

Jamie, in a kind inimitable way, has informed me that some of the scumware sites are showing this page in popups. If you see this alt.spam FAQ in a popup please be assured that spyware / adware sites are doing this to try to discredit anti-spam / anti-spyware sites. See:

<http://www.spywareinfo.com/~merijn/downloads.html>

and

<http://www.spywareinfo.com/articles/hijacked/>

Please see my [section on removing spyware](#).

Thanks,

Ken

From: gandalf@digital.net

Subject: alt.spam FAQ or "Figuring out fake E-Mail & Posts". Rev 20050130

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

Summary: This posting describes how to find out where a fake post or e-mail originated from.

Archive-name: net-abuse-faq/spam-faq

Posting-Frequency: monthly

Last-modified: 20050130

URL: <http://gandalf.home.digital.net/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 :-)) :

- o [Introduction](#)
 - o [The Easy Way To Get Rid Of spam](#)
- o [Tracing an e-mail message](#)
 - o [What computer did this e-mail originate from?](#)
 - o [MAILING LIST messages](#)
- o [Reporting Spam and tracing a posted message](#)
- o [WWW IP Lookup URL's](#)
- o [Converting that IP to a name](#)
 - o [What to do with "strange" looking Web links](#)
 - o [Getting a World Wide Web page busted](#)

- o [Usenet complaint addresses](#)
 - o [Viruses / Trojans / Spyware](#)
 - o [Fraud on the Internet and The MMF \(Make Money Fast\) Posts](#)
 - o [Nigerian Advance Fee Fraud](#)
 - o [Hoaxes](#)
 - o [Open system spammers love](#)
- o [Filtering E-Mail BlackMail, procmail or News with Gnus](#)
 - o [Rejecting E-Mail from domains that continue to Spam](#)
- o [Misc. \(Because I can't spell miscellaneous :-\)\) stuff](#)

I couldn't think to put anywhere else.

 - o [Protection for you and your kids on the Internet](#)
 - o [I am interested in eliminating spam from my emails, how do I do this?](#)
 - o [Origins of Spam](#)
 - o [How *did* I get this unsolicited e-mail anyway?](#)
 - o [Can I find the persons name and phone from an e-mail address?](#)
 - o [How To Respond to Spam](#)
 - o [Firewalls and protecting your computer](#)
- o [Revenge - What to do & not to do \(mostly not\)](#)
 - o [Telephoning someone](#)
 - o [Snail Mailing someone](#)
- o [1-900, 1-800, 888, 877 and 1-### may be expensive long distance phone calls](#)
- o [Junk Mail - The Law](#)
- o [Additional Resources - Lots Of Links](#)

Introduction

=====

Jamie, in a kind inimitable way, has informed me that some of the scumware sites are showing this page in popups. If you see this alt.spam FAQ in a popup please be assured that spyware / adware sites are doing this to try to discredit anti-spam / anti-spyware sites. See:

<http://www.spywareinfo.com/~merijn/downloads.html>

And

<http://www.spywareinfo.com/articles/hijacked/>

Also please see my [expanded section on removing spyware](#).

Please feel free to repost this, e-mail it, put this FAQ on CD's or any other media you can think of. Just please do not pop it up on the screen of anybody who didn't request it.

The latest & greatest version of the Spam FAQ is found at:

<http://gandalf.home.digital.net/spamfaq.html>

or

<http://home.digital.net/~gandalf/spamfaq.html>

or

<ftp://rtfm.mit.edu/pub/usenet/alt.spam/>

Also see:

<ftp://rtfm.mit.edu/pub/usenet/alt.syntax.tactical/>

Please email follow-ups / additions / changes comments / questions to gandalf@digital.net . . . BUT PLEASE **NOTE** because I receive (on the average) over 200 e-mails **EVERY** day (of which 195 or so are spam) you **MUST** put the words "Alt.spam" in the subject of the e-mail or there is a **VERY** good chance the e-mail will be deleted without being read. I get 10 or 15 "No Subject" spams a day.

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.

