Email Abuse

1.Definitions

1a. When is it email, and when is it email abuse?

Email is a tremendously powerful communications tool, used by millions of people in thousands of positive ways. Unfortunately, such a powerful tool has the potential to be used in other, less productive, ways.

Someone sending email incurs no incremental cost; sending one message costs about the same as sending 100 messages. Some folks use this feature of email to send messages to thousands, even millions, of people at once. These are usually advertisements, sometimes sermons on the sender's favorite topic, sometimes pleas for financial assistance or scams intended to defraud the unwitting. Almost all of these messages go to people who did not ask to receive them. Also, some people use email in denial-of-service attacks, using various methods to flood someone's emailbox with so many messages that their email becomes unusable. These are examples of abuse of the email system.

Also, it is possible to impersonate, threaten, disparage, or otherwise harass someone via email. These are examples of abuse on the email system, and are not the subject of this FAQ.

Notable exceptions to bulk email abuse are legitimate mailing lists, where people subscribe to receive messages pertaining to a particular subject. These lists can be large, and they can account for large numbers of messages being sent, but they are in no way abuse of the email system. Quite the opposite, in fact - they are a perfect example of the productive power of email.

1b. What is "unsolicited email"?

Unsolicited email is any email message received where the recipient did not specifically ask to receive it.

Taken by itself, unsolicited email does not constitute abuse; not all unsolicited email is also undesired email. For example, receiving "unsolicited" email from a long-lost friend or relative is certainly not abuse. The reason that it is defined separately is that email abuse takes several forms, all of which begin with the fact that the email received is unsolicited.

NOTE: Usenet convention holds that, by posting to a newsgroup, one is tacitly soliciting individual, topical replies via email.

The following are examples of soliciting email:

a.. posting to Usenet or saying in a chat group: "please send me e-mail about foobars"

b.. sending email to an advertised auto-reply address: "for more information, send email to info@..."
c.. filling out a web form which explicitly mentions email: "fill this out to get email about foo"
"fill this out to get on the mailing list about foo"
"check this box to get on the foo mailing list"
The following acts DO NOT, by themselves, constitute "soliciting"
email:

a.. just posting a message to a Usenet newsgroup or any other public forum (although individual, topical replies to Usenet posts are have long-standing status as normal Usenet practice)
b.. chatting in IRC or other chat groups
c.. simply visiting a web site
d.. filling out a survey form at a Web site that does not explicitly say it is for mailings
e.. putting one's email address on any other form, such as product registrations or magazine subscriptions
f.. posting one's email address on a web page (web page authors should clearly specify the reason an email address appears on the
page)
g.. entering into a business relationship or conducting a business transaction; for example, purchasing a product or service from a company, or downloading a free trial version of a software product from a web site.

1c. What is "bulk email"?

Bulk email is any group of messages sent via email, with substantially identical content, to a large number of addresses at once. Many ISPs specify a threshold for bulk email:

----- 25 or more recipients within a 24-hour period -----

Once again, taken by itself, bulk email is not necessarily abuse of the email system. For example, there are legitimate mailing lists, some with hundreds or thousands of willing recipients.

1d. What is "commercial email"?

Commercial email is any email message sent for the purposes of distributing information about a for-profit institution, soliciting purchase of products or services, or soliciting any transfer of funds. It also includes commercial activities by not-for-profit institutions.

1e. UBE, UCE, MMF, MLM... What do they all mean?

First, a short lesson on the term "SPAM". Spam describes a particular kind of Usenet posting (and canned spiced ham), but is now often used to describe many kinds of inappropriate activities,

including some email-related events. It is technically incorrect to use "spam" to describe email abuse, although attempting to correct the practice would amount to tilting at windmills. For more on the history of the term, look for "2.4) Where did the term 'Spam' come from?" in http://www.cybernothing.org/faqs/net-abuse-faq.html

UBE: Unsolicited Bulk Email
Email with substantially identical content sent to many recipients who did not ask to receive it. Almost all UBE is also UCE (see next). UBE is undoubtedly the single largest form of email abuse today.
There are automated email sending programs that can send millions of messages a day; the bandwidth, storage space, and time consumed by such massive mailing is incredible. One month's worth of mailings from one of the most nefarious bulk email outfits was estimated at over 134 gigabytes, yes that's right, gigabytes. Each message was sent over the email wires, consuming bandwidth. Then, each message was either stored locally or "bounced" back to the sender, taking up storage space and even more bandwidth. Finally, each boxholder was forced to spend time dealing with the message.

These are all legitimate, measurable costs, and they are not borne by the sender of the messages. UBE is, at best, exploitation of email for profit; at worst, theft. There are currently few regulations regarding UBE; the potential for growth is open-ended. All by itself, UBE could render the email system virtually useless for legitimate messages.

