



## Spam Filters - A Legitimate Email Marketer's Friend?

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

In the "early days" of email marketing, it was easy:

Quality content - delivered at a frequency readers want it.

But, in the past 18 months, legitimate email marketers are finding that the rules of the "early days" just don't work any more. Why? Because of the plethora of email filtering solutions that have come on the scene to combat the flow of unwanted email.

Brightmail, spamarrest, Mailblocks, MailWasher, SpamEater, Singlefin, oddpost, and others all help mailbox owners reduce the amount of time they have to spend scanning and deleting unwanted email. Practically each month, we read about others who are offering ways to filter unwanted email - and for good reason.

But, as legitimate email marketers are finding out, publishers are suffering from those same filters. Why? Because of an inherent flaw that results in an endless cycle:

1. Email recipients install client-side filtering software or server-based solutions that filter unwanted email from their mailboxes.
2. The spammers also install and use these same filtering solutions. They study them. And they find out exactly how to get past these filters.
3. The filtering solution vendors figure out how the spammers are able to get past their filters and they come up with new logic to foil the spammers.
4. Repeat steps 2. and 3. forever.

No real solution is ever achieved because **1)** the filtering software is attempting to make decisions as to whether an email is spam based on ever-changing heuristic tests, and **2)** the spammers use the same software to test their filter "stealthiness" and always find ways to get their refuse past the filters and into your mailbox.

Legitimate email publishers are being hurt by these spam filters. And these days, many have touted the infamous Spam Filter as the beginning of the end of the legitimate email marketing industry, as defined in the "early days."

But, is this true? Or can legitimate email marketers turn this kind of thinking on end, and prove that today's spam filters are actually a godsend for legitimate email marketers?

Are there ways that legitimate email marketers and publishers can insure that their publications **always** can get past the spam filters, allowing the filters to do their job in removing all the noise, and putting their legitimate publications in the spotlight - where they belong?

We're happy to inform you that it's easy to accomplish! Using just a few precautions, legitimate email publishers can easily prevent spam filters from affecting their email marketing efforts. And by applying these suggestions, legitimate email publications can easily survive the dreaded spam filters, and become the shining stars that they rightfully are. Here are five precautions that make this happen:

=====  
**1. Provide Whitelisting Instructions For Each Publication.**  
=====

Here's a free tool you can use to generate custom whitelisting instructions for your publication: [Generate Whitelisting Instructions](#)

Just because legitimate email publishers receive those challenge response messages (you know the ones that say "Your email has been filtered. Please enter the text imbedded in the image above, and click the Submit button to prevent future filtering.") doesn't mean that your publication is doomed to never be read by those subscribers.

In fact, if your publication consistently adheres to the principles of excellent permission marketing, it will be anticipated and your readers whose spam filters catch your publication will immediately whitelist it, based on some criteria that will prevent future mailings. So, there's no need for undue stress when you see those challenge response messages after you distribute your publications.

All legitimate email publishers should provide the ability to whitelist their publications by one or both of two criteria:

**A. Subject Line whitelisting.**

This is where you provide instructions that explain the use of one or two keywords that will always be present in the subject line of each mailing of your email publication(s). By always including that one or two keywords, your readers can setup a whitelist entry or specification that tells their filtering solution NOT to filter YOUR publication(s). Of course, you will always use two or more keywords in sequence, so that the whitelist entry can be defined as a phrase, i.e.: TechBits: or I-Sales Digest

**B. Sender Address whitelisting.**

If you always use the same From: mailing address in your mailings, let your readers know this. They can simply add a single Sender address whitelist entry or specification that will prevent future filtering. If you use another scheme in your From: email address such as an imbedded date or volume/issue number, be sure to tell your readers what portion of those addresses will remain constant. Any good spam filtering solution will provide a way to whitelist on this "partial" email address. For example, if you use:

**From: issue-20031214@my-site.com**

consider changing the From: addresses to this format:

**From: 20031214-issue@my-site com**

and provide instructions that a Sender address whitelist entry could be setup to use:

**issue@my-site com**

Be sure to include a prominent link to your whitelisting instructions web page in each mailing you send out. You'll see those challenge response messages decrease quickly.

