



HOW TO SPAM-PROOF YOUR LIFE

by: Joe Halbrook, CTO
Permission Technologies
<http://www.CleanMyMailbox.com>

Have you ever thought about how much time you spend each day, week, or month scanning your e-mailbox to discern the "good stuff" amidst all the other "refuse?"

"The average corporate employee spends an hour a day going through their email. If just 1/6th of that time is spent identifying and deleting spam, that's ten minutes a day, or about 41 hours a year -- more than a 40-hour work week!" - John Audette, I-Sales December 21, 2001 Issue #1474.

"Between 2% and 10% of inbound Internet corporate email can currently be classified as spam, with that number expected to grow to 10%-20% during the next five years (consumer email already comprises about 25% spam)." - Meta Group [Meta 1122]

"A report shows an alarming increase in spam attacks over the last year - increasing from 0.70 million [email volume] in terms of unauthorized mass mailings in April 2001, to around 3.25 million in February 2002." - Business Week April 2002

"Junk mail inflicts an annual cost of 10 billion euros (US\$8.7 billion) on Internet users." - e-Business Advisor-Reduce the Effects of Unwanted Email, 07/01/02

"29% of interviewed organizations had reported suffering email intrusion classified as spam." - KPMG 2002 Global information security survey

"About a third of email the average American receives daily is spam, up from just 10 percent in 1997, consumer groups said." - Gannett News Service 2002

"Hotmail, owned by Microsoft, is, by virtue of its 110 million users, among the world's biggest email providers. It is, therefore, one of the world's biggest spam buckets. The number of messages it gets each day is closing in on 2 billion. Up to 80 percent are spam." - Houston Chronicle July 2002

"Estimates that 34 percent of all messages handled by companies relate to unsolicited commercial email." - Gartner 2002

"Spam is estimated to be costing Internet users Euro 10 billion a year worldwide."
- The European Union, February 2002

"Between 25 and 10% of inbound Internet corporate email can currently be classified as spam, with that number expected to grow to 10% - 20% during the next five years (consumer email already comprises about 25% spam)." - META Group, 2002

Add it up and, if you're like most people with even a moderate spam (Unsolicited Commercial Email, also known as UCE) problem, you might find that you're actually spending an hour or so weekly, maybe even daily - having to invest your valuable time into such an unnecessary task. I don't know about you, but I could sure find plenty to do with an extra 2 to 5 hours a month.

And, if you own an on-line web site, you already know that the amount of spam you receive is getting ludicrous. Over 50% of all incoming e-mail is spam these days. And the problem only appears to be increasing with time.

What can be done, if anything, to reduce the amount of spam we have to look at down to just a trickle? Anything?

Believe it or not, in just 30 minutes, you can take measures to insure that this can become a reality. At least a dramatic decrease in the amount of spam can be achieved.

This is a short writing, but it's all you need to really and truly spam-proof your life!

Here are some things that will help:

- 1) **N**ever respond to the unsubscribe links at the bottom of spam mailings. Especially, if they result in an email message with "remove" in the subject line. This will only validate your email address, and result in it being sold to even more spammers.
- 2) **N**ever publish a bare mailto: tag on your web site.

One of the most common ways that spammers collect (harvest) email addresses from web sites is by using spambots (called robots, spiders, or crawlers) which visit your web site and hop from link to link collecting phrases which have an '@' character in them - those mailto: email addresses - your email addresses!

But, there are numerous techniques that provide an alternative way of displaying your email address and, at the same time, fooling the spambots so they don't find them.

Here are just a couple of those techniques:

a) Using SSI (Server-Side Includes)

By using SSI calls to a CGI script on your server, you eliminate the need to code mailto: tags.

Example:

Contact us here: `<!--#exec cgi="/cgi-bin/print_addr.pl"-->`

In the /CGI-BIN subdirectory of your web server, you simply include a short Perl script named print_addr.pl to display the mailto: tag:

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
print "\<a href=\"\&#109\;ailto\&#58\;youraddr\&#64\;yourdomain\&#46\;com\">\" .
"youraddr\&#64\;yourdomain\&#46\;com\</a>";
exit;
```

When the server processes the SSI line above, it will call the Perl script (runs on almost all web servers) which will output the <A HREF> tag dynamically, so that when spambots visit your web pages, they never see the '@' sign, and thus can't harvest your email addresses.

Notice also the use of encoded characters that will fool the spambots by hiding the : and @ symbols in the link anchor. You can find tools that will do this encoding for you.

One is located here: <http://www.CleanMyMailbox.com/free>

b) Using Javascript

With just a smidgen of Javascript code, you can provide the same client-side protection against roaming spambots and harvesters. Just place this code in your HTML pages wherever you want to display the email addresses:

```
<script language="JavaScript">
<!--
document.write('<a href="&#109;ailto&#58;your
addr&#64;yourdomain&#46;com">youraddr&#64;yourdomain&#46;com</a>');
// -->
</script>
```

NOTE: You should make sure the text of the above (and all Javascript code) is not line-wrapped in your pages, as this will result in unpredictable results.

- c) Use a contact form on your web site, instead of an email address.

When you provide an HTML form for email contact with your site visitors, not only can you manage the incoming correspondences more efficiently by having them come to one place, but you also remove the possibility of roving spambots harvesting email addresses on your web pages.

There are many HTML form-to-email scripts out there, and most of them are FREE. Just search any search engine using the terms "formmail" or "form+mail". You should be able to find a simple script and install it in no time.

If you need assistance, there are thousands of references on how to install CGI scripts, or you can even hire a web developer, who should be able to set it up in under an hour.

- 3) **N**ever use your "main" email address when you subscribe to a new publication.

Always use an address that you can either abandon or filter if you try to unsubscribe and it's not honored, or you start to receive a lot of spam after subscribing to a publication.

Some server-side programs allow you to create "throw-away" alias addresses for this very purpose.

- 4) **U**tilize an anti-spam program for your POP3 mailbox.

By anti-spam program, I mean a program that filters out your incoming UCE (spam) mail so you don't have to waste time doing it manually.

In this area, there are currently five common methods of filtering incoming spam from your mailbox. You must decide which is best for your situation:

- a) Email software setting modifications.

This technique involves your manually setting up filtering criteria to catch incoming UCE. It also involves your manually filtering Sender addresses of those UCE that get past your filters.

This technique also requires that you periodically update your filtering rules as the spammers find their way around them. Many times this is at least weekly.

- b) Client workstation anti-spam software.

This technique involves running a filtering program on your workstation "between" your actual mailbox and your email software, as you pull in the incoming mail.

Again, this technique will require frequent updating of the filtering rules and

blacklist databases - much like you have to update your virus database software periodically.

It also requires processing time on your PC workstation. If you don't have a "large" spam problem, this may be negligible. If you do, it can take between 2 to 6 times the amount of time it usually takes to pull in your mail, in order for it to interrogate each incoming item.

The price is right: between free and under \$100. You can find it at most software download sites.

c) Server-side ISP-imposed spam filtering.

Of course, from the ISP's viewpoint this is the most desirable method of removing spam email. Because it is a way to reject tagged spam messages prior to delivering them to a mailbox.

However, be careful if your ISP uses this approach. Why? Because, many times, any email that is tagged as spam (correctly or incorrectly) is simply "bounced" and you will never even know it was sent to you. When the decision to tag the email is done so incorrectly (and no solution is 100% accurate in tagging email items as such) you could stand to lose \$\$\$ if you receive business email at such a filtered email address.

And, how are such taggings determined? Well, there are numerous methodologies being implemented - most which depend on a software algorithm to make such decisions. Or, most recently, licensing agreements between 3rd party "guarantors" of non-spam mailings, such as Habeas, Inc. (<http://www.habeas.com>) and theoretical opt-in mailing publishers. But, watch out for such implementations, since the burden of proving permission for such mailings is still unclear. My guess is that you will still receive a measure of unwanted email, until permission becomes more quantifiable.

d) Server-side spam filtering services.

This technique has been implemented in a number of ways. But, the general idea is to remove UCE and other unwanted email before it enters your email software (InBox) - while it's still sitting on the mail server.

Some software solutions ask you to update your MX record (a DNS entry that specifies where your email should be routed) to point to a middleware mail server.

At this middleware mail server, your mail is "cleansed" of UCE and only the untagged "good" email is forwarded on to your normal mail server.

This is a nice implementation, because it has no affect on your access to email, and you only see non-tagged email when you download your mail into your email software on the desktop.

But once, again, you must remember this solution is based upon ever-changing 3rd party software solutions that make determinations of what is and is not unwanted email, based on internal algorithms.

The danger here is that it invites a viscous cycle of changing algorithms and compliance because, believe me, spammers use and study the same software. As they learn how to get past the filtering mechanisms, the software authors have to change their algorithms. This cycle goes on and on, and in the end, we still have a spam problem.

e) Server-side reverse spam filtering.

This, in my opinion, is the best practice for eliminating UCE spam. The reason: Instead of relying on a 3rd party definition of what is and is not spam email, this solution allows each individual mailbox owner to decide what truly is and is not unwanted email.

The concept is to filter EVERYTHING that comes into your mailbox, the first time. As you inspect the filtered email, you make a decision as to whether you will accept email from the Senders, based on either their address, the subject line, or the content of their message.

If you wish to continue to receive email from a given Sender, be it your favorite newsletter publishers, your family or friends, etc. you simply add the Sender to a whitelist which is a simple database of Senders that you will accept email from.

Our reverse spam filter solution (CleanMyMailbox.com) allows you to whitelist an address with just one mouse-click. Better yet, any time someone's message is filtered the first time, our solution can send that Sender an authentication email to allow him to prove that he is not spamming you. He does this by clicking on a link in the authentication email, which delivers his original email to your mailbox, and adds his email address to your whitelist. This automates the whitelisting function for you, although you can easily override that whitelisting request.

Adversely, if you never want to accept email from specific Senders, based on their address, the subject line, or the content of their message, you simply add them to a blacklist for your mailbox. (Again with our solution, you can do this with just one mouse-click.)

The beauty of this strategy is that it:

- 1) allows the mailbox owner to make decisions as to what is and is not unwanted email, instead of allowing a 3rd party to do so on the mailbox owner's behalf
- 2) removes the possibility of false-positive and false-negative spam tagging
- 3) negates the need to be involved in the vicious cycle of trying to "outsmart the spammers" and continuously needing to update our filter software

4) gives the mailbox owner absolute control of his mailbox

Well, there it is. Just a few suggestions that might seem simple, but can save you hours of time each month in not having to deal with unwanted email.

Like the old sayings goes: "Where there's a will, there's a way." If you're willing to spend 30 minutes now, you can enjoy a spam-free life in the not too distant future. And the savings in time could be substantial.

Thank you for spending the time to read this. I hope you can make use of these suggestions and implement a winning strategy.

Sincerely,

Joe Halbrook, CTO
Permission Technologies
<http://www.CleanMyMailbox.com>

"We eliminate spam, while you save time"

p.s. Know someone else who complains about spam? Why not pass this information on to someone else who could use it? It's as easy as forwarding it right now.