Some would argue that there is such a thing as "responsible" UBE; those who honor "remove" requests and use the lists on "Remove Me" or "No Spam" web sites would fit their description of "responsible". However, due to the types of messages contained in most UBE, and the historic lack of responsibility on the part of the sending organizations, UBE and UCE have earned a reputation as tawdry, widely unpopular methods of disseminating information.

UCE: Unsolicited Commercial Email
Email containing commercial information that has been sent to a recipient who did not ask to receive it.

This is widely used, and confused with UBE, (see above). UCE must be commercial in nature but does not imply massive numbers. Several ISPs specify a threshold for unsolicited commercial email:

----- sending one UCE is a violation -----

In a specific case, individuals took offense at having been sent commercial messages regarding their web sites. Their addresses were posted for the purpose of comments and suggestions about the site; the messages received were commercial offerings to buy ad space on the site or sell something to the site maintainer.

MMF: Make Money Fast
Messages that "guarantee immediate, incredible profits!", including such schemes as chain letters.

Originally a problem in "snailmail" and on Usenet, these messages are now expanding into email. Chain letters and most MMF schemes are illegal, regardless of any claims they might make to the contrary. They should be reported to the proper authorities. Also, chain letters and MMFs don't work! No one sends the 5 dollars, and claims of unlimited wealth made by people who then ask you for money should be taken with a large grain of salt. Many chain letters and MMFs are sent by clueless college freshmen - a note to the administrator of their system is often sufficient to cure them. For the more serious offenders, the US Post Office, Inspection Service - Consumer Fraud Division, loves to hear about chain letters!

MLM: Multi-Level Marketing
Messages that "guarantee incredible profits!", right after you send them an "initial investment" and recruit others.

Some of the MMF senders will say, "This isn't one of those illegal get-rich-quick schemes. No, this is multi-level marketing, and perfectly legal." However, many MLM schemes are little more than illegal pyramid schemes with a fancy name to confuse the unwitting. Particularly popular recently are "Work at Home!" schemes. Whether or not the offer is legal is not important to this FAQ; MLM is commercial email, so go ahead and complain.

1f. What is a mailbomb?
Delivery of enough email to a mailbox to overload the mailbox or perhaps even the system that the mailbox is hosted on.

Mailbombs generally take one of two forms. A mailbox might be targeted to receive hundreds or thousands of messages; this makes it difficult or impossible for the victim to use their own mailbox, possibly subjects them to additional charges for storage space, and might cause them to miss messages entirely due to overflow. This is seen as a denial-of-service attack, perhaps also harassment, and is not tolerated by any known service providers. Alternatively, a message will be bulk-emailed, with the intended victim's address forged in the From: and/or Reply-To: lines of the headers. The victim is then deluged with responses, mostly angry.

There is a third, particularly nasty, form of mailbomb. This one forges subscription requests to many mailing lists, all for onerecipient. The result is a huge barrage of email arriving in the victim's email box, all of it unwanted, but "legitimate". Many mailing list administrators are countering this form of abuse by sending a confirmation email to each subscription request, which must be returned in order to be subscribed to

the list.

1g. What is email harassment?

Any message or series of messages sent via email that meet the legal definition of harassment.

---

2. Actions

2a. I've been mailbombed - what should I do?

Contact your ISP immediately. They can help stop the inflow, and also help track down the source of the mailbomb.

2b. I've received U*E in my mailbox - who do I exterminate?

By responding in some kind of abusive fashion, you lower yourself to the level of the person who sent you the offending message. You might also lose Net access through your ISP. There are other ways to fight back; read on.

I've received U*E in my mailbox - what should I do?

You could: ask the sender not to send you any more; complain to the appropriate people; just ignore it and delete it.

Ask to be "removed" from their list: Some U*E contains instructions for how to be "removed" from the sender's mailing list. Usually this amounts to sending a specifically formatted message to a particular address. While this is a relatively trivial task, it is not particularly effective; see the sections "2g. I asked to be 'removed' - guess what? I got another U*E", and, "2h. I asked to be 'removed' - guess what? The message bounced", later in this FAQ, for more on why this method is less than perfect.

Complain to the appropriate people:
If you send a complaint, be polite, or at least civil. Most times the person receiving your complaint is not responsible for the U*E; if you expect their help, a little honey goes a long way. Be sure to include full headers when sending a complaint.

Decipher the headers and complain to postmaster@... . Several sources on header-ography can be found in Appendix I of this FAQ. Some service providers also have abuse addresses; e.g., abuse@... . If you are on AOL, or another service which engages in filtering, forward to the appropriate address on your system so that they can see where new sources of UBE are, and possibly add them to the list.
For AOL, forward them to postmaster and abuse.

