



# **Tips on Reducing Spam. How is Your Address Obtained?**

White Paper

Published: February 2, 2004

---

Produced by:

twentysix New York  
a business solutions provider

62 West 45th Street  
New York, NY 10036

[www.26ny.com](http://www.26ny.com)



---

## Introduction

Unsolicited commercial email (spam) is an unavoidable consequence of having an online presence. If your email address is made available to customers, it is likely to be available to spammers. To deal with spam, it is helpful to understand how your email address gets on the lists.

A March 2003 study by the Center for Democracy & Technology attempted to analyze common activities of Internet users and look for evidence of some activities that result in one email address receiving more spam than others. This study showed that the vast majority of spam comes from posting an email address on a public web site or to a public news group. The following are their major conclusions:

- By an overwhelming margin, the greatest amount of spam received was to addresses posted on the public Web
- Most users have no idea that their addresses have been harvested until they begin receiving spam
- Addresses posted in the headers of Newsgroup messages can receive significant spam, though less than a posting on the public Web
- Obscuring an email address is an effective way to avoid spam from harvesters on the Web or on Newsgroups
- Domain name registration does not seem to be a major source of spam
- Even when an email address has not been posted or shared in any way, it is still possible to receive spam through various 'attacks' on a mail server

---

## Reducing spam at home

To reduce spam at home:

- Never respond to a spam email  
For a spammer, one 'hit' among thousands of mailings justifies the practice.
- Never respond to spam email's instructions to be removed from their mailing list  
This only alerts the sender that this is a valid address, which greatly increases its value. If you reply, your address is placed on more lists and you receive more spam.
- Never make lists of email addresses – and if you do, do not email the list  
Everyone gets email from friends with jokes or news that they in turn pass on to other friends. The address list becomes very large, and finally it falls into the hands of someone in the spam trade. To pass on an email to other people, send a separate copy to each recipient, or send it as a BCC (blind copy) and hide all of the addresses.
- Never sign up with sites that promise to remove your name from spam lists  
Each of these sites are used by one of two kinds of recipients: sincere, and spam address collectors.  
The first kind of site is ignored (or exploited) by the spammers, the second is owned by them – in both cases, your address is recorded and valued more highly because you have just identified it as valid.

- Do not post your address on your Web site  
It seems like a good idea at the time, but posting your email address on your personal home page is an invitation to spammers. Spammers and the people who sell spam as a business have software that 'harvests' email addresses from the Internet. This software crawls through the Internet seeking text strings that are -something-@-something-.-something-. When it finds one, it catalogs it on a database of other email addresses to be used for spam purposes.
- Do not give your email address without knowing how it will be used  
Read the terms of use and privacy statements of any site before telling them your address. If a Web site is asking for your email address, they want to use it for something. If you are uncertain of the sincerity of a Web site, do not pass on your address.
- Use a second email address when posting to Newsgroups  
Newsgroups are gathering grounds for spammers. If you post to a group, you are going to get spam – it is just a matter of time. If you want to participate, have a public address and a private address.
- Use a spam filter  
While there is no such thing as a perfect filter, anti-spam software can help manage spam. Some of it is cumbersome, and some works better than others; you might want to try a few.

---

## Reducing spam in the business world

The following technologies are the most frequently used to curtail spam in business:

### ***Content filtering***

This approach scans the subject and body of a message, searching for specified individual words and phrases. To meet your specific needs, a customizable list of words is supplied with these products. While appealing in its simplicity, this method is too crude to be considered as a total solution. If the list of words and phrases is sufficiently comprehensive to block most spam, it will also block many legitimate messages.

Additionally, many spammers succeed in thwarting content filtering by disguising certain key words, misspelling them, and by embedding text within file types that the scanner cannot read. Content filtering is a useful method when used as one aspect of a total solution.

### ***Heuristic filtering***

Heuristic filtering scans message subjects and contents looking for patterns, applying rules to each message to determine its degree of compliance with known spam words and phrases. A message is then classified by a total score, and that score determines if a message is spam or not. Some applications allow the strength of the heuristics applied to be selected by the user – the stronger the heuristics the more spam that will be blocked – but this also increases the risk of blocking more legitimate messages.

## ***Tar pitting***

Tar pitting is an entirely different approach to combat spam. Instead of inspecting the contents of a message, tar pitting looks at such factors as the number of recipients or the number of unsuccessful delivery attempts. If a message has more than a specified number of recipients, for example, a delay is inserted between the delivery times of the message to each recipient. This delay has the effect of 'tar pitting' the spammer, causing them to assume that the connection has stalled and cease sending. Another example of tar pitting counts unsuccessful attempts to deliver a message. When this count exceeds a specified amount, the sender's IP is blocked for the remainder of the session.

## ***Blocking / black list***

Similar to content filtering, spam blocking simply prevents messages from being delivered to the intended recipient if it was sent from a known spammer. Spammers can be identified by their email address, domain, server, IP address, or range of addresses. Products offering this feature have a predefined list of known spammers that can be updated by download. While simple, this solution requires almost daily maintenance because new spammers surface constantly. As with content filtering, blocking is useful only as one part of a complete solution.

## ***Bayesian filter***

Named after Thomas Bayes, an 18th Century English mathematician who developed a means of calculating the probability of an event occurring, Bayesian spam filters calculate the probability of a message being spam, based on its contents. Unlike simple content-based filters, Bayesian spam filtering learns from spam and from good mail, resulting in a very robust, adaptive and efficient anti-spam approach that – best of all – returns hardly any false positives.

## ***What else can be done?***

Disguise email addresses posted on public Web sites.

Spammers 'harvest' email addresses with computer programs that scour web sites, collect and process addresses, and add them to spam mailing lists. If an address must be posted on a public site, it is useful to disguise the address through simple means, such as replacing 'example@domain.com' with its HTML equivalent. For example, the letter 'm' in HTML is represented as `&#109;`; the email address me@mydomain.com can be encoded as:

```
&#109;&#101;&#064;&#109;&#121;&#100;&#111;&#109;&#097;&#105;&#110;&#046;&#099;&#111;&#109;
```

If your employer places your email address online, ask the Webmaster to make sure it is disguised in some way.

---

## **Useful links**

<http://www.ordb.org>

<http://www.spamcon.org>

<http://www.spamcop.net>

<http://mail-abuse.org>

<http://www.spamlaws.com>

<http://spam.abuse.net>

<http://www.cauce.org>

**twentysix**  
NEW YORK