

14 Best Practices that Improve E-Mail Deliverability

A guide to getting bulk e-mails delivered

by Dr. Ralph F. Wilson
Editor, *Web Marketing Today*®
P.O. Box 565, Loomis, California 95650

Revised October 19, 2009

**Please do NOT distribute this e-book to others. It is for your use only.
Unauthorized distribution constitutes theft of my intellectual property.**

091019

Because of the spam deluge, it is harder to get legitimate, bulk e-mails delivered to your recipients' inboxes. E-mail is certainly less reliable these days, but that doesn't mean it is dead. While a few industry pundits trumpet RSS, Twitter, and desktop message delivery systems as e-mail killers, I don't see that happening anytime soon. E-mail remains the most widely used -- and, perhaps, most cursed -- Internet tool, bar none.

For those who rely on bulk e-mail lists to communicate with members, subscribers, customers, or prospects, achieving high inbox delivery rates is vital. This whitepaper is designed to outline the various issues -- and point you to solutions that you can afford.

1. Use a Reputable E-mail Marketing Service (EMS)

These days, do-it-yourself e-mailers can't match the inbox delivery rates achievable through reputable E-mail Marketing Service (EMS) providers. I have long been a proponent of desktop and self-hosted e-mailing systems. I still use [Gammadyne Mailer](http://www.wilsonweb.com/afd/gammadyne.htm) for smaller e-mailings and [AutoResponse Plus](http://www.wilsonweb.com/afd/arp3.htm) for the complex autoresponder system I use to deliver online training programs. However, for my main business list where high deliverability is essential, I use an EMS provider. Good EMS providers achieve high deliverability because they:

- a. **Constantly monitor e-mail delivery.** When they spot a delivery problem with a particular ISP (Internet Service Provider) they deal with it quickly, because they
- b. **Maintain constant working relationships** with the 20 to 30 major ISPs in their market areas. They
- c. **Aggressively protect their reputations** with ISPs by screening out spammers and demanding client compliance with legally required e-mail practices. They sometimes

- d. **Subscribe to e-mail reputation services** that place them on "whitelists." These subscriptions encourage preferential treatment for the e-mails their clients send. (More on this later.)

Small businesses will want to look at [iContact](http://www.wilsonweb.com/afd/icontact.htm) (www.wilsonweb.com/afd/icontact.htm), [AWeber](http://www.wilsonweb.com/afd/aweber.htm) (www.wilsonweb.com/afd/aweber.htm), among others. Space prevents me from providing an exhaustive list of the many excellent EMS providers. The reason I include using EMS providers as my first recommendation is that they help you -- and in some cases, force you -- to follow a number of the best practices outlined below.

2. Unsubscribe Bouncing E-mails

Make sure your system correctly unsubscribes hard bounces ("No user at this address") and soft bounces ("Mailbox full," a sign of an abandoned e-mail address), while *not* deleting temporary bounces ("Out of the office" and "On vacation"). If your list contains a significant number of bouncing e-mail addresses, the major ISPs will stop delivering your e-mails once your bouncing e-mail count reaches their (unpublished) bounce threshold. Keep your list clean.

3. Use Multi-part MIME, Not Bare HTML

ISPs tend to see HTML-only e-mails as more likely to be spam than text-only e-mails. Thus, if you're going to send HTML (which gets a much better response rate), make sure to send a "sandwich" consisting of both text and HTML messages (called "multi-part MIME"). Most modern e-mail software helps you do this. This technique helps only a little, but in deliverability we're dealing with minor improvements to a lot of practices that, taken together, show a significant effect on delivery.

4. Minimize Graphics

ISPs tend to see graphic-heavy messages as more likely to be spam, so keep your graphics to the minimum you actually need. At the same time -- and this point is related *not* to deliverability but to getting e-mails opened and your message across -- don't rely on graphics to carry your message. Rather, use images as *message enhancers*, since an increasing number of web-based e-mail programs, as well as desktop software such as Office Outlook, don't display e-mail images by default.

5. Be Alert to Spam Trigger Words

I see four main types of spam filters (with an increasing number of blurring between types).