If you are in the United States and have not yet written to your Senator or House of Representatives about how terrible the CAN-SPAM act is, I would ask you to do so. Bottom line is that there are many large corporations and over 22.9 million small businesses on the United States. If you received just one e-mail a year from each of the small businesses (I am not even including large companies) you would receive 63,800 e-mails PER DAY. According to CAN-SPAM you would then be required to opt out of each and every one of these e-mails, and the company has 10 days to honor your request. Of course this would not stop spammers from changing company names every 10 days and just start spamming all over again. I have written a letter explaining why I think that this act was poorly written, and I would ask you to write a letter to your representatives also:

<http://home.digital.net/~gandalf/CAN-SPAM.htm>

<http://gandalf.home.digital.net/CAN-SPAM.htm>

How did this incredibly bad law get passed? This law was written without any public hearings, with input from only the marketing industry and Internet Service Provider lobbies (guess who loses, You Do). From <http://www.cauce.org/news/index.shtml> :

"CAUCE is also disappointed that both the House and Senate versions of this law were passed without any public hearings, instead being written and passed solely through back-room compromises and with the input of the marketing industry and Internet Service Provider lobbies, but with scant regard for the interests of America's consumers and business Internet users."

Apparently one of the lobbying groups talking to our representatives (for you) is The Center for Democracy and Technology. They were kind enough to speak for "everybody" in this missive sent to Congress:

<http://www.cdt.org/speech/spam/031015cdt.shtml>

They supported everything the Direct Marketing Association (<http://www.the-dma.org/> (telemarketers)) and spammers wanted in a bill and more.

CDT is supported by many different companies:

<http://www.cdt.org/mission/supporters.shtml>

Find Your Senators at http://www.senate.gov/general/contact_information/senators_cfm.cfm and find your US Representative: <http://www.house.gov/writerep/> (Fill in your state and zip, click "Contact My Representative" and you will be told who your representative is). Go To: <http://www.house.gov/house/MemberWWW.html> , click on their site and your representative should have an address at the bottom of the page for where to write them. I would also suggest that you cc the two sponsors of the bill: Conrad Burns 187 DIRKSEN SENATE OFFICE BUILDING WASHINGTON DC 20510 and Ron Wyden 516 HART SENATE OFFICE BUILDING WASHINGTON DC 20510.

Davjohn suggests going to <http://congress.org> , plug in your zip code and click on GO. Internet Explorer and Netscape will show you your representatives. Safari browser did not work at this site.

And why CAN-SPAM won't work:

<http://www.google.com/search?q=CAN-SPAM+won%27t+work>

<http://www.google.com/search?q=Critics+CAN-SPAM>

<http://www.gripe2ed.com/scoop/story/2003/12/11/9145/0712>

http://www.circleid.com/article/725_0_1_0_C - And how the DMA is trying to convince the public that CAN-SPAM works

Before trying to determine where the post or e-mail originated from, you should realize that (just like 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...

The Easy Way To Get Rid Of spam

=====

Sorry to tell you this but if you received a spam (Unsolicited Commercial E-Mail) there is no "easy" way to get the spam stopped. Generally if you reply (unsubscribe) this confirms that your e-mail address is "live" and just gets your e-mail address sold to other spammers. Spam has to be dealt 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. The "easiest" way to stop getting spam is to change your e-mail address and only give your e-mail address to people you absolutely trust, and to NEVER allow the e-mail address to be posted to a web site or posted ANYWHERE on the internet. To see how many times my e-mail address appears on the Internet go to the following link:

<http://www.google.com/search?q=gandalf%40digital.net>

<http://www.nwfusion.com/newsletters/edu/2003/0324ed1.html> - E-Mail addresses on the web attract the most spam

If your e-mail address shows up on a search engine, then the spammers can find your e-mail address also. Be careful about giving your e-mail address to companies that purport to be against spam:

<http://www.gripe2ed.com/scoop/story/2003/5/15/10299/0559>

There are businesses that make a good living filtering out spam both on a personal and corporate level. I would suggest that if you really don't want to deal with spam that you get an e-mail address from one of these services (Please note I am not recommending this service, just using it as an example). Do a search:

<http://www.google.com/search?q=email+hosting+spam>

And you will come up with companies like:

<http://www.No-JunkMail.com/>

Or if you wish to block it from your personal e-mail account do a search on something like:

<http://www.google.com/search?q=spam+blocking+software>

And you will come up with examples like:

<http://www.spamulor.net/> - Free

<http://www.spambutcher.com/>

Be aware that no spam blocking software (as of yet) is perfect and you may get "false positives". An e-mail from a friend may be detected as spam and may get deleted as spam or moved to the spam box.

