Email Deliverability – Best Practices for Getting to the Inbox

Best practices in email marketing constantly evolve to reflect ever-changing online behavior. It’s important to stay current with the latest email protocols in order to optimize campaign effectiveness and maintain the most positive relationship with your campaign recipients.

The following is a list of things that you might consider avoiding when creating and sending your email messages. Staying away from these “Don’ts” will help you make a more positive impact in your recipients’ inboxes.

DON’T:

- Link to “executable” files like .exe, .zip, .swf, etc. This is likely to cause your messages to get marked as a “phishing” email by spam filters, and placed in the Spam folder or even quarantined.
- Use JavaScript in your content. Most email clients will block JavaScript or strip out that code entirely. As a result, your email may not display as intended and could even be placed in the Spam folder or quarantined.
- Link to external stylesheets – most email clients will block them.
- Use loud colors in the email body text, such as pure red or green. This can come across as “yelling” at your recipients, trying to attract their attention to an area of your message, which is something spammers tend to do.
- Use all capital letters in the subject line or overuse them in the body of the message (same reason as above).
- Use exclamation signs or other punctuation marks more than once (same reason as above).
- Use excessive symbols – use descriptive words instead. When you use dollar signs, make sure you don’t overdo it ($$$).
- Use the word “test” in the subject line, or “dummy” text, like Lorem Ipsum, in the body of the message, even when sending a preliminary version of your message for review. Both could cause your message to go to the Spam folder.
- Use spammy words or phrases unnecessarily, like “mortgage”, “act now!”, “click here!”, “limited time”, and “guaranteed”. 
• Get “creative” with your spelling, like “FR33”, “m0rtgage”, “MON3Y”, etc., especially in the subject line. Spammers do this to try and trick Spam filters, so they’re programmed to look for them.
• Use the word “Dear” when addressing your recipients, as in “Dear Reader” or “Dear Mary”. This will increase your Spam score.
• Display full URLs in the body of the HTML version of the message. Instead, use a text string like “visit our website” that includes the HTML link underneath it in an anchor tag.
• Use a domain in your message content that’s blacklisted. You can use a site like http://mxtoolbox.com/supertool.aspx to check whether a domain is on a blacklist.
• Use ‘Re’ or ‘Fwd’ in the subject line to trick recipients into thinking that your mail is a continuation of a previous conversation. NOTE: Using a misleading subject line is a violation of CAN-SPAM and other Spam laws.
• Offer misleading or unsubstantiated claims in the subject line or message.
• Use bad/broken HTML coding in email. You can validate your code online: validator.w3.org/.
• Convert Microsoft Word files to HTML – even the best conversion tools could miss some of Microsoft’s proprietary or hidden tags, which could cause your messages to be displayed incorrectly, or even get them mistaken as a phishing message or placed in the Spam folder.
• Use a single, large image in your message. This practice is used by spammers to hide their content from Spam filters. Aim for 60% or more text and 40% or less images, and break larger images up into at least two smaller images.

DO:

• Include a “Friendly From’ label along with your ‘From’ address. For example, “Jim’s Online Hardware” <email@ jimshardware.com>. Messages from unknown/unrecognized senders are more likely to be reported as spam.
• Use your company’s domain in your ‘From’ address, and authenticate your messages (SPF/DKIM/DMARC) with your company’s domain as well. This will make your messages more recognizable to Spam filters and your
recipients, give your messages legitimacy, and greatly reduce the chance that they will be seen as a phishing attempt.

- Keep your message size under 100kb, especially for recipients who read messages on a mobile device. That’s not a hard and fast size limit, just a reasonable target to shoot for.
- Use the same/similar text in both the HTML and Text versions of your messages. Spam filters look for this.
- Ensure that the design of your email templates clearly identifies your brand and/or website. Prominently display your logo/brand and/or company name, and use your website’s color scheme so that your recipients immediately recognize who they’re from.
- Ensure that all the images in your message have alternative (alt) text in the image tag so that something descriptive is displayed in their place when they’re not rendered.
- Ask you members to whitelist emails from your chapter email address (updates@chaptername.asse.org – ie updates@chicago.asse.org). Members using their business accounts might need to ask their IT department to perform this task. Members using a personal account like (gmail or yahoo) can simply add the address to their contacts list.

Implementing these tips is not only critical in terms of getting your messages through Spam filters, but it will organically help improve your relationship with your recipients, as well.