- a. **Word-trigger filters**, such as [SpamAssassin](http://spamassassin.apache.org) (spamassassin.apache.org) -- very popular among small businesses because it Open-Source and thus no cost. They scan incoming e-mails for words that might indicate spam.
- b. **Network reporting filters**, such as [Cloudmark](http://www.wilsonweb.com/afd/cloudmark.htm) (which I use, www.wilsonweb.com/afd/cloudmark.htm), nicely priced for individuals and small businesses. If enough people report a message as spam, its "fingerprint" is recorded and marked as spam for all participants.
- c. **Response-required filters**, such as [SpamArrest](http://www.wilsonweb.com/afd/spamarrest.htm) (www.wilsonweb.com/afd/spamarrest.htm), where the sender must respond before the recipient sees the message -- at least the first time a sender e-mails to this recipient. More on this below.
- d. **Whitelists and Blacklists filters**. ISPs increasingly check blacklists to filter out known spammers (such as the RBL list). They also check whitelists that contain "authenticated" e-mailers that use good practices. More about this later.

Marketers should check e-mails before sending them in order to detect excessive marketing "hype" words that would put them over the top in SpamAssassin's point score -- and put their e-mails in the "probably spam" category. To see an example of the [complex list of spam indicators](#) to determine whether a message might be spam, see the current "test performed" at the SpamAssassin site.

Most EMS providers and several online services have such a pre-screening tool you can use. For example, SiteSell SpamCheck Report tests your message at no charge using SpamAssassin and sends you a report. Send your test e-mails to <mailto:sales-spamcheck@sitesell.net> Be careful, however, that you put the word "TEST" (without quotes) as the first word in the subject -- and make sure it is capitalized. Otherwise, the system will delete the mail. Following the word "TEST," add the subject line that would appear in the email normally. Don't avoid trigger words entirely; just make sure that you don't overuse the ones that will signal your message as spam.

6. Ask Subscribers to Add You to Their Whitelist

Many major ISPs and spam filtering programs will automatically place bulk e-mails into a spam folder or bulk folder unless the recipient has identified the sender of the e-mail as "desirable" on some kind of "whitelist." You can find comprehensive instructions you about this that you can pass on to your subscribers at www.cleanmymailbox.com/whitelist.html It's a good idea to link to a set of whitelisting instructions from your subscription form, on your "confirmation" e-mail, and in your "thank you for subscribing" e-mail. I've also tried audio on the thank you page with fairly good results.

7. Study Delivery Reports

Your E-mail Marketing Service (EMS) will tell you the number of e-mails sent, bounced, and opened. But that information is too general to do you much good. A much more precise approach involves using a service that provides 100 or more "seed" e-mail addresses that cover all the major ISPs with two or three e-mail boxes. They monitor these addresses and report when or if an e-mail was received from your mailing. This way you can begin to spot problems in deliverability. Address the problems you've identified with your EMS (best approach) or directly with the ISPs themselves (frustrating). A few of the more expensive EMS providers supply clients with this kind of data, but your best approach is probably a deliverability service. Small businesses may want to take advantage of the 30-day free offer at [Delivery Monitor](http://www.wilsonweb.com/afd/deliverymonitor.htm) from AWeber (www.wilsonweb.com/afd/deliverymonitor.htm), a low-cost service I've used for years. Other services include: ReturnPath's [Mailbox Monitor](http://www.returnpath.biz/delivery/monitor/) (www.returnpath.biz/delivery/monitor/), the [Delivery Monitor component of Lyris Email Advisor](http://www.lyris.com/products/emailadvisor/) (www.lyris.com/products/emailadvisor/), [Pivotal Veracity eDelivery Tracker](http://pivotalveracity.com/solutions/eDelivery.php) (pivotalveracity.com/solutions/eDelivery.php), and [Delivery Watch](http://www.deliverywatch.com) (www.deliverywatch.com) for European e-mailers.

