Slamming Spamming:

Tech Tips	WWW Everyone

What Is Spam

Spam of the email variety is easy to spot. It's a message (sometimes two or three!) from someone you've never heard of, advertising something that you'd never use or touting some opinion that you would rather do without, and, while it appears in your inbox, it isn't actually addressed to you.

And we all also agree on what we want done about spam -- we want to get rid of it and never get any more. The first step is hitting the delete button. But would you like to do something more active? Don't send a flaming reply; that won't accomplish anything, except to confirm that your email address is a good one. What's the right way? Read on for instructions on how to complain about spam and for hints on how to avoid it.

The Origins of Spam

The term spam was originally used in Usenet newsgroups to describe identical commercial or off-topic posts made to multiple newsgroups. It has since been expanded to include ordinary email messages, both **UCE** (unsolicited commercial email) and **UBE** (unsolicited bulk email). (If it's on the Internet, it must have an acronym!)

The use of the name of a canned lunch meat for these postings and messages was inspired by a Monty Python skit in which a group of Vikings sing, "SPAM, SPAM, SPAM, ..." in the background, eventually drowning out all other conversation. Spam certainly is doing that, particularly on Usenet, even though most news servers, including ours, run programs that identify many incoming spam posts and drop them without distributing them.

What about spam on Usenet?

Spam is more broadly defined in Usenet newsgroups. Anything that is not related to the group's subject can be considered offensive. Many groups also have specific restrictions on ads and binaries.
Complaints about Usenet abuse should be directed to the news administrator at the poster's site. At UIC, that's: newsmaster@uic.edu

What about the other SPAM?

Hormel Foods, the makers of SPAM, the luncheon meat, is good-natured about the use of their trademarked name for unsolicited email. They only ask that we use spam in all lower case for the email and save SPAM in all upper case for their product. Visit their Web site, http://www.spam.com, which celebrates "The one in good taste." There's even a SPAM fan club and, of course, SPAM "stuff", including SPAM boxer shorts if you're so inclined.

The Internet wasn't born with spam. In fact, spam on the Internet has a birthday, and I remember it -- I saw several copies of the first widely known spam message. It was sent in 1994 by a law firm advertising their services for obtaining green cards through the U.S. Immigration and Nationalization Service's Diversity Visa lottery. Posting the ad to 6,000 Usenet news groups took them less than 90 minutes. Thousands of people sent flaming email responses back to the firm, which had used its own email address in the posting. The replies swamped the firm's ISP, which responded fairly quickly by terminating their account. (There's a copy on the Urban Legends Web site: http://www.urbanlegends.com/legal/green_card_spam.html Canter was even disbarred for his trouble: from LegalEthics.com, http://www.legalethics.com/states/disbar.htm)
The lawyers behind the Green Card Spam, Laurence Canter and Martha Siegel, went on to further spam glory including writing a book about spam, *How To Make A Fortune On The Information Superhighway*. (Their company, Cybersell, Inc. was and is also the first company listed in the Blacklist of Internet Advertisers.) The book's title explains why spam is still flourishing -- it works. Not well, but at the price -- virtually free -- spammers don't need much of a response rate to turn a profit.

Why Email Spam is Bad

Face it; there's always been spam -- door-to-door salespeople, junk snail mail, telemarketing. What makes email spam worse than other forms of spam? Annoying as the others are, they have a built-in control that keeps them from being too destructive -- they cost the spammer either money or time or both.
There are no such controls on email spam. Sending email spam is virtually free for the spammer. There are software tools that can send millions of copies of a message out in a matter of minutes and there are lots of enterprising people who are anxious to sell spammers the millions of email addresses they'll need to do it. No self-respecting spammer uses their own ISP's outgoing mail services anymore; that might cost them their account. But they don't need to. There are always thousands of other machines on the Internet running poorly configured SMTP services that spammers can use.

Do you run a Unix machine or NT server?

Then you might be helping spammers by running an open email relay. If you think your machine might be an open relay, check out our "Sendmail and Open Mail Relays" Web page, http://www.accc.uic.edu/ecomm/openrelay.html, which explains how to close open relays on several popular flavors of Unix.

Email spam does, of course, cost. When we receive spam, we pay for it in time, aggravation, and perhaps charges for connect time. Businesses pay for it in the time lost as their employees sift through spam to get to their real email, in their network administrators' time, in congestion on their local networks, and in connection charges. And we all pay for the congestion that spam causes on the Internet as a whole.

