

# SPAM: Open the Can Carefully...

By Aaron Turpen

SPAM: Open the Can Carefully...

Aaron Turpen  
aaron@aaronzwebworkz.com

Aaronz WebWorkz <http://www.AaronzWebWorkz.com>

In the past several years, the word "Spam" has changed its common meaning. Until the mid nineties, the word "spam" was a household name referring to a "mystery" canned meat from a company called Hormel. It was epitomized in a Monty Python skit known as "The SPAM Skit." They managed to say the word "SPAM" more than a hundred times in two-and-a-half minutes.

Nerds being nerds (name someone you know who you'd consider a "computer geek" who DOESN'T know any piece of Monty Python word-for-word), the name soon gained a new meaning. As unwanted newsgroup postings on the Usenet grew, they began to be called "SPAM" for their repetitiveness. Eventually this came to be a "catch-all" phrase for any unwanted communication through a computer.

Now the word is still a household name, but has a completely new meaning. Meat in a can has nothing to do with what we label "SPAM" today. Generally the term is in reference to unwanted commercial email. UCE (Unsolicited Commercial Email) is the proper term for what most people term to be "SPAM."

Whatever you call it, you probably hate it. In several polls (both official and amateur), Spam has been listed as the number one annoyance to users on the Internet. It is talked about more and more often as even the politicians have begun to "do something about it." The trouble is no one is REALLY doing much to stop it on a grand scale.

There are many steps in the right direction, however. For now, let's talk about how someone, like you, puts themselves in a position to receive Spam. Then we'll discuss how you can avoid or get rid of it.

## Getting On the SPAMmer's List

There are three common ways that email addresses get put on the SPAMmer's list.

1 - Spiders & Robots: The most common way to get listed is to post your address on a website, forum, chat room, or public profile (such as MSN, ICQ, About.com, etc.). These addresses are easily gathered by programs called "spiders" or "robots." These programs simply troll the Web looking for email addresses to add to the SPAMmer's list.

2 - Nefarious "Opt-In" Scams: The next most common way to get your address listed is to give it to a questionable business on the Internet (usually with all good intentions). That business may then turn around and sell it to someone else as a part of a list.

3 - Random Address Generation: This is another tactic employed by SPAMmers and it's just what its name implies. A piece of software generates random addresses using commonly-known domains (hotmail.com, msn.com, earthlink.net, etc.).

Once your name is on a list with one SPAMmer, it will soon make its way to more. Most of those who build these lists are in the business of selling these lists as well. Not many SPAMmers build their own lists anymore – unless they're very small-time or have a specific way of gathering these lists that makes it very easy. You'd be surprised at how much time it takes to actually generate a sizeable list of email addresses – excepting the random generation method. To get a good list of email addresses – a list that is fairly low on “bad” addresses – takes time and considerable computing power. This is why most “harvesters” (as they're commonly called) are not SPAMmers themselves.

These lists are sold to anyone who will pay the money to obtain them. As the sending of UCE has become more and more competitive, these lists have become more and more “targeted” towards specific industries. Some lists are great for eBay users, some are great for get-rich-quick schemes, some are better for medical markets.

### Staying Off The SPAMmer's List

If you spend any amount of time surfing the Web – especially if you use chat rooms, forums, or other publicly-displayed message areas – you need to get a “disposable” email address. These are widely available for free from places like Hotmail.com, Yahoo.com, and any number of smaller destinations on the Web. If a chat room or user group requires that you post a public address in your profile, use that disposable address. If you post in the UseNet or other groups, set up an email address with your ISP specifically for that posting.

Before giving your real email address to ANYONE, make sure you know who they are. Friends and family are obvious, but what about that business you're giving an address to? How about that eBay seller? Know who they are and whether you can trust them before you give that email address to them. Check if they have an “anti-SPAM policy” or “privacy policy” listed and read what it says.

