

# **DON'T BE AN ACCIDENTAL SPAMMER**

## **Best Practices for Permission Marketers**

Email “spam” is in the eye of the reader—one person's valued information may be another person's spam. You know your list is truly opt-in, but people are so sensitive these days that you risk being branded as a spammer even if you believe you've done nothing wrong. Even if your email is welcome, you run the risk that it will be caught by a spam filter somewhere in the communication chain, and never even reach your subscriber's inbox.

So what's a poor marketer to do? Use common sense and follow these guidelines to reduce the likelihood that your email is perceived as spam or stopped by a spam filter. Your readers will thank you. Your ISP will love you. You'll also protect your reputation and your brand.

### **1) Renting email lists**

- a. NEVER ever be tempted to buy an email list or CD of names for a small amount of money – you've seen the offers; ‘ONE MILLION ADDRESSES for \$99!’. These are guaranteed to be email addresses collected without permission. The same goes for any software that claims to collect or harvest email addresses. Just say NO!
- b. Never gather email addresses off the Internet. This includes chat rooms, addresses posted on websites or any other publicly listed email addresses. Never ever use an email harvester.
- c. If you are renting a list, do a lot of due diligence on the list provider. Check their opt-in practices very carefully, and make sure the list is not 3<sup>rd</sup> generation (i.e., they opted in to a list you bought from a now-dead company) or too general (i.e., they opted in to get information on “technology” as opposed to “email marketing software”). Ask for a spam guarantee—if you get any complaints, the list and/or mailing is free.
- d. If you have any suspicions at all about the list you've just rented, try a very small campaign first just to be certain you haven't been fooled. Your reputation is too important to risk on a large mistake.

### **2) Building your list: opt-in is better than opt-out**

- a. If you use the “opt-out” method of collecting permission (i.e: you will get our emails unless you tell us you don't want them), you run a greater risk that some people will be annoyed. “Opt-in” (where they overtly tell you they want to hear from you) is a better process to use to collect permission.
- b. Send a confirmation email when someone joins your list. It is good manners and it will give people an opportunity to respond before they start getting emails from you on a regular basis. This is especially useful if they've been signed up by a someone else. In the confirmation email, tell them from what address the emails will be coming so they can update their filters – ie: “You will be getting this newsletter from YourCompany's Customer Support, if you use filters, please add this address to your whitelist.”
- c. Better yet, use a double opt-in subscription method, where people must reply to a confirmation email before they can be added to your list. That way, you'll know they entered a valid email address—and if they tried to sign someone else up without permission, that someone can simply disregard the email.
- d. Even if they've opted in, their email system may be set up to stop you with a challenge response. If you are not on your reader's personal “whitelist”, every email you send will send back an acknowledgement request that must be returned by a real person. Sadly, its almost impossible for email delivery software to respond so you must do these manually and avoid them by asking readers who employ this system to add you to their whitelist. Being whitelisted will avoid the need for the acknowledgement in future mailings.

- e. Be wary of appending email addresses to your list of postal addresses. 82.5% of consumers do not think a mailer who has their postal address on file "has the right to send me email."

### 3) Remind the reader of your relationship with them

- a. Tell people up front, at the beginning of the email, why they are getting your email. Example: "You are receiving this email because you recently purchased a gas grill from us, and we'd like to make you this special offer." Put them immediately at ease, remind them of their relationship with you, and the rest of your message will be read from a completely different perspective.
- b. If they did not opt in to you directly, tell people how you got their email address. Example: "You are receiving this email because you signed up to receive special offers from partners of ABC Company," or "We got your email address from a rental list owned by ABC Company." That way, if they do think it's spam, they'll know who the real spammer is.
- c. Even if people did subscribe to you directly, sometimes they forget. A simple reminder is always a good idea. Example: "At the CRM seminar you recently attended in New York, you asked us to keep you up to date on new products and services via email."
- d. Tell them the email address they used when they subscribed. Example: "You subscribed to this newsletter as [abc@gotmarketing.com](mailto:abc@gotmarketing.com). Ask them to send unsubscribe requests from that same email account.
- e. Your 'from' field should also reflect your relationship with your reader. If you've been using your company name, don't suddenly stop. Many people prefer to get email from a person (probably because it looks less like spam), so take time to consider what your readers might like to see... better yet, ask them. Also, if they've set up their filters to let email from your 'from' field through their filter, changing this field may trigger the filter to block you.
- f. Avoid using only a first name in the From field, especially a woman's first name. It's harder to recognize the sender without a last name. Because mail from Tammy, or Cindy or other women's names is increasingly associated with spam, many readers are doing a fast delete on all these emails without opening them.
- g. Don't falsify the sender's domain name. If you aren't eBay, don't say the email is from eBay. This is worse than bad, it's illegal.

