

SPAM Avoidance and Mitigation

Tactics to avoid unsolicited bulk email

Copyright 2008 4ReliableComputers.Net

rev 2008-11-01

Overview: 85% + of all email traffic is SPAM. It has been the fastest growing portion of email use for years. SPAM filters are only marginally effective. They are particularly ineffective at separating SPAM from desirable incoming email originating from new correspondents. Whitelists and blacklists are ineffective for this purpose, because who knows the email address of their next new correspondent? The most difficult problem is protecting addresses which must be open to messages from new senders, due to the role of their human lessees.

There is no meaningful legal penalty for SPAM emitters (or for telemarketers, or junk snail mailers). Fortunately, SPAM avoidance, along with SPAM mitigation can reduce the annoyance and expense to reasonable levels, even without politicians help.

Anti-SPAM tactics grouped by user class. What type is your use?

Those who seek new correspondents, but whose relationship with correspondents is long lived (such as commercial sales personnel): the best choice is to avoid attracting SPAM for as long as possible. Dealing with the onslaught, should it start, is unsatisfying, time-consuming, and only partially effective. Morphing email addresses to dodge SPAM disrupts existing relationships valued by these users. Blended transitions can be used: a primary email address that has become SPAM plagued is superseded by a fresh (SPAM free) address, but still monitored for the duration of many few sales cycles.

Those who seek new correspondents, but whose relationship with correspondents is short lived (such as retail sales personnel): morphing email addresses to dodge SPAM is minimally disruptive to existing relationships, because they are not persistent over time. Blended transitions can be used: a primary email address that has become SPAM plagued is superseded by a fresh (SPAM free) address, but still monitored for the duration of a few sales cycles.

Those with a relatively static list of correspondents: SPAM filters employing whitelists are quite effective. Such users can be less careful about how they disclose their addresses, because they can set a filter to only accept email from addresses that are familiar. Such users tend to be mainly social users. For these people changing

email addresses can be disruptive to correspondents, because they manage address books poorly, or not at all.

All users can benefit from using secondary, or disposable addresses for high-risk correspondence, such as that described below.

Major attractors of SPAM in descending order of risk. Avoid letting addresses you care about fall into these traps:

- Avoid listing, or allowing your address to be posted on any web site in text and/or via un-encoded mailto. Email addresses can be listed on websites, and remain SPAM resistant, if the listing is done properly, in a manner not consistent with the latest SPAM avoidance techniques. It is best to not use any address you care about if it will be listed carelessly on a website. (Disposable email addresses are best for these purposes). The test is this: if you can copy and paste the text of your address from the web site, it is harvestable by SPAM robots, which crawl every web site on the planet eventually. This is distinct from clicking on a link which opens a pre-addressed new message in your email application.
- Avoid listing, or allowing your address to be posted on any blog. Blogs and USENET are structured, threaded websites, so they represent risk if they expose email addresses in text and or un-encoded mailto: They become attractive to SPAMers when the quantity or quality of addresses listed on them becomes sizeable. It is best to not use any address you care about if it will appear in a blog. (Disposable email addresses are best for these purposes).
- Avoid entering email addresses you care about into webforms, especially e-commerce sites, music download sites, chat rooms, social networking sites, etc. Disposable email addresses are best for these purposes. Consider the risk of revealing your complete and true human name as well, particularly if it is unique. A unique human name can be easy to find a physical address for.
- Avoid listing of email addresses you care about on widely distributed literature (rosters, advertisements, business cards, etc) unless the benefit outweighs the risk. Your literature can direct business prospects to a website, from which they can obtain your current email address.

- Avoid allowing your email address you care about to be exposed in emails sent to groups by senders who include it in the TO or CC fields (they should use BCC instead)
- Avoid listserv subscriber lists that can be poached. This is a small portion of listserves, usually managed by fumblers. If in doubt, use a disposable email address for this purpose.
- Avoid listserv subscriber lists intentionally co-opted by administrators. This is a small portion of listserves, usually managed by salespeople or SPAMers masquerading as something else. If in doubt, use a disposable email address for this purpose.
- Avoid entering or allowing an email address you care about into any third party web-based address book, such as evite.com
- Never reply to any SPAM for any reason, even if it tempts you with offers to "unsubscribe". Replying includes enabling any auto-reply, vacation-response, etc.