The spam wars:

<http://computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html>

Davjohn reminds us that if you are required to give a "legal" e-mail address to a company you don't know or trust, go to <http://mail.com> and set up a free account. There are a hundred-or-so variations available. General.delivery@arcticmail.com sounds like a Santa Clause e-mail address. He has 2 addresses there. About once a week he goes in and clicks "empty" and ~flush~ it's all gone.

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 Bob, Dave, Kathy, Michael, Piers, Russ, Simon, Chalmers 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

Eudora V5.1:

1) Double-click on the email subject line in the current mailbox. This displays the same message with a fuller version of the header, which will be enough for some ISPs but not all, and also shows an extra Toolbox which contains the BlahBlahBlah button

2) Click on the BlahBlahBlah button

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 - How to set show the mail headers in hotmail:

1. After you login, just to the right of the tabs, select Options
2. Under Additional Options, select Mail Display Settings
3. In the Message Headers section, click the Advanced button

JUNO - Click on the word "OPTIONS" in the MENU BAR.

On This menu, click on "E-Mail Options (ctrl-E)"

This will get you a Dialog Box:

In the "Show message headers" part, you need to have the "Full" button marked in order to show full message headings.

KMAIL (KDE Mail Client) - Bryan tells us To display all headers in kmail(KDE mail client), go to 'view' and click 'all headers'.

Lotus Notes R4 and R5:

- 1) Examine the fields in the document.

Click on File --> Document Properties

Click on fields tab (square rule)

Scroll down to the "received" fields - there should be one for each "received" header added.

Copy and paste these into a file.

2) Export the headers from the document

important You need to be in the inbox folder in Notes

Select the document.

Click on File --> Export

Enter a temporary file name, ensure File type is "Structured Text"

Under Export options, click on "selected documents", click OK.

The generated file contains all the headers on the message along with the message body.

Lotus Notes R6: Open the mail, View/ Show /Page Source and the OpenNTF mailtemplate has an action to forward the full header (to yourself, or to support for instance). You may want to copy that, or use the template.

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.

Microsoft Outlook 2000 - From the Menu Bar select "View" and then "Options" from that menu.

This displays a dialogue box called "Message Options".

The largest and last text box is called "Internet headers:"

Scroll through this to read all the details.

To save a copy, highlight all the content, and copy it to the clipboard by pressing <Ctrl C> (thats both those keys at the same time), then go into whatever word processor or email program you wish and press <Ctrl V> to paste the text onto that page.

Because Microsoft Outlook has many security flaws, the below instructions may expose your computer to risks. See:

http://www.the-foxhole.org/Disabling_IE_Security_Flaws.htm

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.

Mike tells us a better way to expose the headers and copy the body for **MS Outlook Express** is as follows:

<http://www.spamcop.net/fom-serve/cache/119.html>

The mouse selections are File/ Properties/ Details tab/ Message source button. The keyboard access is alt-Enter ctrl-Tab alt-M. Once accessed the remainder of commands are as discussed elsewhere:

Mouse; R click context menu, Select all, Copy or Keyboard; ctrl-A ctrl-C. The Message Source

described here is the headers + attached spam body. If one only wanted the complete headers without

spam body, they would stop one step earlier at the Details tab section above.

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.

WebTV - <http://www.haltabuse.org/help/headers/webtv.shtml> :

1) While viewing the email, hit "Forward" on the sidebar. Address the document to yourself. Completely erase the subject line.

2) Put your cursor on the first line of the "body" (text area); Hit "Return" (enter) twice. Your cursor should now be on the 3rd line of the text area.