=====  
**2. Clean Your Mailing Lists Periodically.**  
=====

We all know how our mailing lists can get "dirty" in just a short time, as people abandon email address (most likely because of spam) or their mailboxes exceed their ISPs allowable quotas.

This means that every time we send out a mailing, we get bounce-back messages from each addressee who can no longer receive our mailings. While continuing to mail to these addresses may keep our subscription numbers high, it really serves no purpose. Advertisers want results; they're not inclined to spend more money with you just because your numbers are high. With the advent of CPA and CPC strategies, big numbers hold little weight. Advertisers want results - not numbers.

So the need to keep our lists "clean" of undeliverable addresses is of utmost importance. Not only do we want a quality list, we then do our share in not wasting bandwidth both in mailing and receiving bounce-backs from invalid addresses.

Many listserver solutions provide built-in bounce-back processing that allow you to remove addresses after a set number of failed delivery attempts. If yours does not, there are list cleaning services available to do this for you. Just do a search in Google using the search term: "list cleaning" and you will find more than a few companies who offer list cleaning services.

=====

### **3. Make Use of Spam Checking Software.**

=====

Today, there are more than a few ways to make sure your email publication is fairly "filter stealthy." Of course, if you take care of points **1.** and **2.** above, this precaution is not quite as imperative. Still, it can make a huge difference for readers whose filters that are not as whitelist-friendly, and for those newer filtering solutions may take a few months to mature.

There are a few spam filter analysis services, as well as stand-alone programs that you can purchase to pre-test each mailing for it's spam filter stealthiness. Most will return a weighted score that indicates the characteristics that make your publication more or less likely to be caught in the spam filters.

Again, a quick search at Google using the search terms "spam filter trigger words" or just "trigger words" will reveal resources that can help you make sure your mailings are optimized to prevent filtering.

=====

### **4. Watch Out For HTML Mailings.**

=====

Most email client software today can be configured (and many are, by default) to filter HTML emails, simply because of the threat of malicious email-borne viruses. Unfortunately, many users of such email software such as Outlook, Outlook Express, Eudora, Netcape Messenger, etc. do not know that their email clients are configured to do this, and do not know how to change the configuration setting.

Therefore, publishers of HTML email, while many enjoy the format, will lose readers simply because they do not offer text-only versions of their publications.

Our Recommendations:

1. Offer an optional text-based version of your HTML publications, and offer your readers a choice of which format they wish to receive.
2. Explain to your readers how to adjust their email clients to NOT filter or alter HTML emails. (Of course, many will not take advantage of your suggestions, because of the preeminent fear of email-borne viruses.)
3. Continue to use HTML publications, only put them on a web site, and send out only a text-based "ticker" email to your list which contains a Table Of Contents for the publication, and points them to your full web-based version.

=====  
**5. Promote: CleanMyMailbox Web-Base Anti-Spam Solution**  
=====

While some of today's spam filters provide the functionality that facilitate whitelisting using the methods described today - not all do. Therefore, we recommend that you promote the use of the CleanMyMailbox permission-based filtering solution to your readers.

Not only can you rest assured that your mailings will be delivered to gain their "light in the spotlight" where they should be, but your subscribers will thank you for pointing them to the only permission-based filtering solution that does away with today's awkward blacklisting - which have been proven to fail time after time.

Additionally, CleanMyMailbox makes sure that spammers can no longer use the same spam filtering solutions that rid us of unwanted email against mailings of the plethora of excellent legitimate email publications. They cannot get past a filtering solution that is based on a permission whitelist by design.

CleanMyMailbox is a premier filtering solution that is a Friend to all legitimate email publishers, as they strive to get their publications past the 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.