8. Monitor Blacklist Reports

Every e-mailer will eventually be accused of spamming -- whether you actually are or not. Your domain will appear on a blacklist, a list of supposed spammers, when an irate recipient (with nothing better to do) complains that you are spamming. Of course, you want to make sure your Email Service Provider (ESP) isn't on a blacklist (unlikely), but it's vital that you try to get off any blacklists that your domain name may appear on, especially the blacklists routinely used by the larger ISPs. You can check your status by using the free [MX Toolbox](#)

(www.mxtoolbox.com/blacklists.aspx) or by subscribing to a monitoring service, such as [Blacklist Monitor](http://www.wilsonweb.com/afd/blacklist.htm) (www.wilsonweb.com/afd/blacklist.htm) that e-mails you whenever your domain appears on or is removed from a blacklist. The most frustrating task is to find a way to contact a blacklist administrator so he will remove your domain his particular list. Blacklist Monitor comes with current instructions on how to get delisted from each blacklist, but blacklist administrators are notoriously difficult to reach. Good luck. This is one reason you may need a good ESP to go to bat for you.

9. Employ SPF and DomainKeys

Too often, spammers will insert your e-mail addresses in the "from" field, pretending that their e-mail is from you, in order to trick the ISPs. As a result, now ISPs are beginning to employ methods to determine whether a particular e-mail is sent by a legitimate sender from your domain or by a spammer spoofing your domain with a bogus "from" address.

SPF ([Sender Policy Framework](http://www.openspf.org), www.openspf.org) was created in 2003 to prevent spoofing of your e-mail address. The ISP checks a line in your domain information to determine whether the sender is authorized by you to e-mail using your domain name. SPF is quite technical. Ask your ESP for the exact SPF entry that indicates that they are authorized to send your bulk e-mails. There is an [SPF Setup Wizard](http://old.openspf.org/wizard.html) (old.openspf.org/wizard.html) that can provide some help, but you'll probably need to ask your web hosting service to insert the proper line in the DNS (Domain Name Service) information for your domain. You'll need help to accomplish this, but it's important.

[DomainKeys](#) is a newer approach that includes an encoded digital signature in the e-mail message. This allows the ISP to verify whether or not the e-mail originated from the purported domain. Hopefully, your ESP will have implemented this, since increasingly the major ISPs are equipped to check DomainKey signatures.

ISPs will *often* route bulk mail correctly to a recipient's inbox *without* proper SPF records and DomainKeys. But bulk e-mails from domains that *do* follow these protocols are *significantly more likely* to pass through the spam filters unscathed.

10. Respond to Challenge-Response Requests

Some popular spam filters use a challenge-response approach, such as [Spam Arrest](#), EarthLink, and others. An whiny e-mail comes back: "I don't want to

receive spam. So if you want to e-mail me, you'll need to click on a link and type in a code before I'll get your e-mail." This creates a chore for legitimate bulk e-mailers, since the first time you send an e-mail to a particular recipient, the system requires a human being to read and type in a [CAPTCHA graphic](#) before forwarding the e-mail to the recipient. However, since millions of e-mail recipients now employ such techniques, it's vital that you check your e-mail bounces after a bulk mailing and respond promptly to each of the e-mails requesting your response.

11. Deal Quickly with Spam Complaints

As mentioned above, anyone who mails to a sizeable list will be accused of spamming. Yahoo, America Online (AOL), and [Cloudmark](#), for example, make it particularly easy for a recipient to declare an unwanted e-mail message as spam by just clicking a button. You the sender will never know. In fact, it's usually easier to mark an unwanted e-mail as spam than it is to unsubscribe, so subscribers are getting lazy. As a result, e-mailers must (1) keep e-mails continually relevant so they will be perceived as valuable, (2) make unsubscribing clear and easy, and (3) respond quickly to spam complaints that they *do* receive. When your web hosting service, ISP, or a recipient ISP accuses you of spamming, immediately respond to protest your innocence. Prepare a standard e-mail that explains how you carefully follow all the e-mail best practices. Don't put off your response when there is a complaint. Do it immediately. It is one small step in maintaining your reputation as a responsible e-mailer.