### 4) Let them leave if they want to.

- a. ALWAYS put an unsubscribe option in every email. Put the unsubscribe instructions in plain view. Don't try to hide them.
- b. Make it easy to unsubscribe. Include both a one-click link to unsubscribe and an option to reply with "unsubscribe" in the subject. The former makes it easy if they are online, the latter makes it easy if they are offline and want to save their request for later uploading.
- c. Encourage them to use the unsubscribe button rather than the Report as Spam button. This will help you understand who simply wants to leave and who is really not happy with your mailing.
- d. If people do unsubscribe, honor their requests. It's reasonable to send one more email confirming that they want off your list, but after that, you're a spammer. Don't risk it.
- e. Think of all the ways that someone could ask to be taken off your list(s). They might contact your call center, go through your ISP, send a letter. Make sure your company has a process in place to funnel these requests into your list management system.

- f. Increasingly, people expect that their unsubscribe requests will be honored instantly. Try to process all unsubscribe requests as quickly as possible, but certainly not more than 3 days from the date of request. If you just can't do it that quickly, tell people how long it will take.

### 5) Manage frequency expectations ahead of time

- a. Tell them what to expect from you in future mailings. Is it a periodic update, a weekly newsletter or a one-time promotional offer? Once a month may be “just right” for some, “too much” for others. Let them decide before they get overwhelmed—and annoyed.
- b. If you just started building a list but aren't exactly sure how you're going to use it yet, include a field in your opt-in form that asks, “How often would you like to receive email from us?”
- c. If you haven't mailed to your list for longer than 6 months, chances are that most people on this list will have forgotten who you are or that they ever gave you permission to mail them. Your best bet is to send these people a request to re-opt-in – asking them for permission all over again.

### 6) Make it easy for them to contact you

- a. Include your contact information in the email. Put a link directly to your “contact us” page on your website, or better yet, include a street address and phone number directly in the email text.
- b. Make sure that [postmaster@yourcompany.com](mailto:postmaster@yourcompany.com) or [abuse@yourcompany.com](mailto:abuse@yourcompany.com) are valid email addresses so people can complain if they want to.
- c. Never send an email that does not offer a reply mechanism, a link to feedback or some other way for the reader to tell you what they think. Never send an email where the “reply” does not work – it just smells bad when you can't easily reply to a sender, and you'll lose trust instantly.

### 7) Spend time on your subject line

- a. If you're like me, you get a lot of spam. I'm getting pretty good at telling that it's spam before I even open it, so take a minute to examine your own inbox. Look at the emails you just “know” are spam and see what they have in common. Make sure you don't use the same words in your subject line as these emails, and avoid getting deleted before your email is even opened.
- b. Avoid subject lines that include exclamation marks, dollar signs, the words “free”, “extra income”, and any other words that you think will make your readers turn away. These words often trigger spam filters anyway, so even a permission-based email could end up in a spam folder or, worse yet, in the trash.
- c. If it's a newsletter you're sending, consider putting the name of the newsletter in the subject line with a hint about the contents. Subscribers will immediately recognize your newsletter's name (very important if you have more than one) and get a taste of what's in that issue. They'll be more likely to open it.
- d. Be honest – if your email is an advertisement, say so. Include [ADV] in the subject line – in some places its illegal not to, and people appreciate honesty.
- e. Put a consistent identifier – your company name, trademark, newsletter name etc. in square brackets in the subject line. This will make it much easier for users of spam filters to “whitelist” you – ensuring that all emails with that identifier get through to their inbox.
- f. Never use deceptive prefixes in the subject line. These include “RE:”, “FW:” etc.

