Figuring out fake E-Mail & Posts (Rev 2002-01-01)

From: gandalf@digital.net (Ken Hollis)
Newsgroups: alt.2600,alt.spam,alt.newbie,news.admin.net-abuse.misc,
news.admin.net-abuse.email,news.admin.net-abuse.usenet,alt.answers,news.answers
Followup-To: news.admin.net-abuse.misc,alt.spam,news.admin.net-abuse.usenet
Subject: - alt.spam FAQ (1/1) or "Figuring out fake E-Mail & Posts". Rev 20020101
Message-ID: <gandalf-ya023580000101022135070001@news>
Organization: I eat people who spam for breakfast ... Don't spam me :-) ...
Summary: This posting describes how to find out where a fake post or e-mail originated from.
X-Newsreader: Yet Another NewsWatcher 2.3.5
Date: Wed, 02 Jan 2002 03:35:10 GMT
X-Complaints-To: abuse@home.net
X-Trace: news1.elcjn1.sdca.home.com 1009942510 24.11.12.56 (Tue, 01 Jan 2002 19:35:10 PST)
NNTP-Posting-Date: Tue, 01 Jan 2002 19:35:10 PST

Archive-name: net-abuse-faq/spam-faq
Posting-Frequency: monthly
Last-modified: 20020101
URL: http://ddi.digital.net/~gandalf/spamfaq.html

Greetings and Salutations:

This FAQ will help in deciphering which machine a fake E-Mail or post
came from, and who (generally or specifically) you should contact.

The three sections to this twelve portion FAQ (With apologies to
Douglas Adams :-)) :

Introduction

Please feel free to repost this, e-mail it, put this FAQ on CD's or
any other media you can think of.

The latest & greatest version of the Spam FAQ is found at:
http://ddi.digital.net/~gandalf/spamfaq.html
or
http://home.digital.net/~gandalf/spamfaq.html

PLEASE email follow-ups, additions / changes to gandalf@digital.net

My news source is OK, but I sometimes miss items.

I accept all and any input. I consider myself to be the manager of this FAQ for the good of everyone, not the absolute & controlling Owner Of The FAQ. I do not always write in a completely coherent manner. What makes sense to me may not make sense to others. If the community wants something added or deleted, I will do so. I removed any e-mail and last name references to someone making a suggestion / addition. This is so that someone doesn't get upset at this FAQ and do something stupid. If you don't mind having your e-mail in this FAQ (or where it is required), please tell me and I will add it back in.

First off if you received a spam (Unsolicited Commercial E-Mail) there is no "easy" way to get the spam stopped. Generally if you reply (unsubscribe) all this does is confirm that your e-mail address is "live" and just gets your e-mail address sold to other spammers. Spam has to be delt with one at a time. Sorry, it isn't easy to stop the spam. The "Internet" (the collective non-profit and profit entities of the network) is trying to fix this problem but it is taking time.

Before trying to determine where the post or e-mail originated from, you should realize that (just like the The National Enquirer http://www.nationalenquirer.com/ or a logical argument from Canter and Siegel) the message will have *some* amount of truth, but all or most of the information may be forged. Be careful before accusing someone.

Commands used in this FAQ are UNIX & VMS commands. Sorry if they don't work for you, you might wish to try looking around at your commands to find an equivalent command (or I might be able to help out some). There are programs for the Macintosh and Windows machines that do the same thing the UNIX commands do, see the above URL's for where to locate this software.

And no, I am not going to tell you how to post a fake message or fake e-mail. It only took me about 2 days (a few hours a day) to figure it out. It ain't difficult. RTFM (or more appropriately, Read The @&%^@# RFC).

Every e-mail or post will have a point at which it was injected into the information stream. E-mail will have a real computer from which it was passed along. Likewise a post will have a news server that started passing the post. You need to get cooperation of the postmaster at the sites the message passed thru. Then you can get information from the logs telling you what sites the message actually passed thru, and where the message "looked" like it passed thru (but actually didn't). Of course you do have to have the cooperation of all the postmasters in a string of sites...

Tracing an e-mail message

To trace the e-mail you have to look at the header. Most mail readers do not show the header because it contains information that is for computer to computer routing. The information you usually see from the header is the subject, date and the "From" / "Return" address. About the only thing in an e-mail header that can't be faked is the "Received" portion referencing your computer (the last received).

You will need to take a look at the headers on the message as follows (Thanks to Michael, Piers and others) :
Claris E-Mailer - under Mail select Show Long Headers.
Eudora (before ver. 3) - Select Tools , Options... , then Fonts & Display then Show all headers
Eudora (ver. 3.x, 4.x IBM or Macintosh) - Press the BLAH button on the incoming mail message
For Mac Eudora 4.x, hitting the following will cause Eudora to alter its default setting so that BLAH will be automatically selected for all new email received after this switch is set:
<x-eudora-setting:123=y> When checked, Eudora will show all the headers from messages, not just an abbreviated set.
HotMail - To expose the full message header, click "Options" on the Hotmail Navigation Bar on the left side of the page. On the Options page, click "Preferences." Scroll down to "Message Headers" and select "Full."
For Lotus Notes 4.6.x - From the menu bar, select Actions, then Delivery Information. Copy the information from the bottom box into

your e-mail report at the top of the spam.
For Lotus Notes R5 - From the menu bar, select Actions, then Tools, then Delivery Information. Copy the information from the bottom box into your e-mail report at the top of the spam.
MS Outlook - Double click on the email in your inbox. This will bring the message into a window. Click on View - Options. You can also open a message then choose File....Properties....Details.
MS Outlook Express - Alt-Enter, or Alt-F then R.
MS Outlook Express - More Detailed:
To look for, copy and send headers In Outlook Express
1- Press CTRL F3
2- Press CTRL A
3- Press CTRL C
4- Press Alt F4. (At this point the message is already copied)
5- Open a new message. Right click and paste or select Edit and paste.
Netscape 3 - In the mail viewing window: Options > Show Headers > All - When all the headers are displayed in the NS3 mail window, they are formatted. This is much more readable than the display in a text editor such as Notepad.
Netscape 4.xx - Double click on the email in your inbox. Click on View - Headers - All.
PINE - You have to turn on the header option in setup, then just hit "h" to get headers.
Yahoo - 1.Log into your Yahoo! Mail account.
2.Click the "Options" link on the left-hand navigation bar.
3.Click the "Mail Preferences" link on the right.
4.Locate the Show Headers heading and select "All."
5.Click the "Save" button to put your new settings into effect.
Another way to show you how to display headers, please see (with some good screen shots):
http://www.wurd.com/eng/ABCs/ms_headers.htm - MS Outlook Express and Internet Mail
http://www.wurd.com/eng/ABCs/mac_headers.htm - MS Outlook Express for the Mac
http://www.wurd.com/eng/ABCs/ns_headers.htm - Netscape Messenger or Netscape Mail

Programs that do not comply with any Internet standards (like cc-Mail, Beyond Mail, VAX VMS) throw away the headers. You will not be able to get headers from these e-mail messages.

Aussie tells us that in Pegasus to view the full headers for each message, use CTRL-H. This will show the full headers for the particular message, but will not add them to any reply or forward. You need to cut/paste the message into the reply/forward to send these headers.

Richard tells us with Nettamer, a MS DOS based email and USENET group reader you must save the message as an ASCII file, then the full header will be displayed when you open the saved file with your favorite ASCII editor.

At this point if you are "pushing the envelope" on your ability to figure out how to get that complaint to the correct person, I would suggest joining the Usenet group alt.spam or news.admin.net-abuse.email and post the message with a title like "Please help me decipher this header". Unfortunately there is no "single" place to complain to about spam (or Unsolicited Commercial E-Mail). Complaints have to be directed to the correct ISP (Internet Service Provider) that the spam originated from. See the below section entitled "Reporting spam".

URL's to help you figure out how to look at the headers:
http://www.concentric.net/~Nvam
http://www.rahul.net/falk/mailtrack.html

A little different description of headers:
http://ddi.digital.net/~gandalf/trachead.html - Line by line tracing of a spammers e-mail
http://help.mindspring.com/features/emailheaders/index.htm
http://help.mindspring.com/features/emailheaders/extended.htm
http://www.mcs.net/~jcr/junkemaildeal.html - Another Header Analysis
http://www.stopspam.org/email/headers/headers.html - In depth header analysis

There is spamming software that sends the e-mail directly to your computer. This makes only one received line in the e-mail making your life many times easier. The computer that is not your computer is the spamming computer.

Also, please look through the body of the message for e-mail addresses to reply to. Complain to the postmasters of those sites also (see below for a list of complaint addresses).

Gregory tells us that assuming a reasonably standard and recent sendmail setup, a Received line that looks like :

```
Received: from host1 (host2 [ww.xx.yy.zz]) by host3
        (8.7.5/8.7.3) with SMTP id MAA04298; Thu, 18 Jul 1996 12:18:06
-0600
```

shows four pieces of useful information (reading from back to front, in order of decreasing reliability):

- The host that added the Received line (host3)
- The IP address of the incoming SMTP connection (ww.xx.yy.zz)
- The reverse-DNS lookup of that IP address (host2)
- The name the sender used in the SMTP HELO command when they connected (host1).

Looking at the below we see 6 received lines. Received lines are like links in a chain. The message is passed from one computer to the next with no breaks in the chain. The received lines indicate that it ended up at ddi.digital.net (my computer) from mail.bestnetpc.com. It was received at mail.bestnetpc.com from unknown (HELO paul-s.-aiello) ([205.160.183.123]). The last three lines suggests that it was received at in2.|bm.net from mh.tomsurl|.com and from reb50.rs41|1date.net. Since none of these computers are in the first two received lines then we can ignore these lines and every received entry after this line (this UCE had 4 or 5 more faked Received lines in it that were deleted for this example). We also know that these lines are faked because no domain name has a "|" character in the name. Domain names only have alphabetic or numeric characters in the name.

Do not get confused by the "Received: from unknown" portion. The word "unknown" can be *anything* and should be ignored, this is whatever the spammer put in the SMTP HELO command when they connected to the SMTP server.

```
Received: from mail.bestnetpc.com (IDENT: gmailr@mail.bestnetpc.com
[205.160.183.3]) by ddi.digital.net (8.9.1a/8.9.1) with SMTP id
CAA10768 for <gandalf@digital.net>; Thu, 26 Nov 1998 02:55:11 -0500
(EST)
Received: (qmail 25259 invoked from network); 26 Nov 1998 08:05:49 -
0000
Received: from unknown (HELO paul-s.-aiello) ([205.160.183.123])  by
mail.bestnetpc.com with SMTP; 26 Nov 1998 08:05:49 -0000
Received: (from uudp@lcl|lhost) by in2.|bm.net (8.6.9/8.6.9) id
CFF569794 for <suppressed>; Thursday, November 26, 1998
Received: from tomsurl|.com (mh.tomsurl|.com [100.257.57.69]) by
m4.tomsurl|.com (8.6.12/8.6.12) with ESMTP id PAA21932 Thursday,
November 26, 1998
Received: from reb50.rs41|1date.net (root@reb50.rs41|1date.net
[256.36.1.176]) by tomsurl|.com (8.6.12/8.6.12) with ESMTP id
PBA023891 for <suppressed>;
```

So we complain to whomever owns unknown (HELO paul-s.-aiello) ([205.160.183.123]). Make sure that you do a nslookup (or use http://samspade.org/t/ , put the address in the section "address digger", click on WhoIs IP block and Traceroute and click on "do stuff") on the IP address's. I try to verify 205.160.183.123 is paul-s.-aiello. Indeed paul-s.-aiello does not even exist and 205.160.183.123 does not resolve to a name when I do a NSLookup. Next would be a Traceroute. See further below for more in-depth tracking on resolving an IP.

IP portion = 205.160.183.123

```
Traceroute 205.160.183.123 gives us:
Step  Host                          IP
Find route from: 0.0.0.0 to: 205.160.183.123 (205.160.183.123), Max 30
hops, 40 byte packets
<snip>
```

```
13 acsi-sw-gw.customer.alter.net.   (157.130.128.26 ):   235ms
14 atlant-ga-2.espire.net.          (206.222.97.24  ):   272ms
15 206.222.104.37                   (206.222.104.37 ):   279ms
16 orland-fl-1-a5-0.espire.net.     (206.222.99.7   ):   362ms
17 iag.net.orland-fl-1.espire.net.  (206.222.106.6  ):   195ms
18 d1.s0.gw.dayb.fl.iag.net.        (207.30.70.38   ):   230ms
19 s0.gw.bestnetpc.net.             (207.30.70.254  ):   231ms
20 *     *     *
21 205.160.183.123                  (205.160.183.123):   372ms
```

See the Traceroute section below for how to interpret the "*" (and other codes) that are returned from a Traceroute.

Note - if you see something like the following realize that the only portion you can trust is within the "([" and the "])". The spammer put in the (faked) portion "mail.zebra.net (209.12.13.2)" :
Received: from mail.zebra.net (209.12.13.2) ([209.12.69.42])

Kamiel tells us that you might also want to make sure that the IP is not hosted by an intermediary site. Check it out at:
http://www.arin.net

You should complain to the abuse@ or postmaster@<Last Two or Three words at the end of the name>. I would complain to abuse@iag.net OR abuse@espire.net (but NOT both sites) since after looking below at the list of complaint addresses in this FAQ there are no alternate addresses for iag.net or espire.net. Unless it is a "major provider" (someone in the below complaint list) I usually complain to the upstream provider rather than risk the chance of complaining to the spammer and being ignored. If you go too far up the chain, however, it may take quite some time for the complaint to filter down to the correct person.

Louise tells us that you are entitled to make an 'alleged' accusation but to prevent yourself from being libel, prefix your statement with:- "Without prejudice: I suspect you are the culprit of such and such."

The constitutional and legal boundary of 'Without prejudice' exempts Politician's opinions being spoken publicly and this prefix is often adopted by Solicitors (English) or Lawyers/Attorneys (USA).

I use :
abuse@XXXXX - Without prejudice I submit to you this Unsolicited Commercial E-Mail is from your user XXXX. UCE is unappreciated because it costs my provider (and ultimately myself) money to process just like an unsolicited FAX. Please look into this. Thank you.

BE SURE to verify the IP address. Windows '95 machines place the name of the machine as the "name" and place the real IP address after the name, meaning a spammer can give a legitimate "name" of someone else to get someone innocent in trouble. A spammer at cyberpromo changed their SMTP HELO so that it claimed to be from Compuserve. The Received line looked like the below, but a quick verification of the IP address 208.9.65.20 showed it was indeed from cyberpromo :

Received: from dub-img-4.compuserve.com (cyberpromo.com [208.9.65.20])
by karpes.stu.rpi.edu

The below e-mail was passed to me thru a "mule" (un1.satlink.com [200.9.212.3]). The Spammer hijacked an open SMTP port to reroute e-mail to me:
Received: from un1.satlink.com (un1.satlink.com [200.9.212.3]) by ddi.digital.net (8.9.1a/8.9.1) with ESMTP id GAA06372; Fri, 27 Nov 1998 06:53:20 -0500 (EST)
Received: from usa.net ([209.86.128.234]) by un1.satlink.com (Netscape Messaging Server 3.54) with SMTP id AAT2FEA; Fri, 27 Nov 1998 08:46:07 -0200

A NSLookup on 209.86.128.234 resolves to user38ld07a.dialup.mindspring.com, so after I complain to mindspring.com I also send the postmaster of the open SMTP port the following :
postmaster@XXXXX - Your SMTP mail server XXXXX was used as a mule to pass (and waste your system resources) this e-mail on to me. You can stop your SMTP port from allowing rerouting of e-mail back outside of your domain if you wish to. FYI only. Info on how to block your server, see:
http://maps.vix.com/tsi/

http://mail-abuse.org/rbl/usage.html
http://samspade.org/t/
http://www.abuse.net/relay.html - Test for server vulnerability

Now that Cable Modems are so popular, companies are starting to put their "personal" e-mail servers on cable / DSL modems and are (of course) not configuring them correctly. I received UCE from an open SMTP server:

```
Received: from SDMAIN (DT1-A-hfc-0251-d1132e93.rdc1.sdca.coxatwork.com
[209.19.46.147])        by ddi.digital.net (8.9.3/05.21.76) with SMTP id
SAA04761;       Fri, 30 Mar 2001 18:35:24 -0500 (EST)
Received: from Received: (qmail 554 invoked from network); 25 Mar 2001
23:56:02        (ip207.miami41.fl.pub-ip.psi.net [38.37.111.207])       by
SDMAIN; Fri, 30 Mar 2001 10:19:58 -0800
```

Complain to Cox (abuse@home.com in this case) about their open SMTP server.

There are some systems that "claim" to "cloak" e-mail. It is not true. If you receive one that looks like the following :

```
Received: from relay4.ispam.net (root@[207.124.161.39]) by
ddi.digital.net (8.8.5/8.8.5) with ESMTP id KAA28969 for
<gandalf@digital.net>; Thu, 26 Jun 1997 10:41:46 -0400 (EDT)
Received: from --- CLOAKED! ---
      or
Received: from cerberus.njsmu.com ([204.142.120.2]) by ddi.digital.net
(8.8.5/8.8.5) with ESMTP id HAA06250 for <gandalf@digital.net>; Mon,
25 Jan 1999 07:11:18 -0500 (EST)
From: hostme39@aol.com
Received: from The.sender.of.this.untracable.email.used.MAILGOD.by.IMI
```

It is still broken down as follows :
- The route the e-mail took originated from one of the systems above the line marked "cloaked" or the line "untraceable" (in fact this makes it even easier to trace). There is no magic to it. Complain to that provider. If you get no response from the site that spammed, you should ask your provider to no longer allow the above site [207.124.161.39] to connect to your system.