How to Complain

The simplest thing you can do with spam is to delete it as soon as you receive it. But if you feel that you must do something more, and some people who worry about spam think you should, here's how to complain.

Don't complain about spam by replying to the spam message or by trying to send email to an email address given in the body of the spam and asking to be removed from the mailing list.

That worked in 1994, but spammers are much too sophisticated now for replies to affect them at all. And the From: addresses in spam messages are usually faked anyway.

What you should do instead is complain to the ISPs that the spammer used. While there are exceptions, ISPs are generally very interested in keeping their systems free from spam, both because it gives them a bad name and because it takes resources from paying customers.

-- Step 1: Find the machines the spam traveled through.

Unfortunately, figuring out where a spam message really came from isn't as easy as you might hope. You have to look at the message's extended headers -- the header fields that most email programs don't display unless you tell them to. Reading Email Headers explains how to display and interpret extended email headers, in particular, the **Received:** headers that you'll read to follow the trail that the spam message took. (Probably took, that is. Each legit mail server the message passes through will add its own Received: header, but it's quite possible for spammers to add faked Received: headers when they send their spam. So the machine that that appears to be the originating server may not have anything to do with the spam at all.)

As an example, let's consider the spam message in figure 3. It's a real spam message, but the domain names and IP addresses in it have been altered. It:

- Originated at a dialin connection, perhaps in Atlanta, belonging to bigisp.net, line 3.
- Went through a server in Spain, qrd32565.qrd.es, a.k.a. spanishisp.com, lines 2 and 1.
- And the **From:** address is on a server in the United Kingdom, englishisp.com, line 6.

-- Step 2: Check the body of the note for email addresses or Web sites.

If there are email addresses or Web sites in the body of the spam message, add their "upstream providers" to your list of addresses to complain to. Unlike the From:

address, these probably do have something to do with the spammer. Again, don't complain to the actual addresses -- aim your complaints to the ISPs that provide them service.
There aren't any Web sites mentioned in the spam in figure 3. There is an email address, **orderdisknow@freeisp.com**, so we can add freeisp.com to the complaint list. (The real "freeisp.com" is a provider of free email accounts.)

-- Step 3: Find an email address on those machines to send your complaint to.

Most ISPs have an email address for complaints about abuses of their services. It's **abuse@domain.name** often enough that you can just send your complaint there: **abuse@bigisp.net**, **abuse@spanishisp.com**, and so on. If a message to an abuse address bounces, try re-sending it to the **postmaster** account.
If you want to be sure your message will be seen by a real person, you can look the machine's IP address up in Network Solution's Whois database. DShield.org's Whois lookup page is a good way to query Whois: http://www.dshield.org/ipinfo.php
The data returned includes the name and contact info for a technical contact person for the machine.
(DShield is a new Web-based Internet intrusion detection complaint service; it collects and analyzes the intrusion attempt logs kept by personal firewalls such as ZoneAlarm. Personal firewalls were introduced in the April/May/June 2000 issue of the *A3C Connection*.)

-- Step 4: Compose and send your complaint.

Sending a note saying, "You spammed me, stop it now." won't help anyone.
Unless you include a copy of the spam message and all its headers, the ISPs won't be able to do anything about your complaint.

- Always include a copy of the spam message with your complaint, including full headers.
- Always forward the spam to the address you're complaining to rather than replying or creating a new message. Forwarding keeps the message's original headers intact.
- Make sure your complaint is before the body of the spam. ISPs get spam just like the rest of us; if your message looks like spam, they'll probably just delete it.
- Send only one complaint per ISP per spam message. Sending multiple messages won't get your complaint acted on any faster.

Speaking as someone who has to reply to spam complaints now and then, please remember that you're complaining to the ISPs that the spammer is using, not to the spammer. So please keep your complaint short and polite.

For the originating ISP and the ISPs of addresses or Web sites in the body of the spam:

> "This unsolicited email message appears to be from one of your users. Please take appropriate actions to ensure it doesn't happen again."

For ISPs used as relays:

> "This unsolicited email message appears to have been relayed by one of your machines. Please take appropriate actions to close this open relay."

-- Don't expect to receive personalized replies.

While it is true that most ISPs are happy to receive complaints about people who are misusing their services, it is also true the people who take care of these complaints at most ISPs are overworked. And they're likely to have already received other complaints regarding the spam you're complaining about. So you'll probably receive an automated "Thank you for your information" reply. I think that's just fine. I'd rather they spend their time closing the spammers down than sending replies to me.