3) Type any "Alt" character on this line; DO NOT HIT "RETURN"

4) Cut and Paste the "Alt" character onto the subject line: (CMD+"A"), (CMD+"X"), (CMD + "V") The "Alt" character should "jump" down to the message text-area.

5) Hit "Send"; open the received mail.

Ximian Evolution (Linux email program) to display full headers, open the message, go to the VIEW menu and choose message display>full headers.

Yahoo-

-Click on the "Mail Options" link located near the top right-hand side of the page.

-Click the "General Preferences" link.

-Locate the Show Headers heading and select either "Brief" or "All."

-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://help.att.net/docs/use/email/gen/prb_msol_mac_headerinfo.htm?platform=osnone - MS Outlook Express for the Mac

http://help.att.net/docs/howto/other/win/prb_all_all_ns-header.htm?platform=osnone - Netscape Messenger or Netscape Mail

http://www.wurd.com/cl_email_outlook_headers.php - MS Outlook

http://www.wurd.com/cl_email_msie_headers.php - MS Outlook Express

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

George tell us that the gateway that Lotus provides, SMTPLink (is one of those Microsoft-style utilities that's functional, but just barely) has an administrator-configurable setting for handling RFC-822 headers on inbound (to cc:Mail) messages. Headers can be completely discarded, or copied to an attachment.

George also tells us in the R6 client, headers (if saved to an attachment in the gateway) are viewable as an attachment, as noted above. The R8 client handles things differently, hiding the existence of the headers attachment, and making the content available only by going to the inbox or a message folder,

right-clicking on "Properties", then selecting the "history" tab. From there, it's possible to copy/paste into another document. Header information is left in its original chronological order (unlike Notes, which takes the liberty of sorting all the headers into alphabetic order).

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://support.xo.com/abuse/guide/guide1.shtml>

<http://www.rahul.net/falk/mailtrack.html>

A little different description of headers:

<http://digital.net/~gandalf/trachead.html> - Line by line tracing of a spammers e-mail

<http://digital.net/~gandalf/trachead2.html> - Line by line tracing of a spammers e-mail when the spammer has inserted a "Fake" Received line to confuse tracking the e-mail.

<http://help.mindspring.com/docs/006/emailheaders/>

<http://help.mindspring.com/features/emailheaders/extended.htm>

<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 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:qmailr@mail.bestnetpc.com [205.160.183.3]) by 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|host) 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://samspace.org/> , 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 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://www.ordb.org/>

<http://dsbl.org/main>

<http://relays.osirusoft.com/>

<http://relays.osirusoft.com/cgi-bin/rbcheck.cgi> - See if a server is on a BlackHole list, i.e. an open relay

<http://www.dorkslayers.com/>

<http://spamhaus.org/sbl>

<http://mail-abuse.org/rbl/usage.html>

<http://samspade.org/>

<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 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 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 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 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]) by air-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: <13653344018870252@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 Provider) 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 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.

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.

That having been said, e-mail from a Listserv 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 can 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.killfile.org/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://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 B11A 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://groups.google.com/>

WWW IP Lookup URL's

=====
<http://samspade.org/> - My personal favorite. All the tools you need 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://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

Index to Traceroute pages:

http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Software/Networking/Utilities/Traceroute/

<http://www.traceroute.org/>

SWITCH WHOIS Gateway:

http://www.switch.ch/search/whois_form.html

Or

<http://www.networksolutions.com/cgi-bin/whois/whois>

<http://www.ripe.net/perl/whois> - European countries WhoIs

<http://www.apnic.net/apnic-bin/whois.pl>- Asian Pacific WhoIs

<http://whois.nic.or.kr/>- Korean WhoIs

<http://www.arin.net/>- North / South America WhoIs (Upper Right Corner)

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

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

For a full list of bogus IP addresses see:

<http://www.cymru.com/Documents/bogon-dd.html>

<http://www.cymru.com/Documents/bogon-list.html>

And a couple of other "mysterious" private IP addresses (that are not mentioned in any of *my* network books):

169.254.0.0 - 169.254.255.255 - IPV4 Auto Configuration address range (Draft RFC)

192.0.2.0 - 192.0.2.255

See :

http://www.ja.net/CERT/JANET-CERT/prevention/cisco/private_addresses.html

First off try using NSLookup (there is software for PC's, I use <http://samspace.org/> , 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.

