
This chapter is taken from the e-book called "How Do I Stop Spam?"
by Steve Davis & Gloria Craney. Click here to purchase the book!

## What is Spam?

Other than the canned meat distributed by Hormel, spam is a term used to describe Unsolicited Commercial Email (UCE) or Unsolicited Bulk Email (UBE). Some say the keyword is Unsolicited, but we're sure many people have received emails without soliciting them that were not commercial, nor were they sent to multiple accounts. For instance, there's the occasional joke sent in mass from friend to friends and back again, or that all-important virus alert, or the occasional inspiration, etc. But you know these people so it can't be spam, right? Well, it depends on to whom you speak. There are those who dislike having their mailbox fill up with jokes almost as much as commercial advertisements but because its done by someone you know it's tolerated. So, our definition of spam is any unsolicited email sent in bulk by an unknown entity that is uninvited.

In general, the predominant subjects of spam email are the following:

· Chain letters.
· Pyramid schemes (including Multilevel Marketing, or MLM).
· Other "Get Rich Quick" or "Make Money Fast" (MMF) schemes.
· Offers of phone sex lines and ads for pornographic web sites.
· Offers of software for collecting e-mail addresses and sending UCE.
· Offers of bulk e-mailing services for sending UCE.
· Stock offerings for unknown start-up corporations.
· Quack health products and remedies.
· Illegally pirated software.

If you are reading this book, we assume that your toleration level has been compromised with unexpressed frustration and your bloating mailbox can no longer be ignored! Your finger is probably sore from banging on the delete key trying to rid yourself of the junk threatening to take over your inbox but it comes back, day after day, month after month, in growing amounts. But hope is near and you do not have to get a new email artery to lessen the effects of the spam-produced fat cells clinging to your inbox. There are steps you can take, with a marginal amount of effort and computer skills, to reclaim your inbox and put those fat gremlins where they belong, at a distance. With a little exercise and a fat blocker your inbox will smooth out in no time.

## The History of Spam

It's been said that the term spam originated from an old Monty Python sketch that took place in a restaurant where everything on the menu came with spam (the food product). Spam, spam, spam, spam, was repeated over and over in the sketch and someone used it to coin the meaning of an unsolicited commercial post on Usenet (electronic bulletin boards, or better known as newsgroups) in the early 1990's and it stuck, much to Hormel's dismay, but that's another story better left alone.

### Adventures of the First Spammer

One of the first spammers was Dave Rhodes, a college student who wanted to make a little extra cash with little extra effort. He sent the artery clogging fat cells in motion when he cross-posted a pyramid scheme on Usenet. It was later turned into email and file uploads to Bulletin Boards with

the Header "MAKE MONEY FAST". How well Dave did with his spamming adventure is unknown. Internet lore has him in prison for wire fraud but that cannot be proven and was most likely created by those who had to clean up his mess on the newsgroups. Vengeance is mine, sayeth the newsgroup administrators.

**First Usenet Attacks**

Dave may have been one of the first spammers but not the most notorious. That title was given to two Scottsdale, Arizona lawyers, Laurence Canter and Martha Siegel, when they cross-posted their Green Card Assistance Services to 6,000 newsgroups at once on April 12, 1994. When thousands of Usenet users logged on to their favorite newsgroups, expecting to read the latest news on their topic of choice, they were met with Canter and Siegel's Green Card advertisement. They overstepped one of Usenet's basic tenets: post only relevant information to specific, topic rich, newsgroups. Usenet users were enraged and let the two lawyers know with insulting email messages (flames) and mail-bombs: a large email that takes up a huge amount of space on the receiver's server that clogs the system and can cause it to crash.

**The Birth of Mail Bombs**

We do not advocate the use of flames and mail-bombs. For one thing, mail-bombs can end up causing you to pay a large restitution to the server company for crashing their computer system, and flames are ineffectual and immature. But this was 1994 when spam was still relatively new and Usenet users were protective of their newsgroups. No one wanted to weed through irrelevant advertisements to get to the meat of the topic. They expected an apology from Canter and Siegel and got none, causing more frustration and more mail-bombs. After Canter and Siegel's server crashed more than 15 times, their account was terminated. They opened another account with a different server but on May 20th that server terminated their account because of a TV show where Canter boasted that he would spam again.

