

## Anti-Spam Tips

### Spam Prevention Tips for Business Email Users

One of the many problems facing business email users today is that they are allowing spammers to easily identify their email address and are then scrambling to prevent the spam from reaching their inbox. To prevent spammers from harvesting email addresses, we recommend that businesses be very careful about where they publish their email addresses—this will help to prevent their addresses from getting on bulk mailing lists in the first place. We specifically recommend the following:

- Create alias email addresses that can be replaced. We advise that all email users create at least one separate, dedicated email alias address to be used for all e-commerce purchases and when registering for third-party services. Also, use this email address when posting to discussion lists, newsgroups, message boards, and when displaying email addresses to the public, such as on a website. In other words, only list generic email addresses on websites, such as sales1@domain.com, support1@domain.com, etc.

One of the most prominent ways that spammers collect email addresses is by writing automatic scripts that crawl the Internet and pick email addresses off of websites. For this reason, email users and webmasters should only publish generic email aliases on the web. These aliases should, preferably, be replaceable so that once spammers pick up on the aliases, the aliases can be discarded and replaced with another alias address.

- Do not give your email address away unless you are confident that the recipient is a trusted party. If it is an optional request from a third party, leave it blank. If it is required, it is best to use your temporary email alias address or an email account that you have with a free provider such as Yahoo! or Hotmail.
- Do not unsubscribe from spam that you receive unless you know it is from a trusted source. Many spammers use unsubscribe requests to verify that email addresses are in fact legitimate. Once you unsubscribe, they know the email was

received. This actually makes your email address more valuable to spammers. If you believe that you are receiving an unwanted bulk email from a reputable company, un-subscribing will most likely be safe and should be done. However, if you don't know the sender, don't unsubscribe or reply.

- Do not rely on AOL, Hotmail, Yahoo, Gmail, or other generic email addresses for business purposes. Many companies that provide free email services make money by selling email addresses and subscriber information to spammers, advertisers, and other third party marketing organizations. Additionally, because these free email services have millions of users, spammers attack those systems with great frequency.
- Do not reply to or forward long chain letters that you receive via email. Many spammers collect email addresses from these chain letters that are passed through hundreds and sometimes thousands of groups of email users. While this is labor intensive for some spammers, most of the email addresses found within these chain letters are legitimate and may become spam targets.
- Do not sign up for any service that claims to be a "Do Not Spam List," similar to the FCC's "Do Not Call List." Many of these services are fraudulent and actually may lead to your email address being added to more spam lists.
- Use obfuscation techniques when publishing your email address on web pages. Spammers use automated programs to crawl the web in search of email addresses. Therefore, it is a good idea to use HTML tricks to make your email address unreadable by these programs. For example, you can embed HTML comment tags inside of your email address, use character encoding techniques such as HTML escaping and URI encoding, or use JavaScript to write out the address. These techniques would be transparent to your website visitors, but may fool the automated programs.