactive addresses?), it can have very real, negative effects on conscientious senders who are unwittingly removing these addresses—believing that they no longer exist.

On the other hand, a 100 percent success rate at a certain ISP may signify a problem as well. Instead of giving useful (or even deceptive) non-delivery notices, the ISP could be just accepting all of your mail and then dumping it in a bulk folder—or simply deleting it without forwarding it to recipients at all. If a domain has more than a hundred addresses, you really should be seeing at least a few failed deliveries from time to time. If you don't, check to see if there are any actions from recipients at the domain in question. Are there any opens or clickthroughs at all? If not, it's probable the mail isn't getting through.

If you spot a problem, take action! Delivery problems can be frustrating for legitimate marketers, but fortunately there are a number of things you can do to resolve them:

- Slow your sending speed. It's possible that you're sending too quickly for the recipient mail server to respond.

- Perform a deliverability audit. Deliverability services like EmailAdvisor by Lyris are designed specifically to help legitimate senders know whether or not their email is getting through to the inbox at a multitude of major ISPs. Delivery problems are highlighted via an easy, color-coded system, and a number of other tools—legibility checkers, content checkers, blacklist monitors—are designed to enhance overall performance of your campaigns as well. If you'd like to try a test audit, contact us at 800-485-9994 and ask about the EmailAdvisor Service.

- Change the format of your mail. If you're sending in HTML, try sending plain text.

- Send an email to the technical contacts for that domain. Show them you're responsible and ethical, and they are likely to let your mail through. They may also have suggestions on how to improve your email practices as well.

- Enlist the help of your recipients. If the technical contacts for a domain are unresponsive to you, they may listen to customer complaints.

7. __ Test your content.

As a list owner, you may have experienced first-hand the frustration of seeing your opt-in mailing being inappropriately blocked by an anti-spam filter. Combat these "false positives" by checking your message before you send it with Lyris' free content checker, located here:

http://www.lyris.com/resources/tools/contentchecker

8. __ Test for legibility.

With more than 35 major email clients in use by recipients today, legibility has officially become a part of the overall email delivery issue. At Lyris, we see email messages every day from major brands that are broken or rendering improperly in certain email clients, so we highly recommend that you test your messages on multiple email clients before you send or use a service like EmailAdvisor by Lyris to see how your messages will appear in multiple email clients. Remember, if your email arrives in the inbox but looks broken or isn't legible, it's actually worse than if it never arrived at all. In a recent Lyris study of 100 consumers, 70 percent identified broken and badly rendering emails from major brands as the most likely to be fraudulent—even over actual phishing scams.

9. __ Use a professional email marketing solution.

This one will sound obvious to most readers, but we'll state it anyway: the first step towards successful commercial email delivery is to use a professional, dedicated software application or hosting service. The days of using a desktop email client and sending a "CC" or "BCC" message are long over; even if you only have a couple hundred people on your list, don't do it! Sign up for a monthly service that offers proper list management, and you'll be much more likely to see good results on list growth, and response and delivery rates over the long term.

If you use a hosting service, or are in the process of selecting one, again—make sure you confirm that the ASP requires all of its clients to follow industry best practices. Ask about the service's blacklist record: when was the last time they were blacklisted and by whom? Why were they blacklisted in the first place, how long did the block last, and what did they do to resolve it?

10. __ Respect the recipient.

At Lyris, we call this the "Master Practice" because it works best when it permeates every other email practice that you employ. What's so worthwhile about respecting each and every recipient on your list is that it tends to work in your favor as well. A well-timed, well-crafted email is much more likely to accomplish your goals than a steady stream of opportunistic, impersonal, or out-of-context message. These will not only fail to capture the recipient's interest, but they may actually cause recipients to start clicking the handy "this is spam" button in their client—even if they did ask to receive your mail. Over the long term, such complaints will not only negatively impact your email delivery, it can do damage to your organization's brand and reputation as well.

Permission is no longer a one-time event in the email arena; recipients may decide your mail is unwanted at any time. By sending messages they find relevant, interesting and valuable, you ensure that your emails will be welcome, even anticipated, in the recipient's inbox—which may just be the biggest delivery advantage of all.

Founded in 1994, Lyris Technologies provides advanced software and services for email marketing and email delivery. Lyris' solutions are available as software or as hosted applications and are used by more than 5,000 customers worldwide, from Fortune 500 corporations to fast-growing startups.

LYRIS

Lyris Technologies, Inc
5858 Horton Street, Suite 270
Emeryville, CA 94608

USA and Canada: 800-768-2929
International: +1-510-844-1600
Fax: +1-510-844-1598

email: sales@lyris.com
www.lyris.com