It has been kindly pointed out to me that there is a "feature" (read "bug") in the UNIX mail spool wherein the person e-mailing you a message can append a "message" (with the headers) to the end of their message. It makes the mail reader think you have 2 messages when the joker that sent the original message only sent one message (with a fake message appended). If the headers look *really* screwy, you might look at the message before the screwy message and consider if it may not be a "joke" message.

There are also IBM mainframes and misconfigured Sun Sendmail machines (SMI-8.6/SMI-SVR4) that do not include the machine that they received the SMTP traffic from. You have to route the message (with headers) back to the postmaster at that system and ask them to tell you what the IP of the machine is that hooked into their system for that message.

An example of a Microsoft Exchange server that the "HELO" transaction is taken as the "From" portion (and is completely false) :

```
Received: from dpi.dpi-conseil.fr (dpi.dpi-conseil.fr [195.115.136.1])
        by ddi.digital.net (8.9.3/8.9.3) with ESMTP id KAA06614 for
<gandalf@digital.net>; Thu, 26 Aug 1999 10:51:31 -0400 (EDT)
Received: from FIREWALL ([192.168.0.254]) by dpi.dpi-conseil.fr with
SMTP (Microsoft Exchange Internet Mail Service Version 5.5.2448.0)
        id QW11TJV1; Thu, 26 Aug 1999 16:44:38 +0200
```

It has also been pointed out that someone on your server can telnet back to the mail port and send you mail. This also makes the forgery virtually untraceable by you, but as always your admin should be able to catch the telnet back to the server. If they telnet to a foreign SMTP server and then use the "name" of a user on that system, it may appear to you that the message came from that user. Be very careful when making assumptions about where the e-mail came from.

Note for AOL users when looking at headers:
If you get double headers at the end of a message (like the below) the spammer has tacked on a extra set of headers to confuse the issue. Ignore everything except the last set of headers. These are the *real* headers.

```
------------------ Headers --------------------------------
Return-Path: <Gloria@me.net>
Received: from  rly-za05.mx.aol.com (rly-za05.mail.aol.com
[172.31.36.101]) byair-za04.mail.aol.com (v51.16) with SMTP; Mon, 16
Nov 1998 19:16:02 1900
Received: from mailb.telia.com (mailb.telia.com [194.22.194.6]) by
rly-za05.mx.aol.com (8.8.8/8.8.5/AOL-4.0.0) with ESMTP id TAA05189;
Mon, 16 Nov 1998 19:15:53 -0500 (EST)
From: Gloria@me.net
Received: from signal.dk ([194.255.7.40]) by mailb.telia.com
(8.8.8/8.8.8) with SMTP id BAA14174; Tue, 17 Nov 1998 01:15:50 +0100
(CET)
Received: from 194.255.7.40 by signal.dk
viaSMTP(950413.SGI.8.6.12/940406.SGI.AUTO) id AAA28586; Tue, 17 Nov
1998 00:53:13 +0100
Message-Id: <199811162353.AAA28586@signal.dk>
Date: Mon, 16 Nov 98 18:27:19 EST
To: Gloria@papa.fujisankei-g.com.jp
Subject: ATTENTION SMOKERS - QUIT SMOKING IN JUST 7 DAYS
Reply-To: Gloria@papa.fujisankei-g.com.jp

------------------ Headers --------------------------------
Return-Path: <lifeplanner@zcities.com>
Received: from  rly-yd04.mx.aol.com (rly-yd04.mail.aol.com
[172.18.150.4]) by air-yd02.mx.aol.com (v56.14) with SMTP; Mon, 11 Jan
1999 23:54:48 -0500
Received: from phone.net ([207.18.137.42])
          by rly-yd04.mx.aol.com (8.8.8/8.8.5/AOL-4.0.0)
          with SMTP id XAA01327;
          Mon, 11 Jan 1999 23:51:03 -0500 (EST)
From: <lifeplanner@zcities.com>
To: <Someone@aol.com>
Date: Tue, 15 Dec 1998 20:54:19 -0600
Message-ID: <136533440188702520@phone.net>
Subject: Life insurance, do you have it?
Mime-Version: 1.0
Content-Type: text/html
Content-Transfer-Encoding: quoted-printable
```

What computer did this e-mail originate from?

You cannot generally tell by a e-mail header which specific computer the e-mail came from. Just about every time you dial into your ISP (Internet Service Provider) you are assigned a different IP address. If someone sends you an e-mail and they log out, the next time they log in their IP address will most likely be different. If the computer has a permanently assigned IP address *and* you have the cooperation of whomever owns that block of IP addresses you *might* be able to get information on who might have sent the e-mail.

About the only way to tell *exactly* which e-mail account the e-mail was sent from is to get the ISP (Internet Service Provoder) to tell you. Usually the ISP will require you to get the local police involved (a warrant of some type) to force the ISP to give you that information. Even given that you know the account the e-mail originated from, a forger can find out that person's account / password and log in as them, they can gain access to that computer while the person who owns that computer is away from the computer or they could install a back door program that allows them to control that person's computer remotely. If this were to happen then the forger could send the e-mail and the nobody would know who *specifically* sent the e-mail.

MAILING LIST messages

Stephanie kindly defines MAILING LIST versus LISTSERVER :

A MAILING LIST is a type of email distribution in which email is sent to a fixed site which holds a list of email recipients and mail is distributed to those recipients automatically (or through a moderator).

A LISTSERVER is a software program designed to manage one or more

mailing lists. One of the more popular packages is named "LISTSERV". Besides Listserv, other popular packages include Listproc which is a Unix Listserv clone (Listservs originated on BITNET), Majordomo and Mailserve. Most importantly -- not all mailing lists run on listservers, there are many mailing lists that are manually managed.

You may hear of mailing lists being referred to as many things, some strange, some which on the surface make sense, like "email discussion groups". But this isn't accurate either, since not all mailing lists are set up for discussion.

Istvan suggests "Majordomo software is remarkably funny about headers. It does not like headers which contain anything odd. All messages the software receives which do not conform to its rigorous standards are simply forwarded to the list moderator. It turns out this feature is effective at stopping between 80 and 90% of spam actually getting to the list."

Kirk tells us that you can set majordomo up so that new subscribers have to reply to a subscribe request, thus verifying the address is legit. Additionally the lists can be configured so that only subscribers can post. And finally you can put filters on content. I've got the list I manage configured to reject multipart email and email which contains html.

Jeff adds that this would be the closed+confirm option in the configuration file so that only subscribers can post. Also, to prevent multipart or HTML this would be the taboo_headers configuration.

Richard mentions "Listserv can be configured to restrict non-members from sending to a list and can restrict spam based on the headers similar to Majordomo. I've used both of these features successfully. You can read more about Listserv capabilities, if you are interested, at:
http://www.lsoft.com/listserv.stm
http://www.lsoft.com/spamorama.html#FILTER (info on its spam filter)
I suspect that Listserv's spam filter may be better than Majordomo's (but I've not managed any Majordomo lists)."

Jeff adds that having ran a majordomo list for almost 4 years, I find majordomo to be every bit as good. I should, however, qualify that; the listowner needs to have his/her clueons in good working order. Simply put, no listowner in their right mind should leave their majordomo lists set to anything other than closed+confirm. Alas, there are listowners who will leave their lists wide open. I've also seen others knock themselves dead creating their own filters just so a listmember can post to the list from a web-based e-mail account while on vacation. I usually tell anyone in such a situation to subscribe to the list from whatever free e-mail account they plan to use. IMO, I cannot justify compromising list security for such reasons. Lists should be closed+confirm...plain and simple.

Example Header appears below:
Received: from dir.bham.ac.uk (dir.bham.ac.uk [147.188.128.25]) by gol1.gol.com (8.7.5/8.6.9) with SMTP id GAA27292 for <XXXX@gol.com>; Sun, 5 May 1996 06:31:15 +0900 (JST)
Received: from bham.ac.uk by dir.bham.ac.uk with SMTP (PP) using DNS id <26706-38@dir.bham.ac.uk>; Sat, 4 May 1996 20:56:49 +0100
Received: from emout09.mail.aol.com (actually emout09.mx.aol.com) by bham.ac.uk with SMTP (PP); Sat, 4 May 1996 21:13:03 +0100
Received: by emout09.mail.aol.com (8.6.12/8.6.12) id PAA29156; Sat, 4 May 1996 15:35:53 -0400
Date: Sat, 4 May 1996 15:35:53 -0400
From: Jeanchev@aol.com
Message-ID: <960504153553_287142426@emout09.mail.aol.com>
Subject: CRaZy Complimentary Offer.....

This is a post from Kevin Lipsitz for his "===>> FREE 1 yr. USA Magazine Subscriptions". The latest information indicates that the state of New York has told him he should stop abusing the Internet for a while ... lets hope it is forever. In relation to the Internet he makes a slimy used car salesman look like a saint.

For more info about "Krazy Kevin" or the Magazine Spam , Tony tells us the page "Stop Spam!" is available in html format at:
http://www.iac.co.jp/~issho/stop-spam.html

But as David reminds us, There are a million Kevin J. Lipsitz's out there. All selling magazines, Amway, vitamins, phone service, etc. All the losers who want to get rich quick, but can't start their own business.
Like :
http://com.primenet.com/spamking/

That having been said, e-mail from a Listserve can usually be broken down the same way as "normal" e-mail headers. There are just more waypoints along the way. As you can see from the above, the e-mail originated from :

emout09.mail.aol.com

Jeff also mentions that news.admin.net.abuse.e-mail is a good newsgroup to monitor about how to keep spam off the listserve. I have seen mailing list issues arise occasionally.

Reporting Spam and tracing a posted message

If someone posts a message with your e-mail in the From: or Reply-To: field, it can (and will if you request) be canceled. Please repost the message to news.admin.net-abuse.misc WITH THE HEADERS (or it will probably be ignored) so that the message cam be canceled (the message-id is the most important) with a suggested subject of the following:

Subject: FORGERY <Subject from the Spam message>

Or you can look at the Cancel FAQ at :
http://www.ews.uiuc.edu/~tskirvin/faqs/cancel.html

Try to make sure that the message has not already been posted to news.admin.net-abuse.misc, news.admin.net-abuse.email or news.admin.net-abuse.usenet and that it is less than 4 or 5 days old. Chris reminds us that yes, there are a lot of annoying, off-topic and stupid postings out there. But that doesn't make it spam. _Really_. All we're concerned with is _volume_. Don't report any potential spams unless you see at least two copies in at least 4 groups. The content is irrelevant. Spam canceling cannot be by content.

For off topic posts, see http://ddi.digital.net/~gandalf/trollfaq.html

The first thing to do is to post the ENTIRE message (PLEASE put the header in or it will probably be ignored) to the newsgroup news.admin.net-abuse.misc. Do not reply or post it back to the original group. A suggested subject is one of the following:

Subject: EMP <Subject from the Spam message>
Subject: ECP <Subject from the Spam message>
Subject: UCE <Subject from the Spam message>
Subject: SEX <Subject from the Spam message>

Please include the original Subject: from the original Spam so that it can easily be spotted. Thank you.

Take a careful look at the header, if there are "curious characters" (characters that look like garbage) in the X-Mailer: line, or any other line in the header, then delete those characters otherwise the message may end up truncated. The offending line consists of the EIGHT characters D0 CF 11 E0 A1 B1 1A E1 (in hex).

If the post is particularly amusing (Spammer threat or a postmaster threat), put C&C in the subject. Seymour tells us it means Coffee and cats. This originated from a post claiming that a particular outrageous article had caused spewing of coffee into the keyboard and jumping while holding a cat, resulting in scratched thighs.

An Excessive Multiple Post (EMP) may exceed the spam threshold and may be canceled. An Excessive Cross Post (ECP) may not be canceled because it hasn't reached the threshold. A UCE is for Unsolicited Commercial Email, SEX is for off-topic sex-ad postings.

Make Money Fast message is immediately cancelable and are usually canceled already by others, so please do not report MMF posts. See MMF section below.

Tracing a fake post is probably easier than a fake e-mail because of some posting peculiarities. You just have to save and look at a few

"normal" posts to try to spot peculiarities. Most people are not energetic to go to the lengths of the below, but you never know.

Dan reminds us that first you should gather the same post from *several* different sites (get your friends to mail the posts to you) and look at the "Path" line. Somewhere it should "branch". If there is a portion that is common to all posts, then the "actual" posting computer is (most likely) in that portion of the path. That should be the starting postmaster to contact. Be sure to do this expeditiously because the log files that help to trace these posts may be deleted daily.

If you *really* want to see some fake posts, look in alt.test or in the alt.binaries.warez.* groups.

A fake post:

Path:
...!news.sprintlink.net!in2.uu.net!news.net99.net!news!s46.phxslip4.indirect.com!vac
From: XXX@indirect.com(Female User)
Subject: Femdom In Search of Naughty Boys
Message-ID: <DHLMvE.24H@goodnet.com>
Sender: XXX@indirect.com(Female User)
Nntp-Posting-Host: s46.phxslip4.indirect.com
Organization: Internet Direct, Inc.
X-Newsreader: Trumpet for Windows[Version 1.0 Rev B final beta #1]
Date: Mon, 6 Nov 1995 01:59:38 GMT
Approved: XXX@indirect.com
Lines: 13

This poor lady (Name deleted by suggestion) was abused by someone for a couple of days in an epic spam. Many messages were gathered. The message ID was different for several messages. But several anomalies showed an inept poster.

The headers were screwed up, and when looking at a selection of messages from several sites, the central site was news.net99.net, where goodnet.com gets / injects news at. This lead to the conclusion that either goodnet.com or news.net99.net should be contacted to see who the original spammer was. I never heard the results of this, but the spamming eventually stopped.

You can try looking at sites & see if they have that message by :
telnet s46.phxslip4.indirect.com 119
Connected to s46.phxslip4.indirect.com.
200 s46.phxslip4.indirect.com InterNetNews server INN 1.4 22-Dec-93 ready
head <DHLMvE.24H@goodnet.com>
430

Message was not found at that site, so it did not go thru that computer, or the article has already expired or been deleted off of that news reader.

If you wish to track a particular phrase, user-id (whatever) take a look at the URL for getting all the posts pertaining to "X" :

http://www.deja.com/
http://www.altavista.com/

WWW IP Lookup URL's
==========
http://samspade.org/t/ - My personal favorite. All the tools on one page.
http://www.geektools.com - Does lookups at all of the servers (Arin, RIPE, APNIC, etc.)
http://www1.dshield.org/ipinfo.php - Look up IP address / complaint address for Denial of Service attacks.
http://andrew.triumf.ca/cgi-bin/spamalyzer.pl - Check and see if the address is in one of the real time abuse databases.
http://www.amnesi.com/hostinfo/ipinfo.jhtml - Reverse lookup
http://cities.lk.net/trlist.html - Traceroute Lists by States and Backbone Maps List
http://www.net.cmu.edu/cgi-bin/netops.cgi - Traceroute and ping
Note : Studio42 lists its blocked users as: "All UU.Net dial-ups, thus most MSN subscribers and a percentage of Earthlink users."
http://www.studio42.com/cgi-spam/nph-traceroute.pl - Traceroute

http://www.studio42.com/cgi-spam/nph-nslookup.pl - NSLookup
http://www.studio42.com/cgi-spam/nph-dig.pl - Dig
Index to Traceroute pages:
http://dir.yahoo.com/Computers_and_Internet/Communications_and_Network
ing/Software/Networking/Utilities/Traceroute/
http://www.traceroute.org/
http://boardwatch.internet.com/traceroute.html - Traceroute Server
Index
SWITCH WHOIS Gateway:
http://www.switch.ch/search/whois_form.html
  Or
http://www.networksolutions.com/cgi-bin/whois/whois
http://www.ripe.net/db/whois.html - European countries WhoIs
http://www.apnic.net/apnic-bin/whois.pl - Asian Pacific WhoIs
whois.nic.or.kr - Korean Whois
http://www.arin.net/whois/arinwhois.html - North / South America WhoIs
http://mjhb.marina-del-rey.ca.us/cgi-bin/ipw.pl - Whois
IP to Lat - Lon (For those times when only a Tactical Nuke will do ;-
)) :
http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2ll/
Yet Another IP to name:
http://cello.cs.uiuc.edu/cgi-bin/slamm/ip2name
What do those domain names mean :
http://www.alldomains.com/alltlds.html
http://www.ics.uci.edu/pub/websoft/wwwstat/country-codes.txt - Country
Codes for the last characters in a domain name
http://x.deja.com/article/660567270 - Badly Formed DNS article

Converting that IP to a name
============================
When all you have is a number the looks like "204.183.126.181", and no
computer name, then you have to figure out what the name of that
computer is. Most likely if you complain to "
postmaster@[204.183.126.181] " it will go directly to the spammer
themselves (if it goes anywhere at all).

Whois or a traceroute will give you the upstream provider, complain to
that organization.