What is email good for if I have to observe all these caveats? Consider separating your usage into tiers. Keep one address for uses where the effort and disruption of change is high (persistent social and business relationships with humans). Use less permanent addresses for higher risk correspondence (such as e-commerce) with organizations where your relationship is sporadic, or short lived. Most email providers make multiple addresses available to you. Most email applications allow you to send from more than one address. (See the section below on selecting and morphing email addresses).

E-commerce purchasing without SPAM: In most cases, the email address used needs only remain valid for the duration of the transaction. Why risk SPAM from a vendor's abuse of your address? Simply use a disposable addresses for tasks that do not require persistence. Yahoo.com, hotmail.com, gmail.com, etc offer these.

But protecting my email address is less important to me than using it! Have your cake(s) and eat them too! Use secondary, or disposable addresses for high risk correspondence, such as that described below. If you like, use free addresses from various vendors, via webmail. Most email providers offer multiple addresses at no additional charge. Configure and use them for different purposes. You will find that some of your uses attract SPAM, while some do not. By segmenting the problem, more specific and effective tactics can be applied. Examples of common functions for addresses:

4social@yourdomain.com
4ecommerce@freedisposableaddress.com
4listserves@yourdomain.com
4sales@yourdomain.com

When starting with a fresh email address: Avoidance of the problem is the best tactic when starting with a fresh address. Being careless, attracting SPAM, and then trying to limit the irritation with SPAM filters is unsatisfying, time consuming and only partially effective. The reason is that SPAM filters tend to snag email you wanted to see. Tuning them is difficult and imprecise. If you use addresses you care about carefully and specifically, a SPAM problem is less likely to arise.

Periodically start with a clean slate by simply morphing addresses when they start picking up SPAM.

jane4riverz2006@yourdomain.com
jane4riverz2007@yourdomain.com
jane4riverz2009@yourdomain.com
...
jane4riverzYYYY@yourdomain.com

Do not use primary ISP (DSL, cable provider) email address for anything other than administrative purposes. Never give it to anyone. If it becomes SPAM infested, you cannot abandon it, because you need it to get important account notices from your Internet Service Provider (ISP). Create secondary addresses in the beginning, and use them exclusively, morphing as necessary.

Avoid creating addresses comprised solely of a dictionary word. Avoid constructing the portion preceding the @ solely of dictionary word(s) or common human names of any language, spelled forwards or backwards. Uniqueness is desirable! This is why the address jane@yourdomain.com is a poor choice. Jane4riverz2007@yourdomain.com is a better choice. Placing your full human name in an email address has profound security implications; consider them carefully!

AddressGuard / Disposable addresses: Consider getting Yahoo Mail Plus (\$20/yr), then utilizing their disposable address function for e-commerce and other situations. Other email providers may implement something similar. (Some credit card companies offer a similar concept for ccard transactions - a one-use, limited \$, limited duration ccard number; this is a great fraud prevention tool for e-commerce transactions).

Avoid configuring computer operating systems with valid personal identifying information: Entering your full name and any valid unique identifying information (phone number, snail mail address, email address)

into a workstation's operating system configuration pages is a bad idea, because various methods allow outsiders to pry while you are browsing. During configuration of an operating system (examples include Windows XP, Vista, Mac OSX), if the forms will not allow blanks, enter decoys.

Examples include:

NoFirstName
NoSurName
123 anywhere Street
San Francisco CA 94123
987-654-3210
notme@notmydomain.com

Email servers routinely carry the workstation name in email headers, no matter which address email is sent from. Workstation names are often generated from human names entered during initial configuration of the machine. Ever wonder how you got SPAM this week specific to products you searched for via web last week, even though you didn't enter your email address in any of the web sites you visited? Not following the recommendations in this paragraph enables such pilfering. Anti-Spyware scanners, Phishing filters, and Privacy Filters are imperfect, and require effort to tune. Preventing the problem is easier than fixing it after occurrence.

We are ready to assist you in prevention of SPAM and security risks, and mitigation of existing SPAM and security problems. For all your computer needs, contact us:

[4ReliableComputers.Net](#)