If you are so inclined, you can do a bit more detective work and possibly find more victi--- umm, legitimate recipients for your complaint. If the message originated in the US, using whois, or a visit to InterNIC at
http://www.internic.net/cgi-bin/whois
or its European counterpart at
http://www.ripe.net
might turn up a few more addresses. Traceroute or a similar tool (tracert from the DOS prompt in Win95) will show the sender's upstream provider; some people lodge a complaint with them also. There are several web sites available that will do a traceroute and display the results; use your favorite search engine to find them.

Also, there are usually folks on news.admin.net-abuse.email who are willing to help you decipher headers; be sure to include the complete header in your post.

(WSPING32 for Win95 has traceroute and DNS lookups built into it The traceroute in it is much more intuitive for Windows users. It is available at TUCOWS, and many other Winsock sites. For Mac users, the program "Mac TCP Watcher" has DNS lookup and a traceroute
function.)

If you have the tools available, you can also block any further email from the source of the U*E. See "I never want to see another message from UBEs-Our-Biz.com again!" in this FAQ for more information.

Just ignore it and delete it:
If you only ever get one or two U*E messages, this is a logical and reasonable course of action. When the numbers increase, come back to this FAQ and read about other actions.

2d. Where do these people get my email address?

1.. Run programs that collect email addresses out of Usenet posting headers
2.. Cull them from subscriber lists (such as AOL's Member Profile list)
3.. Use web-crawling programs that look for mailto: codes in HTML documents
4.. Rip them out of online "white pages" directories
5.. Buy a list from someone who already has one
6.. Take them from you without your knowledge when you visit their web site. For the latest on web browser security issues, see
http://www.cert.org/
7.. Use finger on a host computer to find online users addresses 8.. Collect member names from online "chat rooms".

4e. How do I keep my address off the lists?

For a junk-free mailbox, don't browse the web, don't put your email address on a web page, don't subscribe to a large ISP, and don't post to Usenet. In other words, don't use the Internet.

Some people have taken to forging their own From: and Reply-to: lines in their posts. They might add an easily-recognized "spam- block" to their address, or they might use those header lines to tell folks where to look for their real address (usually in the sig). Some attempt to boast of their elitist-Unix-nerd-programmer capabilities by burying their email address in a maze of code. Such measures, while effective, are frowned upon by some as "giving in" to the bulk emailers.

If you do a lot of web browsing, be careful about filling out forms; some outfits take such action as carte blanche to stuff your mailbox. There are also those who sell addresses collected in this manner. Don't assume that because you are visiting the site of a "reputable company" that this will not happen to you.

2f. I did all that and I still get U*E!

Your options are few; your address is probably on one of the lists that gets swapped/bought/sold among the bulk email "community". Your only alternative might be a new address. Also, see "I never want to see another message from UBEs-Our-Biz.com again!" for ways to gird your mailbox against the advancing hordes.

There have been several reports of U*E dropping off considerably as soon as someone has stopped posting to Usenet; this may indicate that the U*E outfits are constantly creating new lists, and not reusing old lists.

2g. I asked to be "removed" - guess what? I got another U*E

Not surprisingly, many UBE outfits treat a "remove" request as evidence that the address is "live"; a "remove" request to some bulk emailers will actually guarantee that they will send more to you. For many others, the remove procedure does not work, either by chance or design. At this point perhaps you're starting to get a feel for the type of people with whom you are dealing.

Also, getting removed doesn't keep you from being added the next time they mine for addresses, nor will it get you off other copies of the list that have been sold or traded to others. In summary, there is no evidence of "remove" requests being an effective way to stop UBE.

2h. I asked to be "removed" - guess what? The message bounced

Probably the remove procedure was false. Any remove procedure that tells you to send remove requests to AOL, CompuServe, Prodigy, Hotmail, or Juno is certainly false. The bulk emailers are an unpopular lot; they forge headers, inject messages into open SMTP ports, use temporary accounts, and pull other stunts to avoid the tirade of complaints that follow every mailing.

2i. What about "Remove Me" web sites and other global "Remove" Lists?

They depend on the goodwill of the UBE-sending agencies to work. That is, the senders must use and honor the lists for them to be effective. There is no evidence that they do so. There is nothing to stop them from adding all those addresses to their lists! Also, because UCE and UBE is sent postage-due, such sites are effectivelyattempting to legitimize a form of recipient-paid advertising; you'll have to decide for yourself whether you want to support such an effort by placing your address there.