Marty reminds us that there are some "special" IP's that are allocated
as private networks. These fall within the confines of 0.0.0.0 to
255.255.255.255 but should be ignored. If the number is greater than
255 then it is faked. The addresses are :

```
Class  Start Address  End Address
  A     10.0.0.0     10.255.255.255
       127.0.0.0    127.255.255.255 - Loopback addresses
  B   172.16.0.0     172.31.255.255
  C  192.168.0.0    192.168.255.255
  D    224.0.0.0    239.255.255.255 - Multicast
  E    240.0.0.0    255.255.255.255 - Multicast
```

See :
http://www.umnet.umich.edu/groups/UMnet-
Routing/UAssignedPrivateIP.html

First off try using NSLookup (there is software for PC's, I use
http://samspade.org/t/ , put the address in the section "address
digger", click on Whois IP block and Traceroute and click on "do
stuff" or look at the URL's at the bottom of this FAQ). If the
NSLookup does not give you a name then try a Traceroute. Somewhere
you will get a "name" and at that point I would complain to the
postmaster@<that name>. See below for complaint addresses.

See (as of 1997):
http://ipindex.dragonstar.net/a/indexa.html - Who owns which Class A
addresses
http://ipindex.dragonstar.net/b/indexb.html - Who owns which Class B
addresses
http://ipindex.dragonstar.net/c/indexc.html - Who owns which Class C
addresses

What to do with "strange" looking Web links
===

http://1%30%38%35%338%31%32%39%32/ has some %-encoded characters, but
decoding those gives http://1085381292/

1085381292 is just another way of writing the IP address
64.177.154.172

To convert a decimal number to a "dotted quad octet" :
http://3438189385/yt/rotten1/

You can put this "strange" number in at any of the following :
http://samspade.org/t/
http://www.webspawner.com/users/ipconverter
http://www.isit.nl/cgi-bin/isitbv/ip.cgi
You can also download Cyberkit v. 2.5 to do the translation.

http://www.netdemon.net/ - Automatic url decoder built in for Windows 95.
As well as the Windows 95 based URL decoding tool, it has been ported and made available to everyone as a CGI:
http://www.netdemon.net/decode.html
This CGI handles ALL the recent types of spammer tricks, including decimal, octal, hex addresses, username/password tricks, hex encoded characters, and redirectors.

And you get an answer like:
204.238.155.73

You can try the "strange" number at :
http://www.abuse.net/cgi-bin/unpackit

Kirk tells us wsftp and the traceroute that comes with wsftp will take those number and automatically translate them into the IP addresses.

Or under Widows 95 :
 start --> Programs --> Accessories --> Calculator
Choose view --> Scientific
Put in the "strange" number (3438189385) and click on HEX. You get:
CCEE9B49

Then type in each of the two characters in HEX and click DEC after each number:
CC = 204
EE = 238
9B = 155
49 = 73

Viola ... Your IP is 204.238.155.73

For more general funny URLs, like
http://23123443~32:3758493879/www.samspade.org/10.00.0.1/xxxstuff.html
, try http://samspade.org/t/url.cgi?x

If you get a strange URL like:
http://www.nt.dahouc.mx^T^B^T^E^T.com|net.fr^B^E^T^B^T^E^T^T.ooooooooo
ooooooooo.com:80/nt/dahouchy/
Where the ^B = Control "B", ^T = Control "T", etc. you can look at the very end right before the first "/" to figure out what the site is, on this case it is ooooooooooooooooo.com, using port 80. The rest of it is "decoded" by ooooooooooooooooo.com to give the "real" site name.
For MS Windows the program at http://www.netdemon.net will decode these with ease.

If you are looking thru the HTML source and yo get something like:
<!-- CHANGE EMAIL ADDRESS IN ACTION OF FORM --><FORM name="form"
method="post"
action="mailto:mor&#11
6;mail6@yahoo.&
#99;om?subject=&#68
;ebt1" enctype="text/plain"
Then take the "funny" looking part and paste it into the "Obfuscated URLs" section of http://samspade.org/t/ like so:
http://mailto:mor&#116
;mail6@yahoo.&#
99;om?subject=D
ebt&#49
And you get:
http://mailto:mortmail6@yahoo.com?subject=Debt1

So then you send a complaint to yahoo.com asking them to delete their user mortmail6@yahoo.com.

If the site is a IP address like "198.41.0.5", you can do a DNS lookup to backtrack the site. A DNS lookup or a host command (see example below) uses the info in a Domain Name Server database. This is the same info that is used for packet routing. The UNIX command is :

```
nslookup 198.41.0.5
Commands:
nslookup hostname dns_server
  or
dig @dns_server hostname
```

And you get :

```
Name:    whois.arin.net
Addresses:  198.41.0.5, 198.41.0.6
```

If you are having problems with this, Josh suggests you try :

```
$ nslookup
Default Server:  ddi.digital.net
Address:  198.69.104.2

> set type=ptr
> 181.126.183.204.in-addr.arpa
Server:  ddi.digital.net
Address:  198.69.104.2

Non-authoritative answer:
181.126.183.204.in-addr.arpa    name = kjl.com

Authoritative answers can be found from:
126.183.204.IN-ADDR.ARPA        nameserver = escape.com
126.183.204.IN-ADDR.ARPA        nameserver = ns.uu.net
escape.com      Internet address = 198.6.71.10
ns.uu.net       Internet address = 137.39.1.3
```

Looking up IP address ownership

InterNIC is your friend. The InterNIC Registration Services Host contains ONLY Internet Information (Networks, ASN's, Domains, and POC's). Please use the whois server at nic.ddn.mil for MILNET Information. Try :

Bruce tells us that there are three places where you can lookup an IP address, being the current trinity of Regional Internet Registries. These RIRs are:

Jeef says Geektools will work out which one, as well as display the results.

Asia and Pacific Rim: APNIC - Asia Pacific Network Information Centre
whois.apnic.net
http://www.apnic.net/apnic-bin/whois.pl

Americas and parts of Africa: ARIN - American Registry for Internet Numbers
whois.arin.net
http://www.arin.net/cgi-bin/whois.pl

Europe and Surrounding Areas: RIPE NCC - Réseaux IP Européens, Network Coordination Centre
whois.ripe.net
http://www.ripe.net/db/whois.html

Under Unix, you can use:

```
whois -h whois.arin.net 198.41.0.5
      or
whois -h whois.apnic.net 198.41.0.5
      or
whois -h whois.ripe.net 198.41.0.5
```

Each of the above three RIRs may refer to one of the other RIRs. Please do not send complaints to any of the RIRs as they merely provide contact information, and are not related in any way to the possible spammers.

Dan has said that the NIC technical contact is the address to contact if there is a technical problem with the name service records for that

domain. Sending spam notifications to the zone tech contact is an abuse of the NIC whois records. Sending to the admin contact is marginally more justifiable, but should only be used after postmaster and abuse address has been tried. Sending a complaint to all of the intermediate sites in a traceroute should *not* be done, these sites in all likelyhood cannot do anything about the problem (with the exception of possibly the next to last site).

For domains that have invalid contact information you should contact the appropriate RIR (see above)

To see who the upstream provider is, try :

traceroute ip30.abq-dialin.hollyberry.com

You might get :
traceroute to IP30.ABQ-DIALIN.HOLLYBERRY.COM (165.247.201.30), 30 hops max, 38 byte packets
 1 cpe2.Washington.mci.net (192.41.177.181) 190 ms 210 ms 120 ms
 2 borderx1-hssi2-0.Washington.mci.net (204.70.74.101) 100 ms 100 ms 60 ms
 3 core-fddi-0.Washington.mci.net (204.70.2.1) 180 ms 130 ms 70 ms
 4 core1-hssi-4.LosAngeles.mci.net (204.70.1.177) 150 ms 140 ms 150 ms
 5 core-hssi-4.Bloomington.mci.net (204.70.1.142) 180 ms 200 ms 180 ms
 6 border1-fddi-0.Bloomington.mci.net (204.70.2.130) 170 ms 290 ms 240 ms
 7 internet-direct.Bloomington.mci.net (204.70.48.30) 300 ms 210 ms 270 ms
 8 165.247.70.1 (165.247.70.1) 180 ms 240 ms 180 ms
 9 abq-phx-gw1.indirect.com (165.247.202.253) 290 ms 220 ms 230 ms
10 * * *

The first column is the "hop" that traceroute is working on. The next is the "computer" (and IP) of the computer at that hop. The last three numbers are the milliseconds it took to get an answer from that computer.

You can get "codes" instead of the milliseconds. An example of a "code" is the "* * *" for hop 10.

Here is a list of the codes:
? Unknown packet type.
H Host unreachable.
N Network unreachable.
P Protocol unreachable.
Q Source quench.
U Port unreachable.
* The Traceroute Packet timed out (did not return to you).

Chris clarifies that a '*' in actuality could be caused by a timeout OR something listening on the UDP ports traceroute uses to get it's port unreachables back from, to work, OR the router simply does not support ICMP/UDP unreachable ports and traceroute cannot determine it's status so it displays asterisks.

Humm..... Seems that after abq-phx-gw1.indirect.com we get no response, so *that* is who I would complain to... or you can just send a message to postmaster@indirect.com ... If that doesn't work then complain to MCI.net.

JamBreaker sez : Be sure to let the traceroute go until the traceroute stops after 30 hops or so. A reply of "* * *" doesn't mean that you've got the right destination; it just means that either the gateways don't send ICMP "time exceeded" messages or that they send them with a ttl (time-to-live) too small to reach you.

Try 'dig' (or one of its derivatives), it is used to search DNS records :
(For the software :
http://www.rediris.es/ftp/infoiris/red/ip/dns/dig-2.0/)

yourhost> dig -x 38.11.185.89

; <<>> dig 2.0 <<>> -x
;; ->>HEADER<<- opcode: QUERY , status: NOERROR, id: 6
;; flags: qr aa rd ra ; Ques: 1, Ans: 1, Auth: 3, Addit: 3

```
;; QUESTIONS:
;;      89.185.11.38.in-addr.arpa, type = ANY, class = IN

;; ANSWERS:
89.185.11.38.in-addr.arpa.      86400   PTR
ip89.albuquerque.nm.interramp.com.

;; AUTHORITY RECORDS:
11.38.in-addr.arpa.     86400   NS      ns.psi.net.
11.38.in-addr.arpa.     86400   NS      ns2.psi.net.
11.38.in-addr.arpa.     86400   NS      ns5.psi.net.

;; ADDITIONAL RECORDS:
ns.psi.net.     86400   A       192.33.4.10
ns2.psi.net.    86400   A       38.8.50.2
ns5.psi.net.    86400   A       38.8.5.2

;; Sent 1 pkts, answer found in time: 64 msec
;; FROM: (yourhostname) to SERVER: default -- (yourDNSip)
;; WHEN: Thu Nov 16 23:30:42 1995
;; MSG SIZE  sent: 43  rcvd: 216
```

Getting a World Wide Web page busted

Many spammers use throw away accounts, accounts that they know will be deleted as soon as the service gets a complaint. Of course the spammers mentality is "if it is free it is for me to abuse". If the spammer really annoyed you then you might wish to dig and get every account possible deleted. What you need to do is actually go to the WWW page that they advertise, look at the page and usually the page will redirect you to another site (or possibly redirect 2 or 3 times). Send a complaint to these sites (with the original spam). It is important to explain to the site you are complaining to how you got to their site so that they don't ignore you.

In Netscape and Explorer there is an option to "view source". This will pop up a page with all of the http source from the page. This page will have all of the "links" to the next site.

If you look at the http source and it is unreadable (and sez "Haywyre"), take a look at :
http://www.netdemon.net/haywyre/

A list of Usenet complaint addresses

O.K... So you have a common site that you can complain to. Good. If you cannot figure out where the message came from, you can post the FULL HEADERS (this is *very* important for tracing) to alt.spam, news.admin.net-abuse.misc, news.admin.net-abuse.email or news.admin.net-abuse.usenet (see the section entitled Reporting Spam and tracing a posted message). Usually you can get someone to help with the message.

If you complain (or asked to be removed) to the spammer directly, you may just be confirming a "real" live e-mail address, which may lead to even more junk e-mail. I would suggest complaining to the owner of the site only. You can send e-mail to foo.bar.com@abuse.net (where foo.bar.com is the provider you are complaining to) and it will get forwarded to the "best" e-mail address.. See http://www.abuse.net/

There is a list of admins to contact (besides the list contained here):
http://www-fofa.concordia.ca/spam/complaints.shtml

Greg reminds us that if you are complaining to a postmaster about a week-old post, don't bother. It's not on their server, they can't verify it. Make sure you use terms correctly. A recent trend is to call any off-topic post "spam". It's not. I deal with spammers and off-topic or advertising posters differently. Other providers do also. Also, try to keep the clutter in your complaints down. I don't need a copy of the referenced RFC or statute. It doesn't help either of us if I can't find your complaint in between all the mumbo jumbo.

Send complaint with FULL HEADERS in e-mail to any or all of the below :
abuse@spammer.site.net

postmaster@spammer.site.net
master@spammer.site.net (This seems to be the normal addess for many Asian companies)

The following providers have now created an "abuse" address, so I have listed them to shorten the FAQ. Just send an address to abuse@<the provider listed> for a complaint, i.e abuse@bikerider.com :
2die4.com, ABAC.COM - http://www.abac.com/use.html , Above.Net - http://www.above.net/images/aug.pdf , academics.net - http://www.abuse.theplanet.net , Access1.net, accountant.com, adexec.com, africamail.com, AGIS.NET, Airnet.net, ALABANZA.COM, Alladvantage.com, allergist.com, Alltel.net, Aloha.Net, Altavistausa.com, alumnidirector.com, Ameritech.net - http://www.snet.net/support/legal - http://dsl.snet.net/support/legal/ , ANV.NET - http://www.accessnv.com , APEXMAIL.COM, Appliedtheory.net, archaeologist.com, arcticmail.com, Arizonaone.com, artlover.com, asia.com, ASR.net, Atlantic.Net - http://www.atlantic.net/company_info/acceptable.htm , australiamail.com, Autonet.net, AXS.net, Bayoucom.net, Bellatlantic.net, Bellglobal.com, Bellsouth, berlin.com, Best.com, Bigger.net, Bigpond.com, bikerider.com, Boo.net, Bright.net, BT.net, Buzzlink.com, Cableinet.net, Cais.net - http://www.cais.com/comp_aup.htm , Catalog.Com, catlover.com, Centurytel.net - http://www.centurytel.net/terms.html , CERF.net - http://www.ipservices.att.com/policy.html , Cetlink.net - http://www.cetlink.net/cetlink/terms.html , cheerful.com, chemist.com, CJB.net, Clara.net - http://www.clara.net/aup.html , clara.net - http://www.clara.net/aup.html , Clear.net.nz, clerk.com, cliffhanger.com, Clover.Net, CNX.NET, coam.net, columnist.com, Combase.COM, comic.com, Compuweb.com, Connect.ab.ca, Connect.com.au - http://info.connect.com.au/docs/legalese/acceptuse.html , Connectnet.com - http://support.cp.net/AUP/ , consultant.com, counsellor.com, CriticalPath.net, cutey.com, CWI.NET - http://www.cwix.net/business_solutions/internet/aup.html , Cyberlynk.net - http://www.cyberlynk.net/policies.html , Cyberthrill.com - http://www.cyberthrill.com/antispam.html , deliveryman.com, Demon.net - http://www.demon.net/connect/aup/ , Demos.net, Dencity.com - http://www.dencity.com/terms/ , Dialsprint.net, Digiweb.com, diplomats.com, dN.NET - http://www.dn.net/aup , doctor.com, doglover.com, Dol.ru, dr.com, dublin.com, EasyStreet.com, Eclipse.net, efortress.com, engineer.com, ENI.net - http://www.eni.net/Our_Network/aup.html , Erols.com, Espire.net - abuse@espire.net - http://www2.espire.net/aup498.cfm , europe.com, evcom.net - http://www.evcom.net/services/access/acceptab.htm , execs.com, Execulink.com, Exodus.net - http://www.exodus.net/corp/about/antispam.html / http://www.exodus.net/about_us/policies.html#online , Fastpoint.net, financier.com, Flashmail.com, FLIPS.NET - http://www.flips.net/terms.html / http://www.flips.net/spamnote.htm , Forfree.at - http://forfree.at/registration/ , Fortunecity.com, Freecybercity.com, Freenet.carleton.ca, freeserve.net - http://www.abuse.theplanet.net , Freeservers.com - http://WWW.FREESERVERS.COM/policies/abuse.html , Freestation.com, Freeuk.com - http://www.freeuk.com/support/terms.html , Freeyellow.com - http://home.freeyellow.com/tos/ , Fuse Internet Access - http://www.fuse.net/service/account/ca.html , gardener.com, Gate.net, Geocities.com - http://docs.yahoo.com/info/terms/geoterms.html , geologist.com, Globalcenter.net - http://www.globalcenter.net/aup/ , Globix.net, GMX.net, Golden.net - http://welcome.golden.net/aup.shtml - $200 cleanup fee !!!, goodnet.com, Gotoworld.com, graphic-designer.com, greatxscape.com - http://www.abuse.theplanet.net , Gridnet.com, GSTIS.NET, GXN.NET, hairdresser.net, HiSpeed.com - http://hispeed.com/about/policies.shtml , HK.Super.NET - http://www.hk.super.net/email-aup , HKnet.com - http://www.hknet.com/iPage/policy.html , Home.net / Home.com - http://www.home.net/aup , Homepage.com / Homepagecorp.com, Homestead.com, hot-shot.com, HotPOP.com, HSACorp.net, IBM.net - http://help.ibm.net/service/abuse.html , IDT.Net - http://www.idt.net/usage , IMPSAT.NET.AR, IMSIS.COM, india.com, Infi.net - http://www.infi.net/policy.html , InfoAve.Net, inorbit.com, insurer.com, Interaccess.com, Intergate.bc.ca - http://www.intergate.ca/personal/icsa.htm , Interland.net, Intermedia.com - http://www.intermedia.com/aup , internetprimus.net - http://www.abuse.theplanet.net , interramp.com, INVISIO.COM, Island.net, istar.ca, japan.com, journalist.com, junglelink.net - AUP http://www.abuse.theplanet.net , lawyer.com, legislator.com, Lietome.com,