- g. Don't mislead readers with your subject line. Make sure the subject copy reflects the content of the email.

## 8) Simple truths about content

- a. Watch how often you use Upper Case. CAPITAL LETTERS ARE SEEN BY BOTH HUMANS AND SPAM FILTERS AS "YELLING" AND "SPAMMY". Watch especially for titles of sections that are commonly capitalized.
- b. Keep your emails "light". Some filters trigger on size of email. A good rule of thumb is to keep your HTML emails under 50K. Dial-up users will thank you for it – as your mail will download much more quickly.
- c. Make sure all links included in your content have an http:// prefix.
- d. Don't include links to URLs that contain only numbers, ie: http://0.12.101.4.
- e. Avoid suspect spam phrases. There is a great list of phrases and words to avoid at [http://wilsonweb.com/wmt8/spamfilter\\_phrases.htm](http://wilsonweb.com/wmt8/spamfilter_phrases.htm).
- f. Walk the talk but don't talk the talk. Only spammers claim in their emails that they observe all spam laws. Mentions of House Bill 4176 or H.R.3113 will cost you points in any spam filter system.
- g. According to a recent study done by Quris, 4 of the top 5 most popular forms of email had two things in common. They were personalized and the content was relevant to the readers. Read these last two sentences one more time and put them into action. It's the best investment you can make.

## 9) Manage your list carefully

- a. Continually check your list for suspicious or duplicate addresses, and then verify or remove them.
- b. Clean up your list on a regular basis. Make sure you suppress all Hard-bounced email addresses on future mailings, or your ISP will label you a spammer before your readers do. Make sure your email service provider suppresses or deletes all Hard-bounced addresses for you, or get a report and do it yourself. Trust me, this is worth the effort.
- c. NEVER put your entire list of recipients in the "to" or "cc" fields, for two reasons: (1) Everyone on the "to" or "cc" line can see every email address in those fields, and use those addresses in any way they see fit—ethical or otherwise; and, (2) If someone hits "reply all," everyone in the "to" and "cc" fields will receive the reply, whether that person intended them to get it or not. Put your own email address in the "to" field and then use email software that is smart enough to send individual emails to each person on your list.
- d. Encourage feedback. Sometimes we don't see things the same way our readers do. Better that they write and tell you of anything that annoys them, than you finding out when you get blacklisted. Put your own "Report as Spam" link in every email, and do the same on your website.
- e. Track your complaints. Some ISPs, like AOL, have introduced a "Report as Spam" button on their email reader. This allows readers to send a complaint with a single click. AOL strongly recommends that you track complaints relative to the volume of email sent and watch for trends per mailing and/or where the names came from. They also recommend that you remove anyone who complains but that you NOT follow up with a confirmation on their removal. Ask how your email service provider handles AOL user complaints. If you use your own systems to send email, you can set-up a Complaint Feedback Loop with AOL by contacting their Postmaster group and any complaints about your mailings will be sent to you directly.

- f. Get a Bounce report from your email service provider or IT department if you use in-house software. Look for multiple Soft-bounced email addresses from the same mail domain. This is a strong indication that the company in question is using a spam filtering system (and over 70% of corporations do) and that your email is being blocked to all their employees. Ask your readers to approach their IT department to get your mail domain on a corporate “white list”.