**Internet Commerce Blooms**

What set Canter and Siegel apart from other spammers and helped install them into the Spammers Hall of Fame was their unrepentant stance and the book they wrote, "How to Make A Fortune on the Information Superhighway: Everyone's Guerrilla Guide to Marketing on the Internet and Other Online Services." Their reference to "Guerrilla Guide" says it all. They not only supported spamming as a viable marketing tool, they said everyone had a right to advertise on all the newsgroups as they saw fit. They even likened the Usenet community to a true communist society because advertising isn't allowed, except by the government who owns everything. This unbelievable statement comes after they chide the idea that Cyberspace can have a viable community. There are many such contradictions throughout this book, which didn't make the best sellers list, but it did set a precedence that most spammers still abide by: If you don't like it, delete it, we're just exercising our right to free speech. The free speech debate is still a hot one between spammers and Anti-spammers and until there is a law that spells it out for all concerned, it will continue to be debated.

Canter and Siegel's book appears to no longer be in print but you can buy a used copy on Amazon.com and the authors are offering it in PDF format that can be downloaded for $8.00, also on Amazon.com. We personally would not pay for the book unless we were doing research on how not to market on the Internet Superhighway. In fact, we did read one Internet marketing how-to manuscript that spawned the creation of this E-book. Not because it offered good Internet marketing concepts but because it offered spamming tips and tricks, including how to harvest email addresses. The E-book you're reading now is our way of fighting back!

## What's Wrong With Spam?

### Time Costs

If you are receiving two or three Unsolicited Emails a day you probably think spam isn't all that bad, it's just a minor inconvenience. But if you are receiving 40 to 50+ a day, and you're spending an average of 10 seconds each to decide what you want to do with each message, then you're wasting around 60 hours a year dealing with spam. That's over seven workdays wasted each year! Not to mention the raw frustration and distraction of doing a task that takes you from your productive work.

### Server Costs

Then there are the costs to your server of having to manage large amounts of mail entering their system. When too much is sent or arrives at one time it can cause the system to crash, leaving their customers without the ability to send or receive email. One Internet Service Provider that's known for allowing spammers to send bulk mail through its system crashed when several of its users sent large amounts of mail at the same time. It was down for several days and many anti-spammers thought that justice had its own way of dealing with spammers and hoped the Provider would start enforcing it's own Terms of Use. No such luck, its back and spammers are sending their junk mail in mass amounts once again.

### Consumer Costs

Some consumers have to pay long distance phone charges to connect to the Internet (mostly in countries outside of the US) and some countries charge for every phone call made by their customers. In these cases, the user wastes connection time by downloading and sorting through unwanted email.

### Privacy Costs

It's our belief that the biggest problem with spam, other than having to look at it, is that 90% of those sending it do it in a fraudulent way. They buy software that hides their identity, forges email headers, steals others' identities (read about one man's experience with identity theft at Behind Enemy Lines), use bogus cancellation addresses, and stake out a claim to their right to intrude on your privacy. Some even claim you signed up to receive their spam advertisement (which may contain some measure of truth but we will comment on that under How Did They Get My Email Address? If that were true, why then do they go to such lengths to hide their true identities?

### Bad Press for True Opt-In Markets

Then there are the spammers who are compromising viable opt-in markets. Opt-in means you signed up to receive email on something of interest to you. On every email there is an opt-out feature that's honored by reputable businesses or those merely offering free information on specific topics. Spammers are now adding opt-in, opt-out, to their spam to make it look more legitimate and fool you into thinking that maybe you did sign up to receive their spam. But if you're dealing with a true spammer, the opt-out address is bogus and your email will simply bounce. These tactics are making it more difficult to know the difference between a spammer and a reputable opt-in email that finds its way into your inbox.

### Ethical Costs

The ethical costs of spam might best be explained by the experience of one of the authors of this book, Gloria Craney:

The single most corrupt type of spam comes from illegal pornographic material, whether it's

wanted or not. I'm not referring to the average porn site. Receiving and interacting with pornographic material is a personal choice and I'm not here to make a moral judgment on those who request this kind of material. But when it comes to the sick violent porn, child pornography, and things like bestiality that threaten to invade every household in every country where there's a connection to the Internet and access to an email account, I draw the line. It is totally unacceptable and leaves a vial taste in my mouth. I ignored the spam I was receiving, which amounted to about 40+ a day, until I received one on bestiality.