LIGHTNING.NET - http://www.lightning.net/support/AUP.html , LN.NET, lobbyist.com, london.com, loveable.com, mad.scientist.com, madrid.com, mail.com, Maximumhost.com, Mediacity.com, MediaOne.com, Micron.net - http://www.micron.net/subtlbx/acc_use.html#policy , MicroServe.net - http://www.microserve.net/aup / http://www.naispa.org/aup , milehigh.net, minister.com, ML.org, Monisys.ca, Monmouth.com, moscowmail.com, msn.com - http://www.msn.com/aup.htm , munich.com, musician.org, myezmail.com, myfreeoffice.com, myself.com, NameSecure.com, nashville.com, NaviNet.net - http://www.navinet.net/aup.html , neta.com - http://www.neta.com / http://www.getnet.com , Netcom.ca, Netfirms.com, Netforward.com, Netins.net, Netins.net, NETSCAPE.NET, netzero.net, nextra.no, nextra.sk, nextra.de, nextra.at, nextra.cz, nextra.ch, nextra.it, Nid.ru, NIS.net, Nodewarrior.net, nycmail.com, oleane.net, oneandonlynetwork.com, onebox.com - http://www.onebox.com/service/privacy.html , optician.com, outblaze.net - http://anti-spam.outblaze.com/ , OZemail.com.au, Pacbell.net - http://public.pacbell.net/dialup/usepolicy , Pacwest.com , Pagepark.com , Pair.com - http://www.pair.com/abuse/ , paris.com, Peclink.net - http://www.peclink.net/ , pediatrician.com, planet.net.uk - http://www.abuse.theplanet.net , playful.com, poetic.com, pol.co.uk - http://www.abuse.theplanet.net , popstar.com, post.com, Power-tech.net, Powernet.net, POWERSITE.NET, presidency.com, priest.com, prodigy.net, programmer.net, PSI Net - http://www.support.psinet.com/PSIabusetik/ - http://www.psi.net/legalinfo/netabusepolicy.html , publicist.com, pwrnet.com, Quixtar.com - http://www.quixtar.com , Rain.net, realtyagent.com, registerednurses.com, Relcom.ru - http://www.relcom.ru/English/Services/Reglament/ , repairman.com, representative.com, rescueteam.com, Rocketmail.com - http://www.rocketmail.com/py/RMailTermsText.py , rome.com, sageconnect.co.uk - http://www.abuse.theplanet.net , Sagenetworks.com, saintly.com, samerica.com, sanfranmail.com, Savvis.net, scientist.com, Seanet.com - http://www.seanet.com/help/abuse.FAQ.html , seductive.com, Seed.net.tw, SendMoreInfo.com - http://www.sendmoreinfo.com/members/spam.cfm , Sensewave.com, singapore.com, Singnet.com.sg, Slip.net, Snap.com, sociologist.com, Softaware.com - http://www.softaware.com/support/policies.html , soon.com, Splitinfinity.net, Splitrock.net, Sprint.ca, Sprint.net, Sprintlink.net - http://www.sprintbiz.com/ip/policy.html , Sprintmail.com, Stargate.net - http://www.stargate.net/stargate/policies-terms.html - http://www.noc.stargate.net/abuse/ , State.net - http://www.state.net/MNonline/Admin/aup.html , SWBell.net - http://public.swbell.net/faq/spam.html , swinternet.net - http://www.abuse.theplanet.net , Sympatico.ca, teacher.com, techie.com, Teleport.com - http://www.teleport.com/info/tos.phtml , Telstra Big Pond Direct - http://www.direct.bigpond.com/ , Terra.es, TerraNova.net - http://www.terranova.net/policy.html , Thedoghousemail.com, Theplanet.net - http://www.abuse.theplanet.net, Theplanet.net.uk - http://www.abuse.theplanet.net , TIAC.net, Tin.it, TIR.com - http://www.tir.com/about/terms.htm#spamming , Together.net, tokyo.com, Total.net - http://central.total.net/centrale/totalnet/usepolicy.shtml (French) - http://central.total.net/central/totalnet/usepolicy.shtml (English), tpnet.co.uk - http://www.abuse.theplanet.net , Tripod.com, UAlberta.ca, ULINK.NET, umpire.com, Unbounded.net, underwriters.com, usa.com, USA.Net - http://netaddress.usa.net/tpl/Info/Main , USwest.net, USWest.net - http://www.uswest.com/siteincludes/legal/terms.html , uunet.ca - http://www.uunet.ca/aup.html , Valueweb.net, VCnet.com, Verio.net, Videotron.net, Virtualave.net, VPWEBHOSTING.NET, WCom.Net, Webbernet.net, Webjump.com, Webtv.net - http://webtv.net/tos.html , whoever.com, Wild.net, winning.com, Winstar.com - http://www.winstar.com/solutions/copyright/index.asp , witty.com, Worldwideinet.com, writeme.com, wwwatt.net - http://www.abuse.theplanet.net , xoom.com, Yahoo.com - http://edit.my.yahoo.com/config/form?.form=yahoomail_agree , yours.com, Zebra.net, Ziplink.net - http://www.ziplink.net/accept.html , Zipmail.com, Zippp.com

For the following providers the correct e-mail address is:
1-800-242-0363 # (Some Extension) - abuse@digitcom.net - Digitcom Nationwide Services
1-800-600-0343 # (Some Extension) - abuse@digitcom.net - Digitcom sells flat rate $19.95 per month services, 100 messages per day. Spammers love this as it is no muss no fuss flat rate.
1-800-607-6006 # (Some extension) - webmaster@linkems.com - Associated

with www.linkems.com
1-800-811-2141 Code # (some code number) - anti_spam@topsecrets100.com
9netave.com - security@9netave.com - AUP
www.9netave.com/forms/au_policy.shtml
ABSnet - support@abs.net or abs-admin@abs.net
Accesspro.net - support@mail.accesspro.net -
http://accesspro.net/techsuppn.htm
ACN US Tech - techsupport@acninc.net
Adobe software piracy - piracy@adobe.com
AiNET - network-abuse@ai.net - http://www.ai.net/aup.html
Allinfosys.com - abuse@savvis.net - Allinfosys advertises an open
SMTP port at smtp1.allinfosys.com [209.44.59.8]
Alter.net - abuse-mail@uu.net
Angelfire.com or angelfire.com - antispam@staff.angelfire.com -
http://pages.whowhere.com/internet/nospammers
AOL - E-Mail abuse tosemail1@aol.com - UseNet (News) abuse
tosusenet@aol.com - Internet security issues, member harassment or
threats TOSGeneral@aol.com - AOL Web pages which do not comply with
AOL's Terms of Service TosWeb@aol.com - IRC abuse tosirc@aol.com -
http://www.aol.com/info/bulkemail.html - AOL UCE policy
APNIC.net - IP Lookup - whois -h whois.apnic.net <IP address> - APNIC
Does not provide network services. APNIC is the Internet registry for
the Asia and Pacific Rim regions -- we primarily delegate blocks of
addresses to service providers. We do not run a network (other than
our internal network) nor do we have customers or non-staff accounts.
ArgosWeb.net - http://www.ArgosWeb.net/ - Postmaster@ArgosWeb.net
AT&T - dial-access.att.net - abuse@att.net
AT&T WorldNet Services - abuse@worldnet.att.net
ATTmail.com - elsaphelp@attmail.com
AudioPhile.com - abuse@netforward.com
avsofchoice.com - abuse@cyberage.com -
http://www.cyberage.com/email.html
B-INTOUCH - abuse@befree.com / gfindon@befree.com
BBN.com / BBNplanet.com - abuse@bbnplanet.com
BCtel.ca / BCtel.net - abuse.tac@telus.com - http://www.bctel.net/aup
befree.com - abuse@befree.com / gfindon@befree.com
bfast.com - abuse@befree.com / gfindon@befree.com
bfit.com - abuse@befree.com / gfindon@befree.com
BFP.net - postmaster@bfp.net ??? (They deleted abuse@bfp.net). No
website, no AUP. Obviously rogue.
bigfoot.com - abuse@bigfoot.com - To check and see if a user is
active, go to http://www.bigfoot.com/RUN?FN=sendpassword_frameset ,
put in the user and click on "Get It". If that user is still active
then Bigfoot will reply with password sent, otherwise you will get an
error.
Biglobe.ne.jp - info@biglobe.or.jp / support@bcs.biglobe.ne.jp /
support@biglobe.or.jp
Bigstep.net / Bigstep.com - support@bigstep.net
BioGate.com - abuse@netforward.com
Biosys.net - abuse@netforward.com
bitmail.com - abuse@freetradeweb.com
BitSmart.com - abuse@netforward.com
Biz-E-Bot.com - tosviolation@biz-e-bot.com
Biznizlist.com - www.biznizlist.com - abuse@psi.com - Spam friendly
see : http://www.biznizlist.com/FAQ/faq.html
bounce.to - abuse@come.to - http://come.to/abuse.html
browse.to - abuse@come.to - http://come.to/abuse.html
Businessman.org - support@sitesinternet.com / abuse@sitesinternet.com
(abuse mailbox was full ...)
Campus.MCI.Net - postmaster@campus.mci.net
cci-29palms.com - postmaster@cci-29palms.com / collins@cci-29palms.com
Cen2k.com - spam@cyberentertainment.net
Cetin.net.cn - database@cetin.net.cn
change.to - abuse@come.to - http://come.to/abuse.html
China.com - abuse@china.com - Web report of spamming -
http://english.china.com/webpages/antispam.html -
http://www.hkispa.org.hk/antispam/
Chinanet.cn.net - anti-spam@ns.chinanet.cn.net
CLANNET.COM - thilton@twinstar.com / dshart@twinstar.com -
rprice@sofwerks.com - http://www.CLANNET.COM/support.htm
CN.Net - anti-spam@ns.chinanet.cn.net
CNC.net - abuse@xo.com - http://home.concentric.net/support/tos.html -
http://home.concentric.net/support/faq/general/aup.html
Codetel.net.do - SysAdmin@auth2.codetel.net.do
Coloradosoft.com - Wrote a mail merge program that used to allow
spamming, has since fixed the code but old versions are still out
there ... Please do not complain to them ...
Com.BR - Policy - demi@agestado.com.br security violations write the

list cert-br@listas.ansp.br
Come.to - abuse@come.to - http://come.to/abuse.html - Complaint form
at http://v3.come.to/webmaster.html
Commtouch.com - spam@commtouch.com
ComPorts.com - abuse@netforward.com
Compuserve - abuse-mail@compuserve.net : Email "spam"/massmail
complaints - abuse-news@compuserve.net : News "spam" complaints
Concentric.net - abuse@xo.com -
http://home.concentric.net/support/tos.html -
http://home.concentric.net/support/faq/general/aup.html
CoreComm / corecomm.net - abuse@voyager.net -
http://home.execpc.com/web/customersupport/systempolicies/index.html
Coxatwork.com - abuse@home.com
CRL.com - abuse@crl.com / support@crl.com - Send to One and ONLY one
address or it will bounce back to you unsent, and a bug in the
software they have will *not* let you send that complaint to only one
recipient after that first e-mail.
Cryogen.com - abuse@netforward.com
CW.net - Spamcomplaints@cwixmail.com - Cable and Wireless - Security -
http://security.cw.net/
CWIE.net - Abuse@cavecreek.com - http://www.cavecreek.net/aup.htm
CWIX.NET - Spamcomplaints@cwixmail.com -
http://www.cwusa.com/internet_aup.htm
CWUSA.com - Spamcomplaints@cwusa.com -
http://www.cwusa.com/internet_aup.htm
CWW.com - abuse@china.com - Web report of spamming -
http://english.china.com/webpages/antispam.html -
http://www.hkispa.org.hk/antispam/
CyberJunkie.com - abuse@netforward.com
CyberTours.COM - postmaster@cybertours.com
da.ru - master@da.ru
DeathsDoor.com - abuse@netforward.com
dedicatedns.com - abuse@ALABANZA.COM
DejaNews - abuse@deja.com - http://www.deja.com/help/faq.shtml#abuse -
http://www.deja.com/info/postrules.shtml
demon.nl / nl.demon.net - abuse@demon.nl - Dutch
http://www.demon.nl/extra/algemenevoorwaarden.html
Dhs.org - abuse-<full hostname>@dhs.org Example: abuse-
spam123.dhs.org@dhs.org
Dial-access.att.net - abuse@att.net
Digex.net - abuse@intermedia.com (along with your real name) see
http://www.intermedia.com/aup
DigiCron.com - abuse@netforward.com
Direct.CA - complaints@direct.ca
DittosRush.com - abuse@netforward.com
DRAGG.NET - postmaster@DRAGG.NET
drive.to - abuse@come.to - http://come.to/abuse.html
dynamicweb.net - abuse@webhosting.com
EarthCorp.com - abuse@netforward.com
Earthlink.net - abuse@mindspring.com -
http://www.mindspring.com/aboutms/policy.html
ELI.net - abuse@eli.net (reports to postmaster@eli.net are NOT
forwarded to abuse@eli.net , they are deleted).
http://www.eli.net/techsupport/aup.shtml
Email.com - abuse@snap.com
Empirenet.com - abuse@globalcenter.net -
http://www.globalcenter.net/launchpad/util/antispam.html
eranet.net - postmaster@eracom.com.tw
excite.com - abuse.support@excitecorp.com -
http://www.excite.com/terms.html
excitecorp.com - abuse.support@excitecorp.com -
http://www.excite.com/terms.html
Execpc.com - abuse@voyager.net -
http://home.execpc.com/web/customersupport/systempolicies/index.html
Fastresponse.net - NetworkTeam@fastresponse.net
Flashnet - postmaster@flash.net -
http://www.flash.net/~support/esupport/postmast.html
fly.to - abuse@come.to - http://come.to/abuse.html
FLYINGCROC.com - postmaster@FLYINGCROC.com
Freei.net - support@freei.net
Freepage4u.net - No contact, no AUP. Appears to be rogue. Contact
abuse-mail@uu.net
Freewebco.net- abuse@techie.com
Frontiernet.net - abuse@globalcenter.net -
http://www.globalcenter.net/aup/
Funcity.com.tw - postmaster@funcity.com.tw
Funtv.com - webmaster@funtv.com
GalaxyCorp.com - abuse@netforward.com