2j. List of Basic Administrative Contacts

The search for the best person to complain to at any site has led to much speculation and arguments, even among admins at the same site. However, if a message to the original poster doesn't get you anywhere, somebody at one of the following addresses might be able to help. Be aware, though that some of the more experienced and well- financed junksters have their own domains, and simply drop complaints to some of the addresses below into the bit-bucket. Moving upstream may be your only choice. Some specific addresses are listed in Appendix I of this FAQ, under "Abuse Addresses of major service providers".

abuse

A lot of ISP's and network backbones have created "abuse" addresses for complaints about net-abuse. That's usually the best place to start.

postmaster

RFC 822, the document which set most of the current standards for Internet e-mail back in 1982, makes it mandatory for all sites which pass e-mail to have a postmaster address so that problems can be reported. The purpose of postmaster has expanded at many sites to include net-abuse, both e-mail and otherwise.

Administrative or Technical Contacts

If you have access to the whois command, you can type (for example) whois example.com to find out who the administrative and technical contacts are for a domain. This will list their e-mail address, and often their phone and FAX numbers. Whois for InterNIC is available
via the web at:
http://www.internic.net/cgi-bin/whois
its European counterpart is at:
http://www.ripe.net
The bulk emailers are aware of this resource as well, and InterNIC does very little to check the integrity or authenticity of the supplied information. So don't be surprised to find contact addresses such as "nobody@...", and phone numbers that don't work.

Upstream Providers
Determining who's upstream using email headers can often be confusing--many people get it wrong, due to their own inexperience or forgery on the part of the sender. U*E is worthless unless it contains some legitimate contact information, though. If you've been around the block vis-a-vis headers, and you're familiar with the whois and traceroute tools, you can probably find the upstream provider.

abuse.net
Now you can send mail to domain.name@..., and it will (probably) be sent to the appropriate contact for that domain. Be advised that this is a wholly experimental service. Be sure to visit the web site before sending email to this service; it will explain the what the service does, and how to subscribe to it. You can find it at:
http://www.abuse.net

2k. I've contacted everyone involved - heard nothing back!

Not all ISP's respond to every complaint. With some, this is because the bulk emailer is his own ISP. With others, it is due to the volume of complaints received. Many of the larger ISPs and backbone providers will send an automated response. Don't be offended by this; they are probably deluged with complaints. The more they get, the sooner they'll find a permanent solution, so keep sending them. Also, although the responses are automated, they may still contain specific information; UUNet's replies contain a unique ID number, intended for use in any further communications regarding that particular incident.

2l. I've contacted everyone involved - they told me to go away!

Complain to the next step up the chain. If they, too, brush you off,keep complaining anyway. Some of the upstream providers claim no responsibility for the actions of their customers; in lieu of a "short, sharp, shock", the best thing to do is to keep badgering them. Still other ISPs will tell you there is nothing they can do about such activities; that is pure poppycock. If they happen to be your provider, you might consider letting them know what you think of their incompetence/laziness/irresponsibility by finding another ISP. Be sure to tell all your friends.

2m. They told me they canceled the account, but I got another U*E!

Some sites have been created for no other purpose than sending UBE. Some of these will do their best to spread confusion about theimatures by misleading and outright lying to those who complain. This has included "removing" offending accounts, only to give the user another account to start over again. Also, some UBE "operators" use a "hit-and-run" strategy, getting free trial or "throwaway" accounts at other ISP's to actually send the mail.

In addition to that, forging headers is extremely common. At least one UBE'r has been kicked off an account, forged his next barrage with the (no longer valid) address from the ISP that kicked him off, and bounced the mail off of that provider's mail server. In UBE, appearances are often deceiving.

2n. I sent a complaint - they said they had nothing to do with it!

1.. They had nothing to do with it. The headers were misread or forged.
2.. They're a bunch of lying, no-good such-and-so's. If you're pretty certain that's the case, send as much evidence as you have to their postmaster and their upstream provider.

2o. I sent a complaint - they responded with threats!

See 2) above. Sometimes, threats come from newbies, so simply sending evidence to their postmaster is enough to get them booted. Also, depending on the nature of the threat, other legal measures may be available to you.

2p. I never want to see another message from UBEs-Our-Biz.com again!

Some ISPs maintain server-level junk filters. If your ISP does notdo this, ask them to consider it. They may also subscribe to the Realtime Blacklist (RBL), which is a list of sites deemed to be sources of net abuse.

AOL also gives its members another tool, keyword 'Mail Controls', to block email at the individual level. Ask your ISP to provide similar tools. Better still, ask them to provide even -better- tools.

Some email client programs are equipped with filters which will dump, bounce, or auto-reply to email based on user-defined criteria. Note that this does not prevent the U*E from being received and stored on your mail server until you deal with it. Some email programs will download and act on just the headers; others require the entire message to be downloaded before acting on it.

Consider getting a procmail filter set up if your connection method and ISP will allow it. Procmail is a subject in and of itself; some good starting points can be found in The Email Abuse Resource List,
found at http://members.aol.com/emailfaq/resource-list.html