



HOW TO AVOID FILTER-FALLOUT

by: Joe Halbrook, CTO
Permission Technologies
<http://www.CleanMyMailbox.com>

Seemed like in the first six months of 2002, all we read about were spam filters. Client-side software, or server-imposed mechanisms that attempt to "weed out" the "bad" email from the "good."

MailWasher, SpamEater Pro, Brightmail, Singlefin, SpamArrest, CleanMyMailbox, etc. all do this. Now everyone seems to be offering a way to filter unwanted email - and for good reason.

But, are legitimate email marketers and publishers getting caught in those filters? And, are such publications losing their reach because of these filters. Yes, and here's why?

It seems that spam filters do a good job of weeding out the UCE (Unsolicited Commercial Email) as well as the obvious spam email. But most of them also will, from time to time, filter out email from legitimate newsletters and email publications that were originally approved by recipients.

And the reason they do this, is because of an age-old problem:

Spammers mimic the same mailing and presentation techniques used by legitimate newsletter publishers. Quite frankly, it's getting harder and harder to distinguish the two types of incoming email.

And with the onslaught in sheer volume of spam email we all get these days, it's very easy to overlook the "good" email that might be erroneously identified as "bad." (These are called false-positives.)

So what is the solution? Are there ways that legitimate email marketers and publishers can somehow differentiate the way they send their mailings - and the content those mailings contain - to let the spam filters know they are legitimate opt-in mailings?

Of course, there is:

And, the best way to illustrate such a solution is to provide documented examples of some common practices of known spammers, how they present their information, and how they distribute them.

=====

SPAM DELIVERY TECHNIQUES

=====

Spam is delivered to your mailbox in a variety of ways. Here is a list of some of the most identifiable characteristics of delivered spam email:

- * Relayed through another mail server (open relay). Or, if your mail passes through two or more mail servers, multiple Received: headers will appear in your mailings. This will be trapped by many spam filters.
- * Sent many times with a string of numeric digits in the Sending From: address in the email header - either starting or ending in a numeric string, or containing both alpha and numerics.
- * Sent To: header contains the string: <undisclosed-recipients>.
- * Sent To: header has a missing address.
- * Sent To: a single mailing list address, instead of sending individual mailings to each recipient.
- * The Reply-To: header is blank or missing.
- * The From: and To: headers have the same address.
- * Excessive amount of CC: and/or BC: headers
- * To: or CC: headers contain many addresses with same domain.
- * To: or CC: headers contain many user names that are the same.
- * The mail server uses quoted-printable format, but some lines in the mailings are longer than 76 characters.

If you avoid these common "red flags," you will avoid having your email newsletter or publication being caught by many of today's spam filters.

=====

SPAM SUBJECT LINE CHARACTERISTICS

=====

Do you use the word FREE in your subject lines? Well, although the word FREE attracts the attention of many readers, it also attracts the attention of most spam filters!

Here are other pitfalls that you will want to watch out when constructing your Subject lines:

- * Exclamation / question marks. One may be ok, but not more than one.
- * Subject line ends in a string of numeric digits.
- * All capital letters. Stands out, especially to spam filters.
- * Subject line is omitted or blank. Big red flag!
- * Subject contains: ADV: or Adv: Required in some states, but this will almost always get your message filtered.
- * Subject contains G.a.p.p.y T.e.x.t or lots of whitespace between words.
- * Contains obvious spam words like: porn, viagra, teen, etc.

This is a tricky "subject!" But, seriously, these are one of the first things that many spam filters apply heavy weighting to when they find them. You can still construct captivating subject lines without using words or symbols that can force your message straight to the filter bin.

=====

SPAM CONTENT CHARACTERISTICS

=====

Probably the hardest task in differentiating your legitimate email message from those of the spammers is to learn what things to avoid in constructing the copy, or body, of your messages.

This is complicated further by the fact that this is one area that changes constantly, as the spammers realize what works, and what does not.

Here are a few suggestions to consider when developing the body of your email correspondences:

- * List removal instructions. Yes, you must have them! But, there is a right way to do this. Some techniques may not be to your advantage.

Good: * Custom-encoded instant removal links
* Removal instructions via email without the mailto: tag

Bad: * mailto: links with 'Remove' in the subject of the link
This will almost always get your message filtered.

- * Don't say "we honor all removal requests" or things of that nature. Filters look at this as a big "red flag."

- * Don't include a form that sends an email in the body of your mailings. If possible, don't use a form at all. Instead, use a hyperlink to your web site form.

- * Don't use common spam phrases like "be amazed", "your income", "subject to credit approval", "earn xxxx per week", "check or money order", "print out and fax", "call now", "if you did not opt in", etc. in the body.

- * Watch out for marketing hype about email, MLM, or fast cash opportunities in your copy. Sometimes, this means even look closely at what your advertisers are saying in their ads!

- * You might investigate some of the newer filter-trapping software that has been making it's way to the market. This software allows you to cut and paste your newsletter into a text area, then have the software scan the content to produce a list of trigger words or phrases that can cause it to be trapped by today's spam filters.

Note: Make sure you use one that provides a way to update trigger word lists. We suggest: **Filter Breeze**: <http://www.CleanMyMailbox.com/fb>

=====
SYNOPSIS
=====

This is a limited, but good starting list of items to consider when developing and delivering legitimate email correspondences to your readers.

Some of these suggestions may seem extreme and may not be fully acceptable to you. That's fine. But, please take them very serious because these are the exact things that today's spam filters look for.

If you implement these practices, you'll have much better success in reaching the largest segment of your audience and enjoying the benefits from doing so.

Thank you for spending the time to read this. I hope you can make use of these suggestions and implement a winning strategy that keeps your publication or newsletter free and clear of spam filters.

Sincerely,

Joe Halbrook, CTO
Permission Technologies
<http://www.CleanMyMailbox.com>
"We eliminate spam, while you save time"

p.s. Know someone else who complains about spam filtering? Why not pass this information on to someone else who could use it? It's as easy as forwarding it right now.