

[Spam: Where it Came From, and How to Escape It](#)

Who Cooked This!? (How did it all start?)

The modern meaning of the word "spam" has nothing to do with spiced ham. In the early 1990's, a skit by British comedy group Monty Python led to the word's common usage. "The SPAM Skit" follows a couple struggling to order dinner from a menu consisting entirely of Hormel's canned ham.

Repetition is key to the skit's hilarity. The actors cram the word "SPAM" into the 2.5 minute skit more than 104 times! This flood prompted Usenet readers to call unwanted newsgroup postings "spam." The name stuck.

Spammers soon focused on e-mail, and the terminology moved with them. Today, the word has come out of technical obscurity. Now, "spam" is the common term for "Unsolicited Commercial E-Mail", or "UCE."

Why Does Bad Spam Happen to Good People?

Chances are, you've been spammed before. Somehow, your e-mail address has found it's way into the hands of a spammer, and your inbox is suffering the consequences. How does this happen? There are several possibilities.

Backstabbing Businesses

Businesses often keep lists of their customers' e-mail addresses. This is a completely legitimate practice and, usually, nothing bad comes of it. Sometimes though, the temptation to make a quick buck is too great, and these lists are sold or rented to outside advertisers. The result? A lot of unsolicited e-mail, and a serious breach of trust.

Random Address Generation

Computer programs called random address generators simply "guess" e-mail addresses. Over 100 million hotmail addresses exist - how hard could it be to guess some of them? Unfortunately for many unsuspecting netizens - not too hard. Many spammers also guess at "standard" addresses, like "support@yourdomain.com", "info@yourdomain.com", and "billing@yourdomain.com."

Web Spiders

Today's most insidious list-gathering tools are web spiders. All of the major search engines spider the web, saving information about each page. Spammers use tools that also spider the web, but save any e-mail address they come across. Your personal web page lists your e-mail address? Prepare for an onslaught!

Chat Room Harvesting

ISP's offer vastly popular chat rooms where users are known only by their screen names. Of course, spammers know that your screen name is the first part of your e-mail address. Why waste time guessing e-mail addresses when a few hours of lurking in a chat room can net a list of actively-used addresses?

The Poor Man's Bad Marketing Idea

It didn't work for the phone companies, and it won't work for e-mail marketers. But, some spammers still keep their own friends-and-family-style e-mail lists. Compiled from the addresses of other known spammers, and people or businesses that the owner has come across in the past, these lists are still illegitimate. Why? Only you can give someone permission to send you e-mail. A friend-of-a-friend's permission won't cut it.

Stop The Flood to Your Inbox

Already drowning in spam? Try using your e-mail client's filters - many provide a way to block specific e-mail addresses. Each time you're spammed, block the sender's address. Spammers skip from address to address, and you may be on many lists, but this method will at least slow the flow.

Also, use more than one e-mail address, and keep one "clean." Many netizens find that this technique turns the spam flood into a trickle. Use one address for only spam-safe activities like e-mailing your friends, or signing on with trustworthy businesses. Never use your clean address on the web! Get a free address to use on the web and in chat rooms.

If nothing else helps, consider changing screen names, or opening an entirely new e-mail account. When you do, you'll start with a clean, spam-free slate. This time, protect your e-mail address!

Stay Off Spammed Lists in the Future

Want to surf the web without getting sucked into the spam-flood? Prevention is your best policy. Don't use an easy-to-guess e-mail address. Keep your address clean by not using it for spam-centric activities. Don't post it on any web pages, and don't use it in chat rooms or newsgroups.

Before giving your clean e-mail address to a business, check the company out. Are sections of its user agreement dedicated to anti-spam rules? Does a privacy policy explain exactly what will be done with your address? The most considerate companies also post an anti-spam policy written in plain English, so you can be absolutely sure of what you're getting into.

Think You're Not a Spammer? Be Sure.

Many a first-time marketer has inadvertently spammed his audience. The first several hundred complaints and some nasty phone messages usually stop him in his tracks. But by then, the spammer may be faced with cleanup bills from his ISP, and a bad reputation that it's not easy to overcome.

The best way to avoid this situation is to have a clear understanding of what spam is: If anyone who receives your mass e-mails did not specifically ask to hear from you, then you are spamming them.

Stick with your gut. Don't buy a million addresses for \$10, no matter how much the seller swears by them! If something sounds fishy, just say no. You'll save yourself a lot in the end.

The Final Blow

The online world is turning the tide on spam. In the end, people will stop sending spam because it stops working. Do your part: never buy from a spammer. When your business seeks out technology companies with which to work, only choose those with a staunch anti-spam stance.

Spam has a long history in both the food and e-mail sectors. This year, Hormel Foods opened a real-world museum dedicated to SPAM. While the museum does feature the Monty Python SPAM Skit, there's no word yet on an unsolicited commercial e-mail exhibit. But, if all upstanding netizens work together, Hormel's ham in a can will far outlive the Internet plague that is UCE.

About the Author

Reprinted with permission of Beka Ruse. Mrs. Ruse fights spam as the Business Development Manager at AWeber Communications. Ad tracking, live stats, and a strict anti-spam policy: Automated E-Mail Follow Up From AWeber. <http://www.emailsdelivered.us>

Source: <http://www.onlineearnings.net>