12. Contract with a Reputation Service Provider

Larger companies should consider contracting with one of the services that authenticates legitimate senders. Unfortunately, some smaller businesses may find that they can't afford the stiff prices charged. These are the leading e-mail reputation service providers:

[Sender Score Certified](#) (SSC, <http://www.senderscorecertified.com>) of ReturnPath (formerly marketed as Bonded Sender) provides a whitelist of clients that adhere to strict standards of e-mail best practices.

[Goodmail](#) (www.goodmail.com) has developed relationships with some of the biggest ISPs such as AOL, Yahoo, Comcast, RoadRunner, and AT&T. While many large ISPs will disable links and images on bulk e-mails, Goodmail clients' e-mails are delivered to participating ISPs with links and graphics intact. Goodmail

CertifiedEmail is identified with a unique, cryptographically secure token. A number of the more expensive Email Service Providers (ESPs) are equipped to send CertifiedEmails for their clients.

13. Offer a Text Alternative for Subscribers

Don't assume that all recipients on your list prefer to receive HTML e-mails. In order to prevent viruses from getting behind corporate firewalls, a number of large corporations, as well as government agencies, routinely strip HTML codes from e-mails and only deliver a text version. A few recipients might even use e-mail programs that don't read HTML e-mails properly. Give your recipients a choice between HTML and text e-mails. Even though I make HTML e-mails the default radio button, I find that about 16% of my subscribers select text-only messages. Those who make it a point to select text-only know they need it. Being responsive will increase the deliverability and readability of your e-mails.

14. Establish Feedback Loops (FBLs) with the Major ISPs

Finally, bulk e-mailers should work to establish relationships with the major ISPs by signing up for their feedback loop, a system that lets you know when their clients complain about your e-mails. Several of the larger ISPs provide a way for your business to be recognized as a legitimate e-mailer and get on internal whitelists by affirming that you follow important e-mail standards. For example:

- [American Online Postmaster](http://postmaster.aol.com) (postmaster.aol.com) allows you to set up a Feedback Loop (FBL) that informs you immediately when AOL members mark your e-mails as spam.
- [Windows Live Hotmail](http://postmaster.msn.com/Services.aspx) will allow you to get on a Junk E-mail Reporting Program (JMRP, <http://postmaster.msn.com/Services.aspx>) by filling out and submitting a questionnaire.
- [Yahoo! Mail Whitelist Form](http://help.yahoo.com/l/us/yahoo/mail/yahoomail/postmaster/bulk.html) (<http://help.yahoo.com/l/us/yahoo/mail/yahoomail/postmaster/bulk.html>) provides a way for your domain to be considered for whitelisting. E-mail from your domain is monitored for a probationary period. If you don't have too many spam complaints, you may be whitelisted so that your e-mails get to the recipient's inbox by default.

It is difficult for individual mailers to keep in touch with the top 20 or so ISPs, but better ESPs make a point of building and maintaining these relationships. That's

why their clients' e-mails tend to be delivered to inboxes at a higher rate than that which individual mailers can achieve by their own efforts.

Throughout this series of articles we've explored the various ways you can improve inbox delivery of your e-mails and avoid the dreaded black hole where spam filters send bad little e-mails. Getting a high delivery rate doesn't require just a single modification of your behavior, but careful implementation of as many of these deliverability best practices as possible. Here's to higher inbox deliverability for you!

About the Author

Dr. Ralph F. Wilson is an Internet marketing pioneer. He founded [Web Marketing Today](http://www.wilsonweb.com) (www.wilsonweb.com), a free weekly Internet marketing e-mail newsletter in 1995. Since then he has provided up-to-date Internet marketing information to his 100,000+ opt-in subscribers.

Dr. Wilson is the recipient of the Tenagra Award for Internet Marketing Excellence. He is the author of hundreds of articles and more than a dozen [books](#) on Internet marketing, including *Planning Your Internet Marketing Strategy* (Wiley, 2001) and *The E-Mail Marketing Handbook* (2nd Edition, 2004). He has spoken widely on Internet marketing at both industry conferences and one-day seminars his company has produced.