Like most people, I had no idea how to deal with my bloating inbox other than to delete the junk and not let the irritation get the best of me. But when I received the pornographic material on bestiality I knew I had to do something. I went in search of how and what I could do to rid myself of disgusting unsolicited email. It took awhile, with a lot of trial and error, but I learned to read email headers and sort through what was real and what was forged. I began to methodically report every piece of spam landing in my inbox. If I didn't have time to trace it back to the sender upon receiving it, I'd save it until I did have the time. Slowly the amount started to decrease and I felt empowered and in control of my mailbox once again.

Believe it or not, I even felt disappointed when a piece of spam didn't land in my inbox. Guess I liked taking back control a little too much but I've since regained some measure of composure. Since then, I've found ways to accomplish the same thing without having to know how to read email headers or how to track the source. Plus, I found ways to keep my personal email address out of the hands of spammers and harvesting robots and so will you!

## Who Benefits From Spam?

We believe that the people making the big bucks are those selling spamming tips and tricks disguised as Internet marketing how-to's, the software companies that create spamming products, and Internet Service Providers who support spammers. Marketing to spammers is far more profitable than being a spammer. We're sure there are people who have tried using spamming techniques to market their services or products that believed they were doing the right thing, only to discover that they compromised their business and were threatened with loosing their Provider's support.

One person we know personally decided to market a new affiliate program by targeting other online businesses that supported affiliate programs on their sites. He used a software program to harvest email addresses from his targeted market and sent his message in mass. In less than 24 hours he received a phone call from his Internet Service Provider informing him of his violation of their Terms of Use and if he continued to send out unsolicited bulk email his account would be terminated. He received hundreds of emails from disgruntled business owners and out of the 6,000 emails he sent, he got 30 positive responses. If you can believe it, he actually thought his spamming experience brought results. The only reason he will never do it again is because he doesn't want to loose his Internet Service Provider. He gave no thought to the fact that he alienated 5,970 potential customers. Spamming is not profitable, but selling to spammers appears to be.

## How Did They Get My Email Address?

There are several ways spammers acquire email addresses. They buy them from someone else, purchase software that harvests email addresses off the Internet, hack their way into online Providers like American Online and send AOL's users bogus deals to fraudulently acquire users passwords and email addresses. If you belong to a newsgroup, ever entered a chat room, signed up for a newsletter, posted on a bulletin board, placed an ad on any classified ad page, sent an e-card, entered sweepstakes, or signed up for anything that required you to give your email

address, your address can and will be harvested. The only exceptions are secured server sign-ups and an opt-in list that secures its address lists in databases that cannot be accessed by robot software.

**Online Surveys**

Have you ever gone to a site that asks you to fill out one of their surveys so they can better serve you? On the survey there is everything from gardening to skydiving. If you filled it out you have just opted-in to receive information on the topics you selected and anything remotely similar will find its way into your mailbox. You have just elected to receive spam. Always read the fine print before filling out any survey, or information form, and never give them your personal email address. More about how to do that and still receive mail you do want in your personal email account under Defensive Measures.

**Email Address Posted on Your Website**

If you have a Web site then you are most likely an unprotected target for email harvesting. But there are ways to protect your email address and still offer your users easy access to your contact information. Not only can you protect your address but you can also give the would-be spammers something they don't want, a slap on their greedy little cyber hands. It's a righteous punishment without being overtly destructive and completely harmless to your Web site and how it functions in cyberspace. These methods are discussed under Spam Protection for Web Site Owners.

**Spyware**

Another sneaky culprit is "spyware". This is a small script placed on your computer, usually without your knowledge, during software download operations, that tracks your movement on the Internet. It was originally designed to help marketers' track advertising campaigns and create statistics on what works and what doesn't work. The problem is that spyware also has the ability to collect and send all the personal information that's on your computer-including your email address-to unscrupulous members of the cyber community, all without your knowledge. Spyware can also get into your computer via cookies (bits of data, placed on your PC by websites, that can be used to track your behavior and identity online). Even after removing the cookies, the spyware can remain and continue to track your movements on the Internet.

If you have ever downloaded freeware and installed it on your computer, you most likely have spyware hiding on your system and sending information without your knowledge or permission. Software companies that offer their products for free still need to make money. Many have banner ads or popup windows with advertisements in them that you see when you use the software. Advertising companies pay the software manufacturer to place the ads in their product, allowing the software manufacturer to offer their product for free to the consumer. An example of free software that has used spyware is Real Audio, although we understand they are no longer using it in their 8.0 version.

Be aware that firewall software will not block spyware from entering and sending information about your surfing habits to its creator. But there is a free software program designed specifically to sniff-out spyware and destroy it!