



## **A Practical Guide to Dealing with SPAM**

**By Ephraim Feig, PhD.,  
CTO & Chief Marketing Officer  
Kintera, Inc.**

If you are the typical email user, you know about SPAM. You are angered by it, frustrated by it, and very likely resigned to living with it, hoping that anti-SPAM efforts will yield better and better results in the future. Various studies have shown that SPAM now accounts for over 50% of all emails and yielded over \$40 billion in financial losses in 2004, more than double 2003 figures. Moreover, a lot of SPAM leads to further intrusion and fraud. SPAM mail may contain spyware that is installed on a user's machine upon opening the SPAM email. More ominously, SPAM email may deploy phishing techniques; these are typically legitimate looking emails from familiar looking sources that are sent to surreptitiously capture private information. A common phishing scheme is to send a link to a website that appears to the user to be a legitimate financial institution (yes, they know where you do your online banking and shopping), asking the user to update sensitive information. Of course the website is a fake, but is constructed so well that it fools the user.

You can take relatively simple proactive steps to mitigate the debilitating effects of SPAM. We address several types of users- end users (receivers of email), both individuals and organizations, and organizations that send out large amounts of legitimate emails. The former group wants to isolate as many SPAM emails as possible while minimizing false positives (non-SPAM emails that are classified as SPAM and isolated). The latter group wants to make sure that as many of their legitimate emails reach their desired destination and not be classified by the receivers' systems as SPAM. Furthermore, even if their emails reach their destination, they don't want their recipients or, even more threateningly, legal authorities, to consider them SPAM.

As an individual, here are steps you can take to minimize SPAM:

- Don't respond to email from a non-familiar source. Even a response rate of one from several thousands makes it worthwhile for spammers. Furthermore, by responding- even if for asking to cease and desist- you are telling spammers that your email address is valid.
- Likewise, don't click on any links in unsolicited emails, even "unsubscribe" and "remove" links. Again, this just confirms that your email address is valid.
- Do not respond to emails that ask you to either send personal information or link you to a website that asks for personal information, even if the source of the email is familiar and the linked website looks legitimate.
- Be careful and limit the number of websites with which you register.

- Don't open unsolicited emails, unless you have blocked HTML graphics. Modern email systems can track if you open HTML emails.
- If you use Microsoft Outlook, turn off the preview pane. Otherwise, any email that is previewed is actually opened, and spammers will have validated your address. If you want to see more details, change the "current view" to enable "messages with AutoPreview." You will only see parts of text content, no HTML.
- If you are overwhelmed with SPAM, change your email address. Make sure you let your contacts know your new address. This is drastic, but most effective. Remember, be vigilant with you new address- follow the suggestions above.

You can minimize the amount of SPAM that is sent to you, but you cannot stop it altogether. In order for you and your organization to divert SPAM that has been sent to you from actually reaching your inbox, you will either have to install a SPAM checker on your computer or use an ISP that already provides such service. If you do it yourself, you can do it on your personal computer, or, at work, your organization may decide to install an enterprise-grade system on its mail server. These will scan your incoming email and parse them according to which ones it determines are SPAM or not. SPAM email will go to a special folder; the rest will flow to wherever they usually flow (most often your regular inbox, unless you direct emails from specific addresses to other folders). Most people are familiar with these filters, even if they have never installed one. For example, if you use Yahoo mail, you may configure your system to direct identified SPAM (by Yahoo's own SPAM checking filter) to its "Bulk" folder. You may scan emails in your SPAM folder, if you are worried about false positives, but be careful- remember the bullets above; most people just delete them.

The simpler SPAM checkers scan email content for telltale signs of SPAM, typically familiar SPAM words or phrases, often called SPAM filter triggers. Unfortunately, spammers are adept at avoiding them, so they pass through quite a lot of SPAM. Furthermore, often these simple filters classify legitimate emails as SPAM (so-called false positive). The more sophisticated filters are provided by specialized services that, in almost real-time, identify IP addresses of servers that send out SPAM. They then send these addresses to their subscribers, who install special software on their computers, where continuously updated "blacklisted" server lists are maintained. When an incoming email comes from any of these blacklisted servers, it is isolated.

Finally, here are some suggestions for those who send emails to make sure they are not SPAM emails nor mistaken for SPAM.

- Always use accurate header information.
- If you are promoting or advertising, include your valid postal address.
- Only use domain names that are registered to actual people or entities.
- Include a prominent return email address and a convenient option to opt-out from receiving further emails.
- Honor opt-out request as soon as you can; definitely within ten days of the request.
- Only buy email lists from reputable vendors.

- Avoid trigger words or phrases. You can find lists of SPAM filter triggers online; A Google search on the words “spam, trigger, words” yields several.
- Test your emails before sending out in bulk. You can do it by sending emails to yourself, colleagues and friends, or by using special tools that test for triggers (some are free, online; for example: [www.enetplace.com/spam-checker.html](http://www.enetplace.com/spam-checker.html)).
- Check if your domain is blacklisted. There are services that will do that for you for a fee, or you can do it free, online. For example, [www.mxtoolbox.com](http://www.mxtoolbox.com) will give you the status of your domain with many common blacklists.
- If you send out massive amounts of email, consider using a reputable service.

The SPAM tug-of-war is like a cat and mouse game. As technology is improving in detecting and stopping SPAM, spammers are finding new ways to evade them. SPAM is illegal (read about the SPAM laws in [www.spamlaws.com](http://www.spamlaws.com)), but so far, even with several famous applications of the law against spammers, the abuse is still rampant and growing. Yet, legal approaches should mitigate the problem in the future. I think the most significant influencers will be average users who adopt common sense protocols of email etiquette and practice SPAM avoidance both as receivers and senders.