

10 Important Rules to Improve Email Deliverability

Hello, and welcome to the first issue of SEO MixTour in the year 2010! We've dedicated this issue to common email deliverability concerns to offer you a list of rules based on CAN-SPAM Act principles, best practices of email service providers and our own experience. Remember, as the creator of Web CEO, a SEO product used by many small business owners, we are deliberately dwelling only on deliverability practices that they can manage themselves.

As you create an email message, then send it and analyze delivery results, remember to stay focused on the following primary concerns.

- **To whom do you send your newsletter?** If you care about your subscribers and your reputation, send messages only to those people who really want to read it. An [opt-in email list](#) will solve unwanted email problems 90% of the time because your message is unlikely to be marked as SPAM. If you offer your site visitors a chance to subscribe to your newsletter, make sure it is a confirmed subscription.
- **Review your 'From' and 'Subject' fields.** The 'From' field should contain your company's name and/or the title of your newsletter. This helps subscribers to recognize your messages immediately. Upon receiving your message, the reader should be able to answer, "Yes" to the question, "Do I know who this is from?" Likewise, your 'Subject' field must include an attractive title. Choosing the right 'Subject' line is really important because it often determines whether your messages are opened or not.
- **Control your message content.** Make sure that all of your emails include current contact information, including phone numbers, email addresses and even your physical address. Check to see if any words in your subject line or message text trigger SPAM filters. You can see a list of the most popular [SPAM triggers](#) by Mequoda. In addition, Lyris offers a free service to [check your message content for SPAM triggers](#). Nowadays, ISPs use smart SPAM filtering systems, so you shouldn't avoid every potential SPAM content word if it is an important part of your message. Though their usage can add SPAM signals to your email, if your message does not score a critical number of such SPAM signals, your email likely won't be filtered. Don't be afraid to use a few common SPAM triggering words if your message will really benefit from them.
- **Use only absolutely necessary graphics in your message.** Spammers and legitimate email marketers alike use loaded images as a metric – to check valid email accounts and calculate open rates. As a result, email programs and web-based services don't download images by default. This means your readers won't see your images unless they click on an option to "display images" in your message. While you shouldn't overload your message with images, if you insert some relevant text into the 'alt' attribute of the image, there's a chance that it will be downloaded by potential readers and your newsletter will be read.
- **Do not attach files to your message** – most savvy Internet users will consider files sent via email too suspicious to open. A better idea is to use a Web link (be sure to check its availability before you send your message!)
- **Deliver a perfect user experience with your newsletter** – make sure your newsletter layout is rendered perfectly by all important Web-based email service providers and email clients.
- **To ensure compliance with the CAN-SPAM Act, your newsletter must be "opt-out."** In other words, be sure to include a valid 'unsubscribe' link in your message. Your unsubscribe requests should be honored immediately. What's more, consider making your unsubscribe page look more like a landing page. Lyris offers a [comprehensive article to help you do this](#).
- **Subscribe to feedback loop services with all important email providers**, such as [Yahoo!](#), [AOAOL](#), [MS HotMail/Live](#), [Comcast](#) and others. Take care to process any abuse emails

r
e

gularly and quickly.

- **Maintain your subscriber list to keep your unknown user rates down.** Regularly remove undeliverable addresses that bounce because ISPs and ESPs track bounce rates and may punish your IP if you repeatedly attempt to deliver messages to closed or non-existing subscriber mailboxes.
- **Be sure to test message delivery from your domain with all the major Email Service Providers (ESPs).** Testing deliverability is easy – create test emails and send your messages to them. You'll see at once if your messages end up in SPAM folders. If you find an issue, try to solve it. Check to see if your domain is present on any known blacklists that ISPs use (www.mxtoolbox.com or www.blacklistalert.org and similar services). If you've been blacklisted, get in touch with the company that maintains the blacklist and follow its instructions to be removed. Another way to avoid blacklisting status is to contract with an email reputation service in order to add your IP addresses to various trusted lists. The most popular email reputation services are:

ReturnPath (www.returnpath.net, www.habeas.com)

SuretyMail (www.isipp.com, www.suretymail.com)

GoodMail (www.goodmail.com)

Our experience has taught us that subscribing to any of the above reputation services makes sense only if you are really a bulk email sender. Otherwise, adhering to the other smart email practices described here should be enough to ensure you maintain email marketing deliverability and success.