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/>

<http://www.webspawner.com/users/ipconverter>

URL Decode:

<http://www.swishweb.com/dec.htm>

An example of a complex URL decode:

<http://home.digital.net/~gandalf/URLDecode.txt>

If you look at the source HTML and you see the following then the spam has been encoded using Base64:

Content-Transfer-Encoding: base64

To decode, just copy / paste everything below the above line and click "Decode" into:

<http://david.carter-tod.com/base64/>

You will now have the HTML code.

This decode decodes scripts encoded with the Microsoft Script Encoder:

<http://www.greymagic.com/security/tools/decoder/>

<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.

<http://www.netdemon.net/tools.html> - All the tools.

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:

CC EE 9B 49

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.sampade.org/10.00.0.1/xxxstuff.html>, try <http://sampade.org/>

Or if that doesn't work, Andreas suggests:

Something like following does NOT work the obfuscated URL form at sampade but I figured out that these can be typed into a html-file with a texteditor or in Netscape composer 6.x in the source-mode, than loading or switching to the html mode will immediately show the decoded characters, should be an URL with a form mailer or something like "mailto:user@domain.nic"

97;ilto:jimmy1440200&#

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.oooooooooooooooooooo.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 ooooooooooooooooooooo.com, using port 80. The rest of it is "decoded" by ooooooooooooooooooooo.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 you get something like:

```
<!-- CHANGE EMAIL ADDRESS IN ACTION OF FORM --><FORM name="form" method="post"
action="&#109;&#97;&#105;&#108;&#116;&#111 ;&#58;&#109;&#111;&#114;&#116;&#109;&#97 ;
&#105;&#108;&#54;&#64;&#121;&#97;&#104 ;&#111;&#111;&#46;&#99;&#111;&#109;&#63 ;
&#115;&#117;&#98;&#106;&#101;&#99;&#116 ;&#61;&#68;&#101;&#98;&#116;&#49;"
enctype="text/plain"
```

Then take the "funny" looking part and paste it into the "Obfuscated URLs" section of <http://sampade.org/> like so:

<http://mailto ;:mortma ;>

il6@yah ;oo.com? ;
subject ;=Debt1

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: digital.net
```

```
Address: 198.69.104.2
```

```
> set type=ptr
```

```
> 181.126.183.204.in-addr.arpa
```

```
Server: 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 - Rseaux IP Europens, 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 likelihood 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 (Domain Information Groper) (or one of its derivatives), it is used to search DNS records :

<http://www.spacereg.com/a.rpl?m=dig>

<http://www.gulftech.org/webtools/webutil.pl?dig>

<http://tools.bintec.com/>

What DIG tells you:

<http://home.att.net/~marjie1/Dig.htm>

```
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  revd: 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/>

There are spammers out there that actually have a clue. They use open Web Proxies to reroute their web page to another location. When you do a ping of a web site, the ping is of the open web proxy. The open web proxy then redirects you when it gets the request for the web page. A complete technical explanation can be found at:

[http://www.google.com/groups?selm=3ee16105\\$1_2@nntp2.nac.net](http://www.google.com/groups?selm=3ee16105$1_2@nntp2.nac.net)

Another thing spammers do is to abuse free WWW services to set up a web page that is encoded with Java script so that you cannot see what the html looks like. The spammer then redirects the information to their "real" site.

<http://www.spamsites.org/decode.html> tells us that to decode the Java script and complain to the people that are actually hosting the spammers, set up a bookmark called "Decode Javascript" and set the URL (thanks to Code by Kicken) as the below, the code is all on one very long line:

```
javascript:h=document.getElementsByTagName('html')[0].innerHTML;function disp(h){h=h.replace(/</g, '\n&lt;');h=h.replace(/>/g,'&gt;');document.getElementsByTagName('body')[0].innerHTML='<pre>&lt;html&gt;'+h.replace(/(\n|r)+/g,'\n')+&lt;/html&gt;</pre>';}void(disp(h));
```

Your computer may take a while to decode all the Java, just be patient.

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/>

I used to post a long list of abuse addresses in the alt.spam FAQ, but the abuse.net lookup is **much** better, in fact it is the way that I look up abuse addresses. Look up the abuse address of the ISP that you think the spammer is a customer:

<http://abuse.net/lookup.phtml>

There is a list of admins to contact:

<http://personalpages.tds.net/~slambo/spamreports.htm>

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.

From : David Jackson (djackson@aol.net) (and this applies to *any* abuse) :

To report an instance of USENET abuse send mail to tosusenet@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>

<http://www-personal.umich.edu/~jmm/papers.html#efi> - Economic FAQ about the Internet

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.

To contact the upstream providers first go to Merit Network Advanced WhoIs query and get their AS:

<http://www.radb.net/cgi-bin/radb/advanced-query.cgi>

It should look something like:

origin: AS15084

Then go to the CIDR report and get their upstreams (change the "AS15084" to something appropriate):

<http://www.cidr-report.org/cgi-bin/as-report?as=AS15084>

Or go to the following, scroll to the bottom and type in the AS:

<http://www.cidr-report.org/>

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. 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

Viruses / Trojans / Spyware

=====

If you do not have anti-virus software loaded on your computer *or* you do not have the latest and greatest virus definitions then run - do not walk - to the closest software store and buy the latest anti-virus software or download the latest definitions if you have the software and haven't updated the definitions lately.

There are several free antivirus programs available:

<http://www.google.com/search?q=Free+Anti-virus>

Like:

<http://free.grisoft.com/doc/1> - AVG

The grief you will have if you are infected with a virus is many times the grief of loading and maintaining anti-virus software.

More and more viruses propagate thru e-mail. If your friends machine is infected you can receive a virus from them because the virus sends a copy of itself to you (the virus send itself to everybody in your friends address book). DO NOT open attachments even if they are from someone you know unless you are ABSOLUTELY CERTAIN the attachment is virus free.

<http://www.incidents.org/react/avinfo.php> - Online scanning of your hard drive and reporting viruses

If you think that you have received a virus in an e-mail, there are some online scanning tools that will scan for the latest and greatest viruses:

<http://housecall.trendmicro.com/>

<http://www.commandondemand.com/>

<http://security1.norton.com/us/intro.asp?venid=sym&langid=us>

You can submit the virus to your choice in anti-virus vendors, please take a look at their site to see if they have any particular submission instructions:

"Command AntiVirus" virus@commandcom.com

http://www.commandcom.com/virus/think_you_have_a_virus.html

"Computer Associates" virus@cai.com

<http://www3.ca.com/virusinfo/>

"F-Secure" samples@F-Secure.com

"Kaspersky AntiVirus" newvirus@kaspersky.com

<http://www.avp.ru/>

"Network Associates" virus_research@nai.com

<http://www.mcafeeb2b.com/naicommon/avert/avert-research-center/submit-sample.asp>

"SARC" avsubmit@symantec.com

<http://www.sarc.com/avcenter/submit.html>

"Trend Micro" virus_doctor@trendmicro.com

<http://www.antivirus.com/vinfo/trendlabs/submit.htm>

A Trojan is a program that you are tricked into executing that has a devious purpose. You run a small game that (in reality) loads itself onto your computer to allow someone else to get into your computer. Most anti-virus programs *should* protect against this. See:

PestPatrol Glossary

<http://www.safersite.com/PestInfo/G/Glossary.asp>

PestPatrol White Paper: About RATs (Remote Admin Trojans)

http://www.safersite.com/Support/About/About_Rats.asp

http://www.pestpatrol.com/whitepapers/Comparison/Product_Details.asp

Also see "A Comparison of Pest Detecting Tools" at:

<http://www.pestpatrol.com/Whitepapers/Comparison/Index.asp>

Spyware is software that tracks what you do at your computer and reports that information via the Internet back to the company that wrote the software. Depending on how paranoid you are and how much you want companies to know what you are doing, you might wish to remove this software from your computer:

<http://grc.com/optout.htm>