-- Spam Complaint Web Pages

Does this all seem like too much trouble? These Web sites offer free spam complaint services.

- Spam Cop: http://spamcop.net/
- Network Abuse Clearinghouse: http://www.abuse.net/

Keep in mind that "free" doesn't mean anonymous. These services could be abused, so they're careful not to respond to false complaints.

Or you can forward your spam email to the US Federal Trade Commission's spam collection address: uce@ftc.org (http://www.ftc.gov/os/1998/9806/email.htm). [Note added May 11, 2001: The FTC's uce address seems to no longer be in use.]

Tricks to Minimize Email Spam

There's nothing you can do to prevent spam. But if you get a lot of it or if it really bothers you, there are some things you can do to protect yourself from it.

-- Never Reply To Spam

The people who worry about spam say you can reduce the amount of spam you receive by never responding to spam email, either directly or by visiting the spammer's Web site. That just identifies you as a real person who read their message. This includes replying to spammers' offers to remove you from their mailing lists. The only exception is if the email in question isn't really "unsolicited" -- say, if it's from a company that you've done online business with. Then unsubscribing is worth a try. You may even get an apology.

-- Use Email Filters

Even if you can't avoid spam altogether, you can keep it from clogging up your inbox. Most spam email isn't addressed directly to you. So, you can set up an email filter to move all messages that aren't addressed directly to you into a separate mailbox. The Eudora filter in figure 1 does just that.

You don't want to delete these messages without looking at them; there will be some that you want to read or save, such as messages from LISTSERV or LSOFT lists and also email sent to you as a Bcc: -- blind carbon copy.

-- Use Usenet Wisely

In the old days, I used to post to Usenet newsgroups that are open to the entire world. In the old days, I used to get a lot of spam email, too. The spam-to-real-email ratio for my **judygs@uic.edu** email address has dropped steadily since I stopped using it to participate in public newsgroups. This is purely circumstantial evidence, but a lot of other people have noted similar circumstances.

Unfortunately never posting to Usenet groups won't prevent you from getting spam, and I've got circumstantial evidence to demonstrate that too. Another of my accounts,

adabyron@uic.edu, is only used for demonstration purposes and has never posted to any Usenet newsgroup -- I don't think I've sent more than ten email messages from it in all. It gets about as many spam messages as **judygs@uic.edu** does.

-- Switch to Email-Based Discussion Lists

I was able to quit using Usenet because I found closed email-based discussion groups -- LISTSERV or LSOFT lists for which no one except for the group's owners can request subscriber lists -- that cover the technical topics that I commonly want to discuss. I was lucky; it's entirely possible that you won't be able to do this.

-- Use a "Throwaway" Address on Usenet

Open an email account on one of the free email services available on the Internet, such as Yahoo! or Hotmail. Use that address when you post to public Usenet newsgroups or when a Web page requires you to enter an email address, and decide that you'll live with whatever spam that account accumulates. Free accounts generally have a small inbox and/or automatic deletion of older (unread) email -- both are good antispam measures.

The bad news is that some Web pages refuse to accept this kind of email address.

-- Fake your own From: address:

Take a hint from the spammers -- avoid getting spam by using a somewhat faked version of your own email address when posting to a public forum or newsgroup. Include some text that makes your address indecipherable to an automated program but easy enough for a person to figure out. For example, I could use this From: address:

> **judygsTAKEOUT@uicREMOVE.edu**

This would make my netid and domain name useless to the average harvester, but people should know what to do with it. (Read "Help I've been Spammed! What do I do?" by Greg Byshenk before you do this, though; he explains how to do it right: http://www.byshenk.net/ive.been.spammed.html)

If your newsreader or your ISP won't let you do this, you could use a Web-based Usenet service such as Deja.com instead (http://www.deja.com/usenet). They don't have any problems with your using an altered From: address.

About UIC Usenet Groups

The UIC-only Usenet groups -- ones whose names start with uic., including all the ones used by UIC classes -- are restricted to distribution on the UIC campus. The restriction is made based on IP address, like most other UIC-only Internet services. This means that only a harvester program that was run on the UIC campus could be used to capture email addresses from posts to these groups. That's not impossible, but it does make it a little harder to harvest UIC addresses.

> Comments are welcome; please send them
> to Judith Grobe Sachs, judygs@uic.edu