### Getting Rid of SPAM You Already Receive

Most email clients, such as Outlook Express, include filtering systems that you can employ to block, trash, or otherwise deal with questionable emails. I have filters that take any email with three or more ! marks (!!!) in the subject and put it in a “Crap” folder. Another filter puts anything with “MLM,” “FFA,” or “Network Marketing” into the same folder. A third has a list of known SPAM addresses that are automatically dumped into the “SPAMforSpamCop” folder. After going through the Crap folder and scanning the subjects to be sure there aren't any legitimate emails in there, I then move all of those to the SPAMforSpamCop folder as well. That entire folder is then packaged up and sent to SpamCop.net for dissection. If you need more information on SpamCop.net, please refer to my article “Reporting Spam to SpamCop.net” on my website. You can read that article here:

<http://www.aaronzwebworkz.com/resources/newsletter/articles.shtml?spamcop>

If you haven't already done so, set up at least one more (I use several) email address. If you sign up for a lot of one-time mailings (eBooks, articles, etc.), consider using a service like SpamGourmet (<http://www.spamgourmet.com>). You can sign up for temporary email addresses that will work only the specified number of times before deactivating. I use them for one-time mailings or, say, a “five-part” series mailing. Then, if they send anything more, it will reject it and I'll never have to deal with it.

Your main email address should not be easy to guess. A good test for this is to call someone who doesn't know your email and ask them what they think your email address probably is. If they can't

guess your username in the first few tries, you've got a good one. If they can, you need to reconsider it or do something to change that.

#### Attacking the SPAMmer

Besides reporting them to SpamCop, what else can you do? Well, if you have a little free time, you can do a few other things to hopefully make their lives miserable in return.

If the SPAM is about a get-rich-quick or multi-level marketing scheme, report it to "uce@fcc.gov." The FCC is now cracking down on illegal schemes online.

If the SPAMmer asks you to visit his/her website, do so. Then look around for a contact form or email address. If you find a form, send them hate mail through it. This is very stress-relieving. If you find an email address, you can get even nastier. NEVER send email directly to them! However, you can go to FFA sites (Free For All sites) around the Internet – just search for FFA on any search site – and post their email address to it. These sites are hotbeds for email gathering for later SPAM. Maybe if they receive enough SPAM, they'll see how hateful it is and stop doing it themselves.

Finally, you can complain to the SPAMmer's ISP directly. If you find their website, you can do a simple search using your domain registrar (go to [www.DirectNIC.com](http://www.DirectNIC.com)). They have a free tool available to anyone called a "whois search." Every registered domain name is REQUIRED to have a few bits of valid information attached to it. One of those pieces is the "nameserver." These usually look like "ns1.domain.com" or "dns.domain.com." Replace the "ns1" or "dns" with "www" and put the URL into your browser. WALA! That is probably the SPAMmer's web host! Now start looking around for an 800 number. Don't send email, as this host may be the SPAMmer himself. You never know. Calling them to complain is always a good way to let off steam and feel like you've at least made a mark, even if you didn't accomplish much. If you're really bored, keep a list and stop at pay phones as you wander the mall or down the street and call just to shout names at them before hanging up. Again, a great way to let off steam.

Finally, if the SPAMmer seems to be using a legitimate email (go ahead, use an address from SpamGourmet to try their return email out), complain to the ISP that hosts that email. Usually these are "disposable" addresses. Use these for the most common ones:

abuse@yahoo.com  
abuse@hotmail.com  
abuse@excite.com

No matter how you go about it, combating SPAM influx to your inbox is something that every Internet user has to face. Otherwise, you'll soon be flooded with an unstoppable amount of unsolicited email. Even those who advocate using UCE as a marketing tool have to admit that there has to be so much of it now that its payoff is becoming ambiguous. Good luck in your battle!

=====

Aaron is the proprietor of Aaronz WebWorkz, a complete provider of web services for small business. Need traffic? Go to [www.HitsGuaranteed.net](http://www.HitsGuaranteed.net). Need hosting, consultation, or web design/development? Go to [www.AaronzWebWorkz.com](http://www.AaronzWebWorkz.com). Whatever your online needs, Aaronz WebWorkz has a solution.

[Get-Articles.com](http://Get-Articles.com) : 1000's of reprintable business and internet marketing-related articles.

[Submit your article for reprint.](#)