Adware is software that loads itself on your computer usually without your specific permission and pops up advertisements while you are on your computer. Both spyware and adware are usually not well programmed and should be removed. This will make your computer run smoothly.

Scanning for Spyware:

<http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=4306576>

Spyware removal tools:

<http://www.securitypipeline.com/showArticle.jhtml?articleId=57702061>

To remove spyware / adware, see the below free tools. Try one at a time and see if it stops your problem:

1) Back up any important data (this *especially* applies before taking your computer into someone to "fix")

2) Run adaware:

<http://www.lavasoftusa.com/software/adaware/>

3) Run Spybot Search And Destroy:

<http://www.safer-networking.org/en/index.html>

4) Run Hijack This

<http://www.spywareinfo.com/~merijn/downloads.html>

5) Microsoft Spyware Removal (I haven't used this yet, so I don't know how well it works):

<http://www.microsoft.com/athome/security/spyware/software/default.msp>

There are companies spamming (and ostensibly making money) off of Trojan programs. They tell customers they can spy on children, spouses, employees, etc (which is, by the way, illegal in the USA and many countries):

"Spy on Anyone by sending them an Email-Greeting Card!

Spy Software records their emails, Hotmail, Yahoo, Outlook, ACTUAL Computer Passwords, Chats, Keystrokes, PLUS MORE."

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).

You must be **very** careful of **any** e-mail that you receive. If the e-mail is asking for any account and password there is a very good chance that this is a fraud. The current vernacular for this on the Internet is "Phishing". The fraud artist is trying to get you to divulge information to them that they should not know. Never click on a link that says anything about updating your account. There are ways that the links you click on "look" like they are pointing to a legitimate site but in reality are pointing to the fraud site that looks JUST LIKE the real site. If you are worried that your account may need updating, go to your browser and type in the site name by hand and then look at your account. See :

<http://www.computerworld.com/newsletter/0,4902,88583,00.html?nlid=SEC2>

Also see:

<http://www.computerworld.com/printthis/2004/0,4814,89096,00.html>

And Suing spammers for fraud:

<http://www.nwfusion.com/newsletters/sec/2004/0105sec2.html>

The Washington Post wrote three articles on victims of Phishing crimes:

<http://www.washingtonpost.com/ac2/wp-dyn/A59347-2004Nov18?language=printer>

<http://www.washingtonpost.com/ac2/wp-dyn/A59349-2004Nov18?language=printer>

<http://www.washingtonpost.com/ac2/wp-dyn/A61916-2004Nov19?language=printer>

Australian Financial Advisor give 419ers 1 Million:

http://www.theregister.co.uk/2004/10/19/aussie_419_victim

Anti-Phishing Working Group (<http://www.anti-phishing.org>) is a coalition of financial institutions, ISPs and online retailers. Visit their website for the latest Phishing scams that are trying to steal accounts, etc.

Many of the different organizations are creating pages to report fraud. For example CitiBank has a page:

http://www.citi.com/domain/spoof/report_abuse.htm

And USbank:

http://www.usbank.com/cgi_w/cfm/promo/personal/fraud_email_info_and_help.cfm

http://www.usbank.com/cgi_w/cfm/personal/achieve_goals/id_theft.cfm

Donna tells us If you would like to see a safe sample of this mischief visit:

<http://www.zaphedingbat.com/security/ex01/vun1.htm>

Examples of the e-mails that I have received that are fraud or viruses purport that they are from E-Bay, PayPal, Amazon, Earthlink, a multitude of banks and from Microsoft. An example of the URL (that looked like it was from Earthlink) and how it was decoded can be found at:

<http://home.digital.net/~gandalf/URLDecode.txt>

In addition some of these fraud artists are targeting technically unsophisticated office workers claiming they have control over the workers computer (when they really don't), or that they will get them in trouble by putting pornography on their computer unless they pay them :

<http://www.computerworld.com/newsletter/0,4902,88623,00.html?nlid=PM>

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.gcn.com/21_9/top-stories/18494-1.html - An article on what the FTC is doing to stop scams

<http://www.ftc.gov/bcp/online/edcams/dotcon/index.html> FTC Scam Page

http://www.infoworld.com/article/03/05/15/HNftcspammer_1.html - The FTC goes against spammers

<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,78551,00.html?SKC=cybercrime-78551> - Internet fraud is expanding. Spam has been sent out with fake sites that

"look" like real sites to steal credit card information, etc.