Genuity.net - abuse@bbnplanet.com
gergs_bane.org (does not exist, it is faked) - See UUNET - help@uunet.uu.net
get.to - abuse@come.to - http://come.to/abuse.html
Getnet.com - Abuse@neta.com - http://www.neta.com / http://www.getnet.com
GlobeComm, Inc. - GlobeComm is the parent company of iName - abuse@corp.mail.com
GNN.Com - For help regarding a problem with a GNN member - GNNadvisor@gnn.com.
go.to - abuse@come.to - http://come.to/abuse.html
Go2net.com - support@go2net.com
Goingplatinum.com.- spam@goingplatinum.com
Good.Net - abuse@goodnet.com
Grid.net - Abuse@Gridnet.com
GTE.net - abuse@bbnplanet.com
GTEI.net - abuse@bbnplanet.com
Gulf.net - postmaster@gulf.net - Spam cleanup charges !!!
Hinet.net - spam@ms1.hinet.net
HKU.HK - Hong Kong University - kty@CC.HKU.HK
HLC.NET - abuse@eni.net - http://www.eni.net/Our_Network/aup.html
hm-software.com - postmaster@hm-software.com
Holonet.net - abuse@holonet.net - Complaint must contain e-mail address, real name, address, and day time telephone number
homeschools.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
HongKong.com - abuse@china.com - Web report of spamming - http://english.china.com/webpages/antispam.html - http://www.hkispa.org.hk/antispam/
HOSTCENTRIC.NET - abuse@HOSTCENTRIC.com
HOSTING4DOMAIN.COM - No e-mail contact, no AUP, but their provider is mediaone.net
Hotbot.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
Hotmail.com - abuse@hotmail.com - http://wy1lg.hotmail.com/cgi-bin/dasp/tos.asp - Also look for "X-Originating-IP: [xxx.xxx.xxx.xxx]" in the header to see where the e-mail originated from.
i.am - abuse@easy.to
icg.net - abuse@icgcomm.com
ICQ - See http://www.icq.com/features/security/spam.html
Idirect.com - spammer@idirect.com
iname.com - abuse@corp.mail.com
information4u.com - abuse@corp.mail.com
Inreach.com - postmaster@inreach.com - http://members.inreach.com/acceptable.html
Intercom.net - abuse@ABAC.COM abuse@aplus.net abuse@intercom.net - http://www.abac.com/use.html
Internex.net - abuse@concentric.net - http://home.concentric.net/support/tos.html
interserve.com.hk - Mr. K H Lee - khlee@interserve.com.hk.
is.net.tw - spam@infoserve.com.tw
Islandonline.net - Nicole@islandonline.net
ISPchannel.com - abuse@mediacity.com
inforamp.net - abuse@iSTAR.ca
hotstar.net - abuse@iSTAR.ca
magi.com - abuse@iSTAR.ca
nstn.ca - abuse@iSTAR.ca
jps.net - abuse@mindspring.com - http://www.mindspring.com/aboutms/policy.html
jump.to - abuse@come.to - http://come.to/abuse.html
Juno.com - postmaster@juno.com
k12mail.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
LAKER.NET admin@laker.net or VOICE 1-954-359-3670 FAX 1-954-359-2741
LD.net - webmaster@ld.net / webmaster@cognigen.com for spamming incidents - http://LD.NET/bizop/bizop.html#nospam - http://ld.net/6.9/LD1999 - Spammer Canceled
Level3.com - Fastest response go to http://incident-report.level3.com/ - Slow response send e-mail to spamtool@Level3.com
LI.net - Owned by longisland.verio.net - abuse@longisland.verio.net or questions@longisland.verio.net
Listbot.com - lbabuse@linkexchange.com
listen.to - abuse@come.to - http://come.to/abuse.html
Logicalhosting.com - abuse@zingusa.com
looksmart.com - spam@commtouch.com
Loop.Com or Loop.net - greg@loop.com
Lycos.com - spam@lycos.com - Also you can report abuse at

http://help.lycos.com
Lycosmail.com - spam@lycos.com
Mail.com - spam@lycos.com
Mailcity.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
Mailexcite.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
MailMe.net - support@sitesinternet.com / abuse@sitesinternet.com (abuse mailbox was full ...)
MALIBU - postmaster@pbi.net
marchmail.com - abuse@outblaze.com - http://anti-spam.outblaze.com/
Maverick.NET - postmaster@MAVERICK.NET
MCI Net - Spamcomplaints@cwixmail.com - Security http://security.cw.net/
mckinley.com - abuse.support@excitecorp.com - http://www.excite.com/terms.html
MCSNet - support@mcs.net
Media3.com - http://www.media3.com/serviceagree.htm - abuse@MEDIA3.NET / admin@MEDIA3.NET . According to MAPS / RBL Media3 refused to require its Web-hosting customers to stop using unsolicited commercial e-mail messages as an advertising tool. Complain to abuse-mail@uu.net ... See http://mail-abuse.org/pressreleases/2001-01-02.html
Members.xoom.com - abuse@xoom.com
Mersinet.co.uk - postmaster@mersinet.co.uk
MicroSoft software piracy - piracy@microsoft.com
Mindspring.com - abuse@earthlink.net
money.com or money.now - postmaster@cam.org
mrearl.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
msl.net - support@spiff.net - mac@msl.net - http://www.msl.net/~mac/usepol.shtml
MWIS.net - root@mwis.net
myworldmail.com - spam@lycos.com (place the offending URL or Email address in the subject)
n2<anything>.com - (Example : n2mail.com, n2adventure.com, n2acting.com) spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
naispa.org - abuse@microserve.net - http://www.microserve.net/aup/ http://www.naispa.org/aup
NAMESERVERS.COM - postmaster@NAMESERVERS.COM
Nap.net - abuse@bbnplanet.com
Netaxs.com - support@netaxs.com / noc@netaxs.com
Netcom.com or @ix.netcom.com - abuse@mindspring.net - http://www.mindspring.com/aboutms/policy.html
Netease.com - Apparently abuse@netease.com is not read (quota exceeded) use postmaster@netease.com - http://corp.163.com/eng/contactus/contactus.html
nextel.no - abuse@nextra.no - http://www.online.no/kundeservice/iguides/nettvett.html (Norwegian only)
NFmail.com - postmaster@nfmail.com "Any use or exploiting of the Project Netfraternity (registered) for profit or commercial aims, by any person or organization, will be pursued by law."
Nic.BR - AntiSPAM Brasil - spambr@abuse.net
NKN.NET - postmaster@veriotexas.net
NL.net / NL.uu.net - postmaster@nl.net or support@nl.uu.net
one-and-only.com - abuse@oneandonlynetwork.com
OneMain - - abuse@mindspring.net - http://www.mindspring.com/aboutms/policy.html
online.no - abuse@nextra.no
OnRamp - postmaster@veriotexas.net
Optilinkcomm.net - postmaster@optilinkcomm.net
Orbita.Starmedia.com - postmaster@starmedia.com
PBI.net - abuse@pacbell.net - http://public.pacbell.net/dialup/usepolicy.html
Pipeline.com - postmaster@pipeline.com
PIPEX- postmaster@dial.pipex.com , International - int-sup@pipex.net , Unipalm PIPEX - postmaster@unipalm.pipex.com
POBoxes.com - abuse@Netforward.com - http://www.netforward.com/rules.shtml
Pompano.net - Abuse@MediaOne.com
popsite.net - postmaster@starnetinc.com (spam) / abuse@starnetinc.com (internet abuse) - Killed users - http://www.popsite.net/kill.html
portal.com - support@portal.com
Primenet.com - spam@globalcenter.net
PRServ.net - AT&T Global Network Services / IBM Global Services -

abuse@prserv.net - http://www.attbusiness.net/
Psynet.net - abuse@netforward.com
QWest.net - abuse@qwest.net
RadioLink.net - abuse@netforward.com
redirect.to - abuse@come.to - http://come.to/abuse.html
REFLEXNET.NET / REFLEXNET.COM - abuse@reflexcomm.com
registeredsite.com - abuse@interland.net -
http://techsupport.interland.net/policies.asp
reporting.net - abuse@befree.com / gfindon@befree.com
Rogers.home.com - abuse@rogers.home.net
Rostelecom.net - postmaster@rostelecom.net
scroll.to - abuse@come.to - http://come.to/abuse.html
SGI.net - abuse@stargate.net -
http://www.stargate.net/stargate/policies-terms.html -
http://www.noc.stargate.net/abuse/
Shore.net - support@shore.net
Siam.to - webmaster@siam.to / faq@siam.to
Sina.com - info@staff.sina.com
Sitesinternet.com - support@sitesinternet.com /
abuse@sitesinternet.com (abuse mailbox was full ...)
Smartworld.net - abuse@smartworld.net - "We will promptly terminate
accounts of UCE originators and occasionally sue them. So please
forward us any spam you get from our dns."
snap.to - abuse@come.to - http://come.to/abuse.html
Southwindent.com - dave@vcity.net
Starmedia.com - postmaster@starmedia.com
Starnetusa.net - postmaster@starnetusa.net -
http://www.starnetinc.com/support/tos.html
start.at - abuse@come.to - http://come.to/abuse.html
State.tx.us - abuse@capnet.state.tx.us
SUMMITPOINT.COM - abuse@state.net - (Merged with State.net) -
http://www.state.net/MNonline/Admin/aup.html
surf.to - abuse@come.to - http://come.to/abuse.html
switch.to - abuse@come.to - http://come.to/abuse.html
Taiwan.com - abuse@china.com - Web report of spamming -
http://english.china.com/webpages/antispam.html -
http://www.hkispa.org.hk/antispam/
talk.to - abuse@come.to - http://come.to/abuse.html
Tande.com - abuse@netforward.com
TeenWorld.POBoxes.com - abuse@netforward.com
Tele2 AB - abuse@swip.net
Telefonica.es - webtelefonica@atento.es or postmaster@telefonica.es
Telefonica-data.net - postmaster@telefonica-data.com
Teleline.es - postmaster@teleline.es
Telenordia.se - postmaster@telenordia.se
The18thHole.com - abuse@netforward.com
Theglobe.com - abuse@corp.theglobe.com
TheGrid - postmaster@thegrid.net
TheGym.net - abuse@netforward.com
Theheadoffice.com - Abuse@FriendlyEmail.com
TheOffice.net - abuse@netforward.com
ThePentagon.com - abuse@netforward.com
TheWaterCooler.com - abuse@netforward.com
tip.net - postmaster@tip.net hh@tip.net
Topsecrets100.com - webmaster@topsecrets100.com
travel.to - abuse@come.to - http://come.to/abuse.html
TSEinc.com - postmaster@tseinc.com
TTD.es - webtelefonica@atento.es or postmaster@telefonica.es
Tucows.com - spammer@idirect.com
UK.uu.net - E-Mail problems - mail@support.uk.uu.net , News problems -
news@support.uk.uu.net , Security problems -
security@support.uk.uu.net
Ultra.net - abuse@rcn.com
UOL.com.br - abuse@uol.com.br - abuse_uolint@uol.com.br -
http://www.uol.com.br/servico/normauso.htm
usol.com - postmaster@usol.com
UTrade.com - support@utrade.com
UUNET - E-Mail Spams abuse-mail@uu.net - Newsgroup Spams abuse-
news@uu.net - If you don't want a reply abuse-noverbose@uu.net -
http://www.usa.uu.net/support/usepolicy/
UWO.CA - postmaster@julian.uwo.ca -
http://publish.uwo.ca/~reggers/spammers
Verizonmail.com - abuse@mail.com
Vids.com - info@vids.com
Voyager.net - abuse@voyager.net -
http://home.execpc.com/web/customersupport/systempolicies/index.html
webcrawler.com - abuse.support@excitecorp.com -
http://www.excite.com/terms.html

Webmaster.se - postmaster@webmaster.se
welcome.to - abuse@come.to - http://come.to/abuse.html
Welnet.com - support@welnet.com
Whowhere.com - spam@lycos.com (place the offending URL or Email address in the subject) - http://pages.whowhere.com/internet/nospammers
window.to - abuse@come.to - http://come.to/abuse.html
WOWmail.com - postmaster@wowmail.com
Writeme.com - abuse@corp.mail.com
XO.net / XO.com - abuse@xo.com - http://support.xo.com/legal/tos.shtml
zap.to - abuse@come.to - http://come.to/abuse.html
Zentek.net - abuse@zentek-international.com - http://www.zentek-international.com/support/aup.shtml
zip.to - abuse@come.to - http://come.to/abuse.html

From : David Jackson (djackson@aol.net) (and this applies to *any* abuse) :
To report an instance of USENET abuse send mail to postmaster@aol.com - please remember to include a complete copy of the USENET article, including all headers, to help us quickly quash the abuse.

Scott reminds us :
It might also be a good idea to remind people that sometimes the postmaster _is_ the spammer. Joe Spam might have his own domain (since they _used_ to be free) inside of which they are the postmaster. This is terrifyingly common with net.twits (kooks, etc.) but seems rare for spam. A quick note that if the spammer is the admin contact in whois, notifying the postmaster will surely generate laughs on their end.

In the letter to the postmaster, you might wish to mention Joel's very good FAQ about advertising on the Internet :

http://www.cs.ruu.nl/wais/html/na-dir/usenet/advertising/how-to/part1.html
http://www.cis.ohio-state.edu/hypertext/faq/usenet/usenet/advertising/how-to/part1/faq.html

One company that was suckered in by a bulk e-mail company received 35 responses to the addresses in the body of the message, and 100% of them were negative. Additionally the ISP that hosted them received 15 complaints asking for them to terminate their service. UUNet received 50+ complaints about this UCE.

And where they *should* advertise :
http://www.cs.ruu.nl/wais/html/na-dir/finding-groups/general.html

Additional business links:
http://www-personal.umich.edu/~jmm/papers.html#efi - Economic FAQ about the Internet
http://www.si.umich.edu/Classes/555/resources/si555syllabus.html - Electronic Commerce
http://www.si.umich.edu/Classes/555/resources/addition.html - Additional Resources

If you don't get a proper response from the postmaster, remember, Whois - rs.internic.net is your friend. See the section labeled "Converting that IP to a name" for more information on Internic.

This *should* get you a person to talk to & their personal e-mail address. If you don't get any response from that postmaster, then you should try the provider to that site. This gets a little trickier, but a traceroute should show you the upstream provider, and from there you can try contacting the postmasters of *that* site.

Any non-profit organization (like a University) should be very happy to help get rid of a spammer if the non-profit organizations resources are being used to spam a for-profit business. The IRS can take their non-profit status away for such things. Talk to the legal council at the non-profit organization if you don't get a positive response from the postmaster.

Worst case, a site can be UDP (Usenet Death Penalty) out so that other sites stop accepting news or even e-mail from that site. They are cut off from the net. Decisions like this are discussed in the news group news.admin.net-abuse.misc .

If the spammer site has problems trying to figure out where the spam

came from, they can *always* get help from the denizens of news.admin.net-abuse.misc, but have them take a look at their logs first and see if they see something like (Thanks to help from Michael):

```
My news logs (for INND) are:
$ cd /usr/log/news
$ ls
OLD                expire.log         news.err           unwanted.log
errlog             news               news.notice
expire.list        news.crit          nntpsend.log

and here is my syslog.conf:
## news stuff
news.crit               /usr/log/news/news.crit
news.err                /usr/log/news/news.err
news.notice             /usr/log/news/news.notice
news.info               /usr/log/news/news
news.debug              /usr/log/news/news.debug

but, what they need to remember, is they HAVE TO LOOK QUICK!.  INND
expire puts all these logs in OLD, and recycles them, and expires them
at the 7th day (and gzips them), i.e., OLD/:
ls -l news.?.*
-r--r-----  1 news      news         181098 May 23 06:26 news.1.gz
...
-r--r-----  1 news      news         319343 May 17 06:29 news.7.gz

so... to grep an old log looking for sfa.ufl.edu:
(the {nn} is how many days ago, 1 is yesterday, 2 is 2 days ago, etc)
cd {log/OLD}
gunzip -c news.1.gz | grep sfa.ufl.edu | more
```

Hoaxes, Fraud on the Internet and The MMF (Make Money Fast) Posts
==========

There are many hoaxes and frauds on the Internet. No different than RL (Real Life). For example there is a letter circulating about "dying boy wants postcards" (Craig Shergold) which is no longer true. Same as with the Blue Star LSD addicting children hoax. See Urban Folklore FAQ at :
http://www.urbanlegends.com/classic/craig.shergold/craig_nyt.html
http://www.urbanlegends.com/classic/blue.star.tattoos/blue_star_lsd_faq.html

A complete Urban Legends listings (It is big) :
http://www.urbanlegends.com/afu.faq/index.html

Some other hoax pages:
http://www.symantec.com/avcenter/hoax.html - Symantec Hoax Page
http://chekware.com/hoax/ - Scams and hoaxes page
http://www.icsa.net/services/consortia/anti-virus/alerthoax.shtml - Hoax
http://www.mercurycenter.com/svtech/news/indepth/docs/virus110399.htm
http://kumite.com/myths/myths
http://ciac.llnl.gov/ciac/CIACChainLetters.html - Chain Letters
http://www.snopes.com/spoons/faxlore/billgate.htm - All about the Bill Gates Hoax chain letter that was followed by a hoax letter from The Gap, Bath & Body Works, Old Navy, Abercrombie & Fitch and probably just about any company you can imagine.
http://www.vmyths.com - Virus Myths
http://www.hoaxkill.com - Look on the site and see if an e-mail is a hoax and if you can't find it forward your e-mails to hoaxcheck@hoaxkill.com and they will look at it for you. If it is a hoax send it to hoaxkill@hoaxkill.com and they will notify everyone in the e-mail that the message is a hoax
http://www.faqs.org/faqs/net-abuse-faq/scams/ - Hoaxes and Scams

And why Disney is *not* giving away 13,000 free trips, why Bill Gates is not collecting e-mail addresses (and many other hoaxes):
http://www.deja.com/article/406150013

My usual response goes something like:

```
<Quote part of the hoax)
> Hi! My name is Janelle McCan, Founder of the Gap. I am offering
> thirty five dollar gift certificates to every seven people you send
> this to.
```

If you ever get an e-mail that tells you to forward it to other people, it is *almost certainly* a hoax. Specifically if it tells you about a "new virus" or free money. Before you send it along *please* look it up by going to http://www.google.com and typing words from the e-mail into the search line, like (in this example) and the word hoax: Gap gift certificates e-mail hoax

Sorry. This is a hoax. See:
http://www.snopes.com/inboxer/nothing/billgate.htm

Plus, if the Gap could trace your e-mails, don't you think the Government could do the same and wouldn't that make you worry *just* a bit? Not that they aren't trying, see:
http://www.zdnet.com/anchordesk/stories/story/0,10738,2606926,00.html

But anyway, there are no free Gap certificates, no free $1,000 bills from Microsoft or any free trips to Disney. Sorry.

PLEASE read about the Gullibility Virus. This is a very funny editorial to be passed along to your friends who send you all these kinds of hoaxes :
http://www.virtualsalt.com/warning.htm
<end of hoax message>

There has been some discussion that such things should be canceled because they exceed the BI 20 index. They are untrue and they waste bandwidth.