## 10) Cherish your relationship with your readers

- a. Unless you have clearly stated that the email addresses you collect will be shared with other companies, NEVER EVER rent, sell, swap or give away your email list – it is one of your most important business assets. Cherish it and treat it carefully and with great discretion.
- b. Always include a privacy statement or a link to your privacy policy on your website. If you don't have a privacy statement, it's time to create one and publish it online. Samples are available at [http://www.truste.org/bus/pub\\_resourceguide.html](http://www.truste.org/bus/pub_resourceguide.html).
- c. Never encourage your readers to sign up their friends to receive emails from you. Encourage them to forward your email intact so their friends can make their own decision on whether to sign up themselves.
- d. Ask your readers to “whitelist” you. Many email services now allow mail users to manage their own personal whitelist – a list of mail domains or senders who they absolutely want to receive mail from. If your readers add you to their personal whitelist, your mail will automatically bypass any filters they have set up.
- f. Think beyond yourself. Your reputation (and your ability to deliver email) is going to be affected by everyone in your company who sends bulk email. Call a meeting of everyone in your company who could be sending bulk email – make sure that EVERYONE employs these Best Practises. Email deliverability falls to the least common denominator and while you may be “pure”, you will suffer if others are not.
- g. Don't send emails too often! According to a study done by Quris, the number one reason for unsubscribing is “emails that come too frequently”.

## 11) Test before you send

- a. Open email accounts with the major ISPs. Make sure to create two on each ISP, one with filters turned on, one without filters. Create a mailing list with these addresses on it, and do a test mailing to see how well your mail is being delivered.
- b. Run your email through a content filter before sending it. Try <http://www.lyris.com/contentchecker> - it will score your email, telling you how “spammy” you look. You can also send your test emails to <mailto:sales-spamcheck@sitesell.net> for a free report. Make sure you put the word TEST (in upper case) as the first word of the subject followed by your regular subject line.
- c. If your email is mission-critical or you do a lot of it, consider employing Assurance Systems (<http://www.assurancesys.com>) who will take your email and screen it for words that might trigger filters, let you know if you appear on any blacklists and assist you in getting off blacklists. They'll also check your email for deliverability to all major ISPs.
- d. See whether your IP address(es) or those of your email service provider are on any Blacklists. At <http://openrbl.org> or <http://DNSSTuff.com> you can enter your mail server IP address(es) to see which blacklists if any you are on. Don't be shocked to see yourself or your provider on at least one – almost all email service providers are listed, and a study done by GotMarketing in early 2003 showed that 1 in 4 of the Fortune 500 were also listed.

## 12) The technical side matters too

- a. Whether you send your emails yourself, or use an email service, make sure that whoever sends your email for you understands and has implemented the following procedures:
  - ?? All email must be RFC compliant. (Refer to <http://www.rfc-editor.org>)
  - ?? All email servers used to send emails must have valid reverse DNS lookups.
  - ?? All email servers used must be closed to third party relaying.
- b. Most systems will retry Soft-bounces – we suggest that you limit your Soft-bounce retries to no more than three attempts.
- c. Make sure your systems can accept all incoming email Bounce notifications. Some ISPs (like AOL) will block you if your system can't accept at least 90% of the Bounce return messages.
- d. Use an email service provider who has good relationships with the major ISPs. Many ISPs use a “whitelist” in addition to blacklists. Mail from senders on the whitelist will go through so it's a wonderful place to be listed. If you use your own inhouse system, you can also approach the ISPs to get whitelisted, but its not a simple process and not all of them use this.

Any email marketer who thinks it's “easier to ask forgiveness than permission” is sadly mistaken and will feel the repercussions on their brand and their bottom line. To avoid being labeled a spammer, honesty is your best policy. In all your email marketing efforts, be straightforward and take responsibility for your actions. Follow the guidelines above and strive to find the right balance between the needs of your business and the needs of your readers and the ISPs who bear the cost of delivering your email campaigns. Above all, do your homework before sending any campaign. When targeted messages are sent to qualified permission-based lists using the guidelines above, everyone can win.

**Lynda Partner** is the founder and former CEO of GotMarketing – a permission-based email service provider. She now runs Partners Inc ([www.partnersinc.biz](http://www.partnersinc.biz)), a marketing services company that specializes in creating excellence in internet marketing. She can be reached at [info@partnersinc.biz](mailto:info@partnersinc.biz).