A partnership of the National Association of Attorneys General, the Federal Trade Commission and The National Consumers League :
http://www.fraud.org/
Call 1-800-876-7060 or fill out an on-line scam sheet:
http://www.fraud.org/info/repoform.htm
http://www.ifccfbi.gov/ - Internet Fraud Complaint Center
http://www.ifccfbi.gov/strategy/howtofile.asp - How to file a complaint - "It is important that you keep any evidence you may have related to your complaint"
http://www.ifccfbi.gov/cf1.asp - File a complaint
http://www.junkemail.org/scamspam/ - FTC ScamSpam - uce@ftc.gov
http://www.ftc.gov/bcp/conline/edcams/dotcon/index.html FTC Scam Page
The Better Business Bureau has a web site at:
http://www.bbb.org
Hoaxes and scams :
http://directory.google.com/Top/Society/Issues/Fraud/
http://HoaxBusters.ciac.org/
http://www.scambusters.com/
http://www.wired.com/news/politics/0,1283,39298,00.html - A scam if you download a program you may pay $250 in telephone charges.
http://www.nwfusion.com/newsletters/sec/2001/00680235.html - Article on Chain e-mail, pyramid schemes, fraud
http://www.dcn.davis.ca.us/~btcarrol/skeptic/pyramid.html - Robert Todd Carroll's history of pyramid frauds

Virus updates, scams and hoaxes:
From Security Wire Digest (http://www.infosecuritymag.com/newsletter)
MTX-TESTING E-MAIL SCAMS USERS
A scam artist has been making money off gullible users by sending a virus alert about testing for the MTX Worm. The e-mail advises users to call a 900 number, which costs $2.69 per minute, for a recorded message that instructs users to visit three antivirus Web sites--sites that provide AV definitions free of charge. Always check virus alerts and possible hoaxes against hoax web sites or legitimate antivirus authorities, such as Sophos, Trend Micro and TruSecure.
http://www.vmyths.com
http://www.sophos.com
http://www.trendmicro.com
http://www.trusecure.com

Robert Heinlein has a saying "TANSTAAFL" (There Ain't No Such Thing As A Free Lunch). If it looks too good, it probably is.
http://www.deja.com/article/518601356 - Article on "HOW TO CONVERT $99 INTO $588 AS MANY TIMES AS YOU WANT" fraud
There is also a fraud promising you millions of dollars from a "government official" in a small country with a "secret" bank account, but all he needs to transfer the money to you is:
(a)Your Companyís Name and Address
(b)Your full Name(s), Telephone, and Fax numbers (Private and Company)

(c)Your Bank Name, Address, Account number, Telex and swift code (if any).
If you send this information, they have all the information they need to drain your account of all money that is in there. See :
http://home.rica.net/alphae/419coal/news1998.htm
http://home.rica.net/alphae/419coal/ - How to contact the US Gov't about this scheme
Send scams to 419.fcd@usss.treas.gov (Put No Monetary Loss in the header if you haven't lost any money)
http://www.scambusters.org/NigerianFee.html - How the fraud works
http://www.cbintel.com/nigeriafraud.htm
http://www.byte.com/column/vox/BYT19990707S0001

In the United States :
The U.S. Securities and Exchange Commission web page (stock solicitations, stock manipulation by sending out spam after buying a stock to get others to buy the stock and increase the price)
http://www.sec.gov/enforce/comctr.htm or Email:
enforcement@sec.gov
http://www.sec.gov/consumer/iemmtips.htm - Pump and Dump tips
http://www.sec.gov/news/netfraud.htm - SEC prosecutions
Net Securities scam: Report to cyberfraud@nasaa.org
The Food and Drug Administration :
http://www.fda.gov/opacom/backgrounders/problem.html
Medical Items:
US Food and Drug Administration - MedWatch - Medwatch@OC.FDA.GOV
I sent Medwatch a spam about a "miracle fat removing creme" and I received the following, so for non-prescribed drugs I guess you retto the following:
Thank you for your comments. The office of MedWatch does not look into this type of complaint. This information may be given directly to FDA via the web. Please go to http://www.fda.gov. Click on: Buying Medical Products Online. Scroll down to the bottom of the page and click on: Notify FDA About Problem Websites.
http://www.fda.gov/oc/buyonline/buyonlineform.htm

Make Money Fast is a pyramid (or Ponzi) scheme where you are in a chain of people wherein you send money to a few people and try to recruit others to send money to you. Basically if it even remotely smells like a MMF scheme it is illegal (even tho' many of the MMF schemes "claim" to have been looked at by a lawyer or checked by the United States Postal Authorities).

For a list of countries where Make Money Fast is illegal see :
http://www.stopspam.org/usenet/mmf/mmf_table.html
http://www.stopspam.org/usenet/mmf/
http://ga.to/mmf/
Scams can be found at places like :
http://ga.to/mmf/currency.html

Please, only report MMFs in news.admin.net-abuse.misc if they're spam and you've seen it in lots of groups and / or the postmaster/user are defiantly stupid.

MMFs should be reported to the user and their postmaster and the following :

Where to send complaints to in Australia:
Ministry of Fair Trading
P O Box 6355
EAST PERTH 6536

In Canada I believe that the applicable Canadian description can be found at :
http://www.rcmp-grc.gc.ca/html/commerc.htm
And from the Canadian Department of Justice server (http://canada.justice.gc.ca/):
STATUTES OF CANADA, C, Competition - PART VI OFFENSES IN RELATION TO COMPETITION - Definition of "scheme of pyramid selling" - Section 55.1
EXTRACT FROM THE CANADIAN CRIMINAL CODE
Chain-letters
206. (1) Every one is guilty of an indictable offense and liable to imprisonment for a term not exceeding two years who . . .
Pyramid Schemes
55.1 (1) For the purposes of this section, "scheme of pyramid selling" means a multi-level marketing plan whereby ...

United Kingdoms:
Consumer Affairs and Competition Policy Directorate 2
Department of Trade and Industry, 1 Victoria Street, London, SW1H 0ET
        Tel: 0171 215 0344
Have a booklet called 'The Trading Schemes Guide' which is very useful
indeed and explains the UK legal details on these things,

In the United States, you should write the Federal Trade Commission
Ms. Broder
(bbroder@ftc.gov). For more info on pyramid schemes use
pyramid@ftc.gov
To find your nearest postal inspector in the USA, see URL
    http://www.usps.gov/ncsc/locators/find-is.html
California MMF law :
http://www.leginfo.ca.gov/cgi-
bin/calawquery?codesection=pen&codebody=endless

DOES ANYBODY HAVE POSTAL INSPECTOR ADDRESSES FOR OTHER COUNTRIES THAT
PONZI / MMF SCHEMES ARE ILLEGAL IN?

Another type of fraud is one where the spammer sends out a HTML
message with a message / URL link that says "try a new game". When
you click on the URL there is nothing related to the original message.
What the spammer has (at the very least) done is gotten some money for
himself by you clicking on his "click to pay" URL. Worst case the
spammer may have taken advatage of a security hole in your brower and
done something nefarious. Bottom line, do not click on the spammers
URL, look at the HTML and complain to the upstream provider.

   Trying to catch the suspect still logged on
==

If you think you know a machine close to the spammer, you can change
your default DNS lookup server (and get *lots* more info ;-)) by :
$ nslookup
> server wb3ffv.abs.net
Default Server: wb3ffv.abs.net
Address: 206.42.80.130
> ls -d kjl.com
[wb3ffv.abs.net]
 kjl.com.   SOA   kjl.com dns-admin.abs.net. (10
21600 3600604800 86400)
 kjl.com.   NS   ns1.abs.net
 kjl.com.   NS   ns2.abs.net
 kjl.com.   MX   10   abs.net
 kjl.com.   SOA   kjl.com dns-admin.abs.net. (10
21600 3600604800 86400)

If you are quick enough, you can see if the spammer is still on by :

rusers rust.nmt.edu

And you might get :

kuller ray timbers jweinman timbers john timbers rayzer

Assuming that the spammer is from ingress.com you can expand the
Spammers UserID (some sites have expn / vrfy turned off) by:

> telnet ingress.com smtp
Trying 199.171.57.2 ...
Connected to ingress.com.
Escape character is '^]'.
220 ingress.com Sendmail 4.1/SMI-4.1 ready at Sun, 22 Oct 95 15:13:39
EDT
expn krazykev
250 Lipsitz Kevin <krazykev@kjl.com>

We connect to port 25 (smtp) and issues an expn command. Looks like
krazykev@kjl.com is being used as a maildrop for this user. I'll
would send my complaint to postmaster@kjl.com as well (not that it
would do any good in Krazy Kevin's case... but the reply to your e-
mail might be amusing).

To find out the Mail Exchange records, do a nslookup for the MX
records only. You can then look up the expansion of the postmaster or

root to see who they really are. For example :
% nslookup
> set type=mx
> gnn.com

gnn.com preference = 20, mail exchanger = mail-e1a.gnn.com
gnn.com preference = 10, mail exchanger = mail-e1b.gnn.com

% telnet mail-e1a.gnn.com smtp
220 mail-e1a.gnn.com ESMTP Sendmail 8.7.1/8.6.9 ready at Thu, 11 Jan
1996 12:54:26 -0500 (EST)
expn postmaster
250-<wross@ans.net>
250 <gnnadvisor@mail-e1a.gnn.com>
expn root
250-<mitch@ans.net>
250 <gnn-monitor@ans.net>

Duncan tells us 80% of sites that have EXPN and VRFY disabled are
"vulnerable" to the following technique. The risk factor is not
exactly huge it can only be used to test whether an address will
bounce at the tested box.
$ telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 domain.name.you.want.to.know.about ESMTP Sendmail 8.8.8/8.7.3;
Mon, 5 Jun
2000 17:54:21 GMT
EHLO my.computers.name.here
250-my.computers.namme.here Hello admin@localhost [127.0.0.1], pleased
to meet
you
250-8BITMIME
250-SIZE
250-DSN
250-ONEX
250-ETRN
250-XUSR
250 HELP
MAIL FROM:<dps@my.mx.record.was.here>
250 <dps@my.mx.record.was.here>... Sender ok
RCPT TO:<jkfhsdi@domain.you.want.to.know.about>
550 <jkfhsdi@domain.you.want.to.know.about>... User unknown
RCPT TO:<dps@domain.you.want.to.know.about>
250 <dps@domain.you.want.to.know.about>... Recipient ok
QUIT
221 domain.name.you.want.to.know.about closing connection
Connection closed by foreign host.

(The names of the computers have been changed to protect spammer's
accounts and my mailboxen. Naturally you would not normally probe your
local machine this way.)

This obviously only works when you are talking to the machine that
actually delviers the email, so pull out your copy of nslookup find
the MX records, and be sure to use the best MX. I sometimes use this
method to test for abuse, which is probably an alias--this method can
not distinigish between aliases and accounts.

You can use the 'host' command. It's really simple:
% host -t any domain.name

This will give you anything your name server can find out.

% host -t ns domain.name

This tells you the name servers. Not all systems have host, but it's a
small program which should be easy to compile (like whois).

The command "last" will tell where the spammer logged on from last,
but it has to be done by a user from that site. For example :

last imrket4u

Would produce :

imrket4u   ttypf   ip30.abq-dialin.hollyberry.com Fri Sep 15 00:27

```
- 00:34 (00:06)
imrket4u     ttyq8    ip30.abq-dialin.hollyberry.com Fri Sep 15 00:19
- 00:20 (00:01)
imrket4u     ttyqc    abq-ts1              Thu Sep 14 20:42 - 22:21
(01:39)
imrket4u     ttyqc    rust.nmt.edu         Thu Sep 14 18:39 - 18:41
(00:01)
imrket4u     ttypb    abq-ts1              Thu Sep 14 17:55 - 17:57
(00:02)
```

Filtering E-Mail BlackMail, procmail or News with Gnus

Filtering with BlackMail. This is free software that works with Mailers Smail, Sendmail, Qmail or Fetchmail under the OSes: Aix, various BSD, Irix, Linux, NeXTStep 3.x, Solaris, SunOs, SVR4:
http://bitgate.com/spam/ - By Ken Hollis (Not me ...)
Or
http://www.jsm-net.demon.co.uk/blackmail/source

Get the procmail FAQ :

http://www.ii.com/internet/faqs/launchers/mail/filtering-faq/
or
http://www.best.com/~ii/internet/faqs/launchers/mail/filtering-faq/

http://www.ii.com/internet/robots/
or
http://www.best.com/~ii/internet/robots/

Procmail ruleset :
http://sepwww.stanford.edu/oldsep/joe/AntiJunkEmail.html

Or read about it when it is posted to :
Newsgroups: comp.mail.misc , comp.mail.elm , comp.mail.pine , comp.answers , news.answers
Subject: Filtering Mail FAQ

Bob tells me that Eudora Pro has a good filtering capability. You can filer based on who you send e-mail to, known spammers, etc. Enough filters and you may see hardly any Spam. Claris E-Mailer, likewise, has a filter option.

Brian has a Gnus scorefile from the Internet blacklist :
http://www.cs.ubc.ca/spider/edmonds/usenet/gnus/BLACKLIST

Or his example global scorefile :
http://www.cs.ubc.ca/spider/edmonds/usenet/gnus/SCORE

Many news readers have a "kill" file that will filter out the posts from either a certain user-id, or posts with certain titles. Each news reader is unique. You might wish to read the help file on the subject of kill files.

Rejecting E-Mail from domains that continue to Spam

Spamfilters can be found at:
http://www.io.com/~johnbob/jm/index.html
http://www.samiam.org/spam/index.html
http://www-new.hrweb.org/spambouncer/

List of spammers:
http://www.samiam.org/spam/spammers.txt
http://www.idot.aol.com/preferredmail/

Or look at a page on how to block e-mail :
http://www.nepean.uws.edu.au/users/david/pe/blockmail.html

Also how to stop your mail server from being a Spam Relay :
http://maps.vix.com/tsi/

Sendmail patch that permits filtering by envelope sender and recipient as well as by Received: lines, header recipient (To: friends@public..) and enables refusing of relaying _before_ transmission of the message:
ftp://ftp.hiss.org/pub/sendmail/

Ask your admin to add the following to their sendmail.cf. This will

reject all mail that continues to come in from domains that only send out spam. This is a group effort from many admins :
Modify your sendmail.cf in the following way.
1. Setup a hash table with the domains you wish to block:
Bad domains (spam kings)
FK/etc/mailspamdomains

2. Add the following rules to S98 (be sure that there are three lines (i.e. the lines are not split up) and be sure to put a TAB character between the $* and the $#error, not a space) :
Spam blockage
R$* < @$*$=K . > $* $#error $@ 5.1.3 $: "Your domain has been blocked due to spam problems. Contact your administrator."
R$* < @$*$=K > $* $#error $@ 5.1.3 $: "Your domain has been blocked due to spam problems. Contact your administrator."

3. Make your hash table. Here is a very small example :
moneyworld.com
globalfn.com

Mail that comes in from any of these domains will be returned to sender with the error. If the sender is bogus, it will bother the postmaster at the bad domain in an appropriate manner.

Keep in mind that *ALL* email from these domains will be blocked. This is really only a good solution for domains that are setup by spammers for spamming. Blocking something like aol.com, although it may seem initially attractive, would cause problems for legitimate users of email in that domain. Compile your list after careful verification that these domains fit the above description.

Misc.

Origins of Spam

The history of calling inappropriate postings in great numbers "Spam" is from a Monty Python skit (yes, it is very silly... see http://www.ironworks.com/comedy/python/spam.htm) where a couple go into a restaurant, and the wife tries to get something other than Spam. In the background are a bunch of Vikings that sing the praises of Spam. Pretty soon the only thing you can hear in the skit is the word "Spam". That same idea would happen to the Internet if large scale inappropriate postings were allowed. You couldn't pick the real postings out from the Spam. See:
http://www.geocities.com/~hkentcraig/HowInternetSpamGotItsName.html

Geek cartoons, some anti-spam cartoons mixed in:
http://www.userfriendly.org/cartoons/archives/

To join a discussion list for Spams, send a message to
listserv@internet.com
In the body of the message type :
subscribe spamad your_name your_affiliation

Or a real mailing list for the discussion on spamming and about what is and/or isn't possible in dealing with this problem. If you would like to join the mailing list send mail to majordomo@psc.edu with the following message in the body :
subscribe spam-list [preferred address]

Black listed Internet Advertisers :
http://math-www.uni-paderborn.de/~axel/BL/ (Europe)

Oldmilk tells us the alt.spam Commandments :
1) Thou shalt not post binaries to a non binary group.
2) Thou shalt not post "sPaM this l00zer" to alt.spam
3) Thou shalt not post to inform us for the thousandth time that this group was started to discuss the fine spiced ham product from Hormel.
4) Thou shalt not spam this newsgroup.
5) Thou shalt not post on a topic that has nothing to do with spam fighting.
6) Thou shalt not harass any regular poster here, lest your ass be spanked to rosy hue.
7) Thou shalt not attempt to make any straw man arguments that spam is good.
8) Thou shalt read the newsgroup before posting.

First off, the only CORRECT way to "SPAM" the net :
http://www.spam.com/
http://www.spam.com/fc.htm - SPAM Fan Club
http://www.spam.com/ci/ci_in.htm - Spam, SPAM and the Internet ...
Use "Spam" when referring to Internet Unsolicited E-Mail, ONLY use "SPAM" (all CAPS) when referring to the Hormel Product.
Show SPAM Gifts http://coyote.co.net/spamgift/
Or for the free SPAM recipe Book ($1.00 postage and handling) :
SPAM recipe Book, P.O. Box 5000, Austin, MN 55912
Or for SPAM merchandise and apparel call 1-800-LUV-SPAM

SPAM Sites (the food) / The Church of Spam :
http://pemtropics.mit.edu/~jcho/spam/ - SPAM Haiku
http://www.go2net.com/internet/useless/useless/spam.html
http://www.iconnect.net/home/jstrong/spam.html
http://www.rsi.com/spam/
http://www.rsi.com/spam/spam-recipes.html - SPAM Recipes
http://www.spam69.demon.co.uk/spam.htm
http://www.stampo.com/spam.html

A conversation with a spammer. I was amused. First time I had ever spoken with one. I also forgot to mention (in our very short conversation) that his World Wide Web service would be deleted (which it was) :
Me (7:04 PM): I got your spam. By Monday morning all your accounts should be canceled. That would be your AT&T account, your Hotmail account and this AOL account. You are welcome. Bye.
GS711 (7:05 PM): <snip - Expletive Deleted>
Me (7:05 PM): Thank you very much. You should learn how to advertise correctly on the Internet.
Me (7:06 PM): If you do it correctly than you won't have to run and hide.
GS711 (7:06 PM): thanks for letting me know who you are
Me (7:06 PM): Who am I? :-) ...
Me (7:06 PM): BTW, all your Spams will be reported by many other people other than myself ...
(He signed off)

And another exchange with a spammer:
http://x.deja.com/article/607067261

A Spammers Soliloquy. I had to keep this one because it was actually very creative (unexpected from a spammer) :
http://ddi.digital.net/~gandalf/spammersoliloquy.html

And a final note to spammers (I try not to make too many "personal" statements in this FAQ ...). It is best not to be such a pain that the Geeks find an intense interest in you. They are almost certainly smarter than you, at the very least they are smarter in the ways that the Internet works. The worst thing for you, however, is that they usually have no life and can easily make you "their life".

How *did* I get this unsolicited e-mail anyway?
==========
Unfortunately just posting a message to a news group can get unsolicited e-mail. Some spammers "harvest" e-mail addresses by stripping e-mail return addresses out of messages people post. Try posting to alt.test a few times. You will get not only a few autoresponder messages (that is how it is *supposed* to work) but also a few unsolicited pieces of e-mail. The solution to this is to "mung" your address when you post by adding in extra characters (like "Spam") in your return address. You then put in your signature something like "Remove the word Spam from my e-mail to contact me". See:
http://www.private.org.il/harvest.html - How spammers harvest addresses
http://home.cnet.com/software/0-3227888-8-6602372-1.html - Riskiest e-mail behaviors on the Net
http://members.aol.com/emailfaq/mungfaq.html - Address Munging
http://www.applelinks.com/articles/2001/07/20010730122944.shtml - converting email addresses to "digital entities"

Another way to get e-mail is to have a World Wide Web page. Some spammers just start a web spider (a piece of software that just traverses World Wide Web pages and collects information) going and collect e-mail that way. To prevent your e-mail from being harvested, you can "mung" your web e-mail.

Yet another way for spammers to verify your address is real is to have multiple unique pages to their site so that when you click on the URL they provide, they know that you (and only you) got that URL. See: http://cnn.com/2000/TECH/computing/01/14/email.privacy.idg/index.html

Pierre suggests that when putting a mailto URL in a web page, precede and follow it with "%20". When someone clicks on it, it will merely put spaces, which will be ignored, around the address, but when a spammer harvests the address, it will have a %20 in it, which will render it undeliverable.

For additional munging see:
http://www.powerup.com.au/~mfleming/antispam/webmung.html

A suggestion of some nasty little HTML items to have in your WWW page (invisible, of course) are :

```
<A HREF="mailto:root@[127.0.0.1]"></a>
 or if your server allows "server-side includes" (and .shtml) :
<a href="mailto:abuse@<!--#echo var="REMOTE_ADDR"--> ">anti
spambot</a>
```

Also you might include a mail to news gateway like the following so that the Spam is posted to Usenet :

See http://www.sabotage.org/~don/mail2news.html for mail to news gateways.

```
<A HREF="mailto:news.admin.net-abuse.email@myriad.alias.net"></a>
    Or
<A HREF="mailto:news.admin.net-abuse.misc@myriad.alias.net"></a>
    Or
<A HREF="mailto:news.admin.net-abuse.usenet@myriad.alias.net"></a>
```

Note : You should note on your World Wide Web page that these links should *not* be followed by Lynx users, as they will see them no matter how you choose not to display them on a graphical interface. The last few in the below list are particularly not nice as they execute commands on a UNIX host. Substitute root@[127.0.0.1] with any of the following :

```
postmaster abuse root admin postmaster@localhost abuse@localhost
root@localhost admin@localhost postmaster@loopback abuse@loopback
root@loopback admin@loopback
`cat /dev/zero > /tmp/...`@localhost
;cat /dev/zero > /tmp/...;@localhost
`umount /tmp`@localhost
;umount /tmp;@localhost
`halt`@localhost
;halt;@localhost
```

Can I find the persons name and phone from an e-mail address

The short answer is no, not unless the person isn't very smart. The only person that can definitivly tell you who owns that e-mail address is the ISP (i.e. rr.com, digital.net, etc). They will most likely not tell you this information unless you have a warrent from the police forcing them to do so. You *might* find something if you search for any e-mail addresses that they used and see if it pops up any information:
http://www.google.com - Search the Internet
http://groups.google.com/ - Search Usenet

How To Respond to Spam

Howard reminds us :
Note to all: NEVER followup to a spam. NEVER. Express your indignation in mail to the poster and/or the postmaster@offending.site, but NEVER in the newsgroups!

Karen asks:
But what about the newbies who look at a group, see lots of spam and ads, see NO posts decrying them, and conclude that ads are therefore OK?

Ran replies :
When it gets bad, you'll usually see some "What can we do about this?" threads. That's a good place to attach a reply that tells people why it's bad, and what they can, in fact, do.

Austin Suggests:
At the risk of attracting flames, let me suggest an exception to Howard's law. A followup is allowed if the following 3 conditions hold.
   1) The offending article is clearly a SCAM (for instance, the *Canada* calls with the Seychelles Islands phone # scam)
   2) No one else has followed-up with a posting identifying it as a scam (in other words, no 'Me too' warnings)
   3) It is unlikely to be canceled soon, either because it seems to be below the thresholds, or it is in a local hierarchy that doesn't get cancels, or Chris Lewis is on vacation in the Seychelles Islands.
If all three conditions are met, a followup that X's out the contact information , severely trims the contents and identifies the post as a scam is exempt from Howard's law.
Bill's and Wolfgang's addition :
   4) Follow-ups should be cross posted to news.admin.net-abuse.misc _and_ the groups of the spam, but Followup-To: *MUST* be set to news.admin.net-abuse.misc *ONLY*
_or_
post a follow-up and *SET* Followup-To: alt.dev.null.
In the first case change
 Subject: Important FREE $$$
to
 Subject: Spam (was Re: Important FREE $$$)
and include the original Newsgroups and Message-ID line, so the professional despammers will immediately find what you're talking about. Do not post unless you're absolutely sure that you can do all that properly. Also 1) - 3) do apply.

If you see the same article with different Message-IDs in several groups, collect the _complete_ headers of each article and check news.admin.net-abuse.misc if it's already been reported. If not, start a thread with Subject: Spam (was Re: <original Subject>) in news.admin.net-abuse.misc or news.admin.net-abuse.usenet . Include all of the headers and as much of the body of one article as you see fit.

Shalon adds:
One note here: in the soc.subculture.bondage-bdsm group, we have 3 or 4 netcops who *do* follow up each spam message with header, whois, traceroute, and contact address info so that those in the group who do not have the technical skills to determine this can complain. It's an unmoderated sex-related newsgroup which has almost no spam -- so it would appear that the technique works extremely well.

 Firewalls and protecting your computer
==========

If your computer is constantly connected to the Internet (DSL, cable modem, thru a corporate connection) you should have *some* kind of software or hardware that monitors to keep ackers out.

Something I put together about firewalls in general:
http://ddi.digital.net/~gandalf/firewall.html

CERT has released a white paper designed to help technical folks spread the word to home users about Internet security:
http://www.cert.org/tech_tips/home_networks.html

A description of of what a firewall looks for / can tell you is at:
http://www.robertgraham.com/pubs/firewall-seen.html

Review and explanation of firewalls:
http://grc.com/su-firewalls.htm

An example of personal firewall software is:
http://www.zonelabs.com/ - Free for personal use
http://www.finjan.com/ - Surfguard Free for personal use (protects against malicious web pages)
http://www.networkice.com/

The problem with some of these types of software is that they are "technical" when they report an "attack" and the "attack" may or may not be worth noting. Network Ice (Black Ice) seems to work fairly

well IMHO, but again you will need to examine each "attack" and see what it really is before complaining to a provider.

Bottom line, if you are constantly connected to the Internet (or even if you dial up for long periods of time) you should either have a firewall in your network, or run software like the above.

Revenge - What to do & not to do

No matter how much we hate Spam and how much we dislike what the spammers to our quiet little corner of the Universe known as the Internet, Spam is not illegal (yet). If you try anything against the spammers, please * do not * put yourself in risk of breaking the law. It only makes them happy if you get in trouble because you were trying to get back at them.

The reason why spammers use "throwaway" accounts is because they know the e-mail account will be deleted. They usually provide either another e-mail address or a name / phone number or postal address so that prospective "customers" can be contacted. Be sure to complain to the postmaster of all e-mail names provided to make sure that this route is inhibited.

There are sites dedicated to revenge like
http://www.spamcentral.tsx.org

You can ask the Attorney General of a state whether or not that business is licensed in that state, and who runs the business. I looked up a business out of Nevada and found :

http://www.naag.org/ - National Association of Attorney Generals

http://www.state.nv.us/ag/ - We welcome any comments or concerns from you regarding Attorney General matters. If you would like a response from this office, please provide your name, address and telephone number, with your electronic inquiry and this office will respond to you by mail.
Write to : aginfo@govmail.state.nv.us

Look the business name / owner up on the WWW for Las Vegas NV :
http://sandgate.co.clark.nv.us:8498/businessLicense/blindex.htm
Which gave me the following info for the spammer "ROAD TO WEALTH INC":
http://sandgate.co.clark.nv.us:8498/servlet/BusinessLicense?instance=b
lotdetl&license_number=000144-533-3

And see if they are paying the correct taxes:
http://www.state.nv.us/binn/license.htm
Nevada Department of Taxation
555 E. Washington Ave.
Suite 1300
Las Vegas, NV 89101
PH: (702)486-2300
FAX: (702)486-2373

City of Las Vegas
Department of Business Services
P.O. Box 1900
400 Stewart Avenue
Las Vegas, NV 89125
(702)229-6281

Telephoning someone

Calling someone once is fine. If enough people are irritated at the spammer and they all call the 1-800 number the spammer provides, the spammer will get the idea (sooner or later) that it is costing them more in irate people (and most especially loss of business) and it is not worth it to spam.

Do not dial any phone numbers more than once from your home. Phone harassment is * illegal * and you * can * be prosecuted in court for this. Even tho' the caller id blocking code (may be *67 or *71 or some other code) prevents your number from being displayed on their telephone at home if they have caller ID, *57 will give the phone company the number, *69 will dial back the phone number via automatic

call back. If it is a 1-800 number there are two problems. First they can *always* get your phone number, and secondly it may *not* be a toll free number. You may be charged for calling a 1-800 number.

Likewise, do not call collect using 1-800-COLLECT or 1-800-CALL-ATT from home, once again this can be traced.

Austin comments : I would say that calling a listed non-800 number *once* collect to voice a complaint is not harassment, but justified. They sent you a postage due message, didn't they? If they don't want to accept collect calls, they should say so - and if they do, you should be a responsible person and not do it again.

AT&T Information for 1-800 numbers is 1-800-555-1212, but that only helps if you know the company name you are trying to call. Also, you can try searching for a 1-800 number (you do not have to know the company name) at :
http://www.anywho.com/tf.html

Other telephone search mechanisms:
http://expertx.com/Free/xPhone/Locate.htm - Where that phone number is located
http://www.zip2.com/
http://www.bigbook.com/
http://www.switchboard.com/
http://www.555-1212.com/
http://www.anywho.com/areacode/areacodes.html - Tells you where in that state that phone number is located

Snail Mailing someone
==========

Likewise, one well thought out letter sent to the spammer might help convince the spammer not to do this again. Especially if the spammer was part of a corporation that didn't realize the detrimental effects of spamming the Internet.

If you decide to deluge the spammers postal address by filling out one or two "bingo" (popcorn) postage paid cards in the technical magazines (by circling a few dozen "product info" requests per card & putting on printed out self sticking labels with the spammers address), or by putting preprinted labels on postage paid cards that come in the mail in the little plastic packages, don't organize a public campaign (that they can point to) against the spammer in the newsgroup.

Scott also reminds us :
Since this is the "Spam FAQ", I'd like to point this out: You're basically Spamming the company offering information in a magazine. It costs companies money, not the one you're spamming. They get a free pile of junk which is easy to throw out. In other words, this may be harming third parties more than the intended target. I'm not trying to be Mr. Nice Guy, just trying to point out an important technicality.

Organizing a campaign against the spammer could lead to the spammer trying to get a cease & desist police order against the organizers. Likewise, FAXes that are inverse pages (black background on white letters) to a spammer could probably give you problems.

1-900, 1-800, 888, 877 and 1-### may be expensive long distance phone calls
==========
http://www.ftc.gov/bcp/conline/pubs/tmarkg/nine.htm - 1-900 explained
http://www.ftc.gov/bcp/conline/pubs/services/cramming.htm - Mysterious Phone charges

Be very careful when dialing a 1-800 or any "toll free" number you are not familiar with. It may end up being a very expensive mistake. Remember to dial these numbers from a phone booth so that your home phone will never be charged. Another reason to call from a pay phone is so that the spammer cannot get your home phone number. Even if you are "Unlisted" when you call a toll free number the spammer gets your phone number.

All 1-800, 888 or 877 numbers are *not* free. You may be charged for

the phone call. You can tell if the number charges by calling from a phone booth. If you cannot get through then it charges. See below.

Likewise, numbers that may "look" like they are United States long distance phone numbers may in fact be out of country and may cost you $25 or more for a couple of minutes call. These calls are not refundable. A scam artist trying to get money from the phone calls (he gets a skim off the top) was dialing random beepers with an out of country number.

A phone scam can be read at http://www.scambusters.org/809Scam.html

Some area codes to look for (some may not be active for another year or two):
(Also see http://www.nanpa.com/number_resource_info/assignments.html)

242 Bahamas
246 Barbados
264 Anguilla
268 Antigua
284 British Virgin Islands
340 U.S. Virgin Islands
345 Cayman Islands
441 Bermuda
473 Grenada
649 Turks and Caicos
664 Monserrat
670 CNMI (Commonwealth of the Northern Mariana Islands?)
671 Guam
758 St. Lucia
767 Dominica
784 St. Vincent and Grenadines
787 Puerto Rico
868 Trinidad and Tobago
869 St. Kitts and Nevis
876 Jamaica

If the ad says "Procall", it is a large service bureau for 1-900 numbers in Arizona. When you call a pay-per-call number, there should be a recorded intro that will give a customer service number. That *should* connect with a live person.

I would like to thank Eileen at the FTC for kindly answering my questions about 1-900 & 1-800 phone numbers.

Paraphrasing what she e-mailed me :
When a 1-900 number is advertised, the price must also be disclosed (this may be found at 16 CFR Part 308).

When calling a 1-800 number that charges, there must be an existing subscription agreement between the buyer and the seller

http://www.ftc.gov/ Federal Trade Commission Home Page
http://www.ftc.gov/bcp/telemark/rule.htm Telemarketing Sales Rule
http://www.ftc.gov/bcp/conline/edcams/telemarketing/index.html - Telemarketing information / scams
http://www.ftc.gov/bcp/conline/fraud.htm Reporting fraud

(from the "Online Scams page)

Junk Mail - The Law
==========

http://www.jmls.edu/cyber/index/spam.html - Collection of legal spam items
http://www.vtwctr.org/casewatch/
http://192.41.4.29/index.html - 'Lectric Law Library
http://spamlaws.com

Kevyn tells us that : In many countries, forgers of headers can be prosecuted. This is the equivalent of forging a postmark and delivering it yourself. When someone sends out spam with forged headers, he or she clearly:
a) knows that what they are doing is wrong, and that they can be punished for it
b) is clearly attempting to evade detection and punishment.

For Norwegians, these pages may be interesting:
http://www.datatilsynet.no/
(Datatilsynet is a government controlled organisation, made to protect people's right to privacy. This page explains that if someone wants to advertise by email or SMS messages, they need prior consent from the victims)
http://odin.dep.no/bfd/norsk/aktuelt/pressem/004051-070038/index-dok000-b-n-a.html

You should also read Title 47 of the United States Code, Section 227. There is a FAQ at cornell.law.edu for the text of the law (gopher or ftp or http://www.law.cornell.edu/uscode/47/227.html), and you can use DejaNews to read the USC 47 thread on news.admin.net-abuse.misc to make up your own mind (it invariably comes up) or you can look at :

http://www.cybernothing.org/docs/code47.5.II.txt

In Washington (State) (for example) fax laws (RCW 80.36.540 - Telefacsimile messages) define "telefacsimile message" in such a way that could be interpreted to include E-mail. It was not originally written to cover E-Mail, but that is for the courts to decide :-). California regulates it thru Section 17538(d) of the Business and Professions Code.
http://www.newsfactor.com/perl/story/11103.html - Washington State's highest court upholds anti-spam law.

Spammers that have actually been prosecuted. See:
http://www.bibliotech.net/spammer.html
http://www.oneworld-design.com/nospam.html

In California (Quoted from http://Spam.abuse.net): Spamming to or from California e-mail service providers against their policy is now a civil offense under California Business and Professions Code Section 17538.45. If you run a California-based e-mail service provider, you need to notify your customers of the law and your anti-spam policy in order to be eligible to collect damages of $50 per message.
Jeff tells us the California Code referring to spam (CA Bus. Prof. Code Sections 17538.4 and 17538.45) may be found through entering "17538" into:
http://www.leginfo.ca.gov/calaw.html (A pretty authoritative source)
That search pointed to:
http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=705326548+0+0+0&WAISaction=retrieve
Also see:
http://www.netatty.com/spam.html - Sue a California spammer

The Virginia law : http://leg1.state.va.us/000/cod/code51.htm

The Washington State Law : http://www.wa.gov/ago/junkemail/
Spammers successfully sued -
http://www.woodyswatch.com/windows/archtemplate.asp?4-13#watchdog

The Federal Computer Fraud and Abuse Act :
http://www4.law.cornell.edu/uscode/18/1030.html

Additional Resources - Lots Of Links and a *really* good book
==========

The latest & greatest version of the Spam FAQ is found at:
http://ddi.digital.net/~gandalf/spamfaq.html
(or http://home.digital.net/~gandalf/spamfaq.html)
Or *nicely* HTML'ed at:
http://www.cs.ruu.nl/wais/html/na-dir/net-abuse-faq/spam-faq.html
http://fuzzo.com/spam_faq.htm
or
http://www.faqs.org/faqs/net-abuse-faq/spam-faq/
Or the archive at:
ftp://rtfm.mit.edu/pub/usenet/alt.spam/
ftp://rtfm.mit.edu/pub/usenet-by-hierarchy/news/admin/net-abuse/misc/

This is addition to the most excellent Net Abuse FAQ (posted to news.admin.net-abuse.misc, alt.current-events.net-abuse etc...), brought to you by J.D. Falk <jdfalk@cybernothing.org> :
http://www.cybernothing.org/faqs/net-abuse-faq.html
http://samspade.org/d/nanaefaq.html - news.admin.net-abuse.email FAQ

http://www.abuse.net/books.html - Spam Books

A most excellent book for novices and System Admin's alike, much more in depth than this FAQ. A full 191 pages of how to fight Spam. Hopefully if they sell enough then this book will stay updated : Stopping Spam - Alan Schwartz and Simson Garfinkel ISBN : 1-56592-388-X - $19.95
O'Reilly & Associates - 90 Sherman St., Cambridge MA 02140 707-829-0515
Or :
http://stopspam.oreilly.com/

Spam cancellation notice (spam guidelines) :
http://spam.ohww.norman.ok.us/notice.htm
http://www.cm.org for info on NoCeM
http://www.ews.uiuc.edu/~tskirvin/faqs/spam.html

Net abuse jargon:
http://www.ncf.carleton.ca/ip/freenet/subs/complaints/spam/jargon.txt
http://www.deja.com/article/391150606

Software to track the headers / eliminate Spam for you :
http://mirrors.cylink.net/tucows/mac/macintosh.html - Mac software
http://samspade.org/t/ - Sam Spade WWW Spam tools - Excellent!
http://samspade.org/classic/ - Classic version
http://www-oss.fnal.gov/~kschu/fnnews.html - INND PERL spam filter written by Jeff Garzik (Version 3)
http://www.areianet.gr/IRIX_Spamshield/ - Spam Block for IRIX (SGI) based on KAI's spamshield 1.40
http://www.cix.co.uk/~net-services/library/ - Windows Spam Hater
http://www.exit109.com/~jeremy/news/cleanfeed.html
http://www.julianhaight.com/spamcop.shtml - Spam Cop - Does the header analysis for you.
http://www.neoworx.com/home122share.asp - NeoTrace - helps to find any IP number, and possibly the name, address, telephone number and Email contacts of the provider.
http://www.netdemon.net/ - 30+ spam tools ...
http://www.newapps.com/appstopics/Win_95_Anti-SPAM_Tools.html
http://www.spamhippo.com/
http://www.spammerslammer.com - Works with windows e-mail programs that uses pop mail
http://www.ssi-us.com/remove - A project to clean your e-mail from spammers list - You decide if it is good or bad ...
http://www.vipul.net/ricochet/ - automated spam tracing and reporting agent
http://andrew.triumf.ca/pub/security/ - UNIX Tools
http://andrew.triumf.ca/pub/security/reporter/ - Report wide scans

To FTP spamhl.exe Send the following E-Mail:
TO: bitftp@pucc.princeton.edu
BODY: open ftp.compulink.co.uk
cd /pub/net-services
get spamhl.exe
quit

Your Daily Spam News:
Spam@MAIL-ME.COM - Web: http://spam.concordia.ca
Subscribe to Spam-News : join-spam-news@mailshield.com
or - nanas-sub@cybernothing.org
http://www.spam-news.com
http://www.spamhippo.com/cgi-bin/newsspam - Top Spam Sites

Spammers and how to stop them :
http://abuse.net/spam-l - Improve your spam-fighting skills
http://abuse.sourceforge.net/ http://spam.sourceforge.net/ - Anti-spam support site
http://combat.uxn.com/spamhaus.html - spam havens listing
http://come.to/the.lumber.cartel - TINLC - There Is No Lumber Cartel
http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Electronic_Mail/Junk_Email/
http://headlines.yahoo.com/Full_Coverage/Tech/Spam_Wars/ - spam news
http://home.att.net/~marjie1/ - Spam killer central
http://home.att.net/~marjie1/faq.htm - FAQ and gives how to view headers (about half way down)
http://home.att.net/~marjie1/Glossary.htm - Glossary of terms
http://i.am/Spam.Anti/ - Spam Anti!
http://members.aol.com/bombagirl/freeware/email4u.txt - getit4u.txt has a Spam section
http://members.aol.com/macabrus/cpfaq.html - CyberPromo Saga

http://members.tripod.com/~cyberstalked/hb140.html - Maryland Anti-Harassment bill
http://members.tripod.com/~cyberstalked/story.html - Stalked by The Woodside Literary Agency
http://members.tripod.com/~JOWazzoo/ConsumateSpamLinks666-FAQs.html Consummate FAQ's page
http://members.tripod.com/~JOWazzoo/ConsumateSpamLinks666.html - Consummate Spam Links Page
http://morehouse.org/hin - Internet Security
http://persona.www.media.mit.edu/judith/Identity/IdentityDeception.html
http://rvl4.ecn.purdue.edu/~cromwell/lt/468.html - Internet Security
http://slashdot.org/articles/99/08/02/129213.shtml - ISP sues spammer
http://spam.abuse.net/spam/
http://spam.abuse.net/spam/howtocomplain.html
http://viper.law.miami.edu/~froomkin/articles/oceanf.htm Regulation of Computing and Information Technology
http://www.connect.ab.ca/~rkinf/spam.htm - Spam Reduction Page
http://www-db.aol.com/corp/news/press/view?release=531& ; - AOL wins against Spammers
http://www-fofa.concordia.ca/spam/complaints.shtml - Complaint Addresses
http://www.abuse.net/cgi-bin/list-abuse-addresses - Complaint
http://www.antionline.com/ - Internet Security
http://www.ao.net/waytosuccess/nospam.html
http://www.ao.net/waytosuccess/spamnews.html
http://www.cabal.net/jason/index.html - A spammer tries to sue the Cabal (TINC)
http://www.cauce.org - Trying to legislate against
http://www.ecofuture.org/ecofuture/jnkmail.html - How to Get Rid of Junk Mail, and Telemarketers
http://www.claws-and-paws.com/spam-l/ - Improve your spam-fighting skills
http://www.claws-and-paws.com/spam-l/tracking.html
http://www.coachnet.com/soho_21.htm - Small Office / Home Office Newsletters Anti-Spam Articles for business
http://www.coachnet.com/soho_22.htm
http://www.coachnet.com/soho_29.htm
http://www.cs.purdue.edu/coast/hotlist/ - Internet Security
http://www.cybercrimecorp.com/ - CyberCrime Corp Hi-Tech Crime Prevention and Investigation
http://www.faqs.org/faqs/by-newsgroup/news/news.admin.net-abuse.email.html
http://www.faqs.org/faqs/net-abuse-faq/
http://www.hostedscripts.com/scripts/antispam.html - A script to generate e-mail addresses
http://www.internetwk.com/columns/frezz020199.htm - A good article on why the Internet should be self governing WRT Spam
http://www.junkemail.org/scamspam/ - "Help stop Scam Spammers!"
http://www.kclink.com/spam/ - A fight to bill Spammers
http://www.looksmart.com/eus1/eus53832/eus53833/eus225492/eus282819/eus278700/r?l&igv& - Spam link list
http://www.mcs.com/~jcr/junkemail.html
http://www.MsgTo.com - spam free e-mail - Asks first-time unsolicited senders of email to prove they're human and not a spambot.
http://www.nags.org/
http://www.onelist.com/subscribe.cgi/anti-spam - Anti-Spam mailing list
http://www.ot.com/~dmuth/spam-l - Maintainer of the Spam-L FAQ
http://www.petemoss.com/
http://www.phase-one.com.au/fravia/pageadvi.htm - Stalking the spammer Enemy
http://www.robertgraham.com/ - Infosec / computer security page
http://www.sengir.demon.co.uk/spam_sites.html - Where spammers get their software
http://www.sengir.demon.co.uk/uf000359.gif - A computer contemplates spam (see http://www.userfriendly.org/static)
http://www.spamcon.org/ - Resources to help Recipients, Marketers, Sysadmins and Legal pros
http://www.spamgirl.com/email.htm
http://www.spamroundtable.com
http://www.stanford.edu/~edhou/StanfordSpamFAQ.html
http://www.stopspam.org/email/headers/headers.html - More Reading Headers
http://www.studio42.com/kill-the-spam/index.html - "I am sick of Spam and I want it to stop"
http://www.sunworld.com/swol-08-1997/swol-08-junkemail.html - Sunworld Anti-Spam

http://www.usenet2.org/ - A Usenet with no Spam
http://www4.zdnet.com/anchordesk/story/story_index_19970819.html -
Special Spam Fighting Edition

E-Mail headers and tracing tools FAQs and links:
ftp://info.cert.org/pub/tech_tips
http://crash.ihug.co.nz/~bryanc/ - Mac WhatRoute
http://eddie.cis.uoguelph.ca/~tburgess/local/spam.html
http://home.earthlink.net/~laser3/simon.html - Yet another newbie
guide
http://kryten.eng.monash.edu.au/gspam.html
http://members.aol.com/emailfaq/emailfaq.html
http://members.aol.com/emailfaq/resource-list.html
http://t2.technion.ac.il/~s2845543/yanig.html - Also yet another
newbie guide
http://www-fofa.concordia.ca/spam/tools.html - Macintosh Spam fighting
http://www.crl.com/~sjkiii/news-admin-net-abuse.html
http://www.deja.com/article/420339665 - Forgery FAQ
http://www.deja.com/article/436881631 - How spammers get your E-Mail
address
http://www.elsop.com/wrc/nospam.htm
http://www.exit109.com/~jeremy/news/antispam.html - Spam Software
http://www.rahul.net/falk/index.html#howtos
http://www.spam-archive.org/ - A collection of email-Spams.
http://www.ultranet.com/~gmcgath/selfdefense.html
http://www.webfoot.com/advice/email.biblio.html - General E-Mail info
http://www.winsite.com/win3/winsock/page6.html - Windows Internet
Utilities
http://www.winsite.com/win95/netutil/index.html - Win 95 Net Utils
http://www.winsite.com/win95/netutil/page11.html - netcop /
netlab95.zip

Spam Info in other languages:
http://cwisdb.cc.kuleuven.ac.be/pisa/nl/spam.htm - Netherlands
http://inews.tecnet.it/articoli/aprile98/Netsurfing9804a.html -
Italian
http://kulichki-lat.rambler.ru/moshkow/SECURITY/stopfash.txt - Russian
http://member.nifty.ne.jp/usr/negi/news.html - Japan
http://member.nifty.ne.jp/usr/negi/newsgroup0.html - Japan
http://people.frankfurt.netsurf.de/Wolfgang.Kynast/nospam.htm - German
Anti-Spam links ...
http://perso.magic.fr/roumazeilles/spamantf.htm - Spam Anti! French
http://www.alkar.net/moshkow/html-KOI/SECURITY/stopfash.txt - Russian
http://www.despaml.interrob.de/ - German Anti-Spam Mailing List
http://www.droit.umontreal.ca/~labbee/ - French (Canadian)
http://www.ethereal.ru/~avk/anti-ad.html - Russian spam & headers page
http://www.euro.cauce.org/ - Many languages
http://www.euro.cauce.org/en/index.html - English
http://www.nextel.no/kundesenter/hjelp/guider/901645506.5885.html -
Norway
http://www.online-recht.de/vorent.html?LGBerlin980514 - German Anti-
Spam and costs
http://www.rewi.hu-berlin.de/~gerlach/falsche-email-adressen.html -
German False E-Mail FAQ
http://www.snafu.de/~laura/de.admin.net-abuse.mail.txt - German net
abuse FAQ
http://www.student.hro.nl/0445746/ - Dutch anti spam site

Translate from/to English French, German, Spanish, Portuguese, Italian
(etc.)
http://babel.altavista.com/translate.dyn
  or
English to French:
http://translate.google.com/translate?hl=fr&sl=en&u=http://ddi.digital
.net/~gandalf/spamfaq.html
English to German:
http://translate.google.com/translate?hl=de&sl=en&u=http://ddi.digital
.net/~gandalf/spamfaq.html
English to Italian:
http://translate.google.com/translate?hl=it&sl=en&u=http://ddi.digital
.net/~gandalf/spamfaq.html
English to Spanish:
http://translate.google.com/translate?hl=es&sl=en&u=http://ddi.digital
.net/~gandalf/spamfaq.html

Or why Netabuse is bad :
http://cnn.com/TECH/computing/9808/10/tastyspam.idg/
http://www.fraudbureau.com/articles/consumer/article14.html - The cost

of spam
http://www.angelfire.com/co2/spamjamr/index.html - Good commentary on why SPAM costs
http://www.nwfusion.com/news/2001/0104spamspam.html - Time and cost of SPAM
http://www.nwfusion.com/news/2001/0104spambust.html - Two busted for Spam fraud / envelope stuffing
http://www.nwfusion.com/columnists/2001/0416gibbs.html - ?Logic? of a spammer and why (if everybody did it) you would get 1,370 e-mails per hour

Protecting your reputation in Cyberspace - How To / How Not To communicate on the Internet:
http://www.nwfusion.com/newsletters/sec/2001/00322091.html - Part 1
http://www.nwfusion.com/newsletters/sec/2001/00380626.html - Part 2
http://www.nwfusion.com/newsletters/sec/2001/00408507.html - Part 3 - Why not to spam
http://www.nwfusion.com/newsletters/sec/2001/00408551.html - Part 4
http://www.nwfusion.com/newsletters/sec/2001/00450966.html - Part 5
http://www.nwfusion.com/newsletters/sec/2001/00477475.html - Part 6
http://www.nwfusion.com/newsletters/sec/2001/00519056.html - Part 7
http://www.nwfusion.com/newsletters/sec/2001/00477474.html - How Not To Send Out An "Alert"

Equal time, The spammer's viewpoint (Why Spam is good):
http://www.juicycerebellum.com/spam.htm
http://listen.to/spammers - Spammers Speak
http://members.theglobe.com/SpamSucks/spamspeak.html - Spammers Speak
http://x.deja.com/article/484286843 - Gerald Kohler (gkohler@worldnet.att.net) argues for spam, with some good rebuttals. Click on "Thread" then click on message 8 then click on next in thread to follow the conversation.
Opinions from one spammer (I wouldn't trust much of what is said in these pages if anything at all ...):
http://www.marketing-2000.net/
http://www.marketing-2000.net/legal.html - Bulk E-Mail - Is It Legal? "Many of these anti-spammer extremists do not have regular jobs" (Hmm ... I guess my 50+ hour a week high tech job doesn't count?)
http://www.marketing-2000.net/survpage.html - Bulk E-Mail Marketing guide
http://www.marketing-2000.net/testify.html - Testimonies
Of course feel free to send your comments to escalate@marketing-2000.net concerns@marketing-2000.net or questions@marketing-2000.net

What the alt.binaries.slack Organization has done to fight Spam :
http://www.sputum.com/spit/Main.htm
http://www.shreve.net/~cuthulu/sputum/

And the Alt.Gothic Special Forces:
http://www.legendsmagazine.net/pan/agsf/index.htm

Proud to be a NetScum (Many anti-Spammers have been added by the spammers) :
http://www.bostonphoenix.com/supplements/TheNet/fall97/NET_SCUM.html
http://www.algebra.com/~ichudov/images/netscum/
http://www.netscum.org/
http://www.aldeberan.org/netscum/index.html - NetScum Site Recreated

Disclaimer : I am not a lawyer, 80% of the Internet is bull, free advice is worth every penny you paid for it :-). Brought to you via News since November 1995.

Do not meddle in the affairs of wizards for they are subtle and quick to anger.
Ken Hollis - Gandalf The White - gandalf@digital.net - O- TINLC
WWW Page - http://ddi.digital.net/~gandalf/
Trace E-Mail forgery - http://ddi.digital.net/~gandalf/spamfaq.html
Trolls crossposts - http://ddi.digital.net/~gandalf/trollfaq.html

Send corrections/additions to the FAQ Maintainer:
gandalf@digital.net (Ken Hollis)

Last Update January 24 2002 @ 00:49 AM