<http://www.acidics.com/> - How all the MMF, envelope stuffing, paid to surf, read e-mail, etc scams work. That is work for the con artists. You (of course) lose money.

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

National Criminal Justice Reference Service has a site on White Collar Crimes and what to do if you are a victim. Under More Issues:

<http://virlib.ncjrs.org/MoreIssues.asp>

Click on White Collar Crime:

<http://virlib.ncjrs.org/more.asp?category=51=152>

Virus updates, scams and hoaxes:

From Security Wire Digest (http://www.infosecuritymag.com/digest_intro.shtml)

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>

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/answers/pumpdump.htm> - Pump and Dump tips

<http://www.sec.gov/news/headlines/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 report to 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>.

Buying Medical Products Online - http://www.fda.gov/fdac/features/2000/100_online.html

Notifying FDA about problem Web Sites - <http://www.fda.gov/oc/buyonline/default.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/>

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

The applicable Canadian description can be found at :

http://www.rcmp-grc.gc.ca/scams/scams_e.htm

Specifically http://www.rcmp-grc.gc.ca/scams/pyramid_e.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 ...

Norway - Sylfest tells us Norwegians should report these via email to the national taskforce on economical crime, the KOKRIM by forwarding the mail with full headers to: <desken@okokrim.no >

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

<http://www.nwfusion.com/news/2002/0212antispam.html?net> - Federal Trade Commission is cracking down on illegal spam

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>

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 advantage of a security hole in your browser and done something nefarious. Bottom line, do not click on the spammers URL, look at the e-mail and complain to the upstream provider.

And just when you thought that the spammers had reached new lows you get a spam from Word-of-Mouth.Org or WordofMouthConnection.com or womc.net (as the scam gets reported I am sure they will continue to change their name). They purport:

"An acquaintance of your's recently shared their experience with you in our online community, Word-of-Mouth.Org. It could be a friend, a family member, co-worker, business associate, or someone else you have run into at some time.

Why are we sending you this email?

When people find out others are talking about them -- whether it is good or bad -- they want to know. At Word-of-Mouth.Org, we feel responsible to alert people so they have an opportunity to find out what is being said."

When you go to the site to find out what is being said, all you can find out for "free" is that your e-mail address is in their database. To find out exactly what is going on you have to "join" (and, of course, pay a fee). After you pay mysteriously your report cannot be found. See:

<http://groups.google.com/groups?q=word-of-mouth+scam>

(Look at the news.admin.net-abuse.email posts)

Also See:

<http://www.snopes.com/computer/internet/wordofmouth.asp>

And:

<http://www.nwfusion.com/newsletters/sec/2003/0901sec1.html>

Yet another fraud arrives via e-mail with a subject of "Pre Action Warning." addressed to "Dear Sir" (didn't even know my name). It specifically stated:

"I am writing to you in connection with you debt that you have with our company, Due to inflation and other factors outside of my control, your debts have exceeded \$1100.94 (one thousand one hundred and ninety four cents) I regret to inform you that we are pushing for legal action against your person. We will offer you the opportunity to pay your debt. within the next 7 business days, if you fail to comply, our partners, hold the right to litigate on behalf of our organization."

The E-Mail went on to state that I could send Banking details, Banking Authorization, etc. Even better it stated:

"CONFIDENTIALITY NOTICE: E-mail may contain confidential information that is legally privileged. Do not read this e-mail if you are not the intended recipient. This e-mail transmission, and any documents, files or previous e-mail messages attached to it may contain confidential and proprietary information that is legally privileged. If you are not the intended recipient, or a person responsible for delivering it to the intended recipient, you are hereby notified that any disclosure, copying, distribution or use of any of the information contained in or attached to this transmission is STRICTLY PROHIBITED."

These are all scare tactics trying to get you to give them money and not report this to someone else. I (of course) immediately complained to uce@ftc.gov and the two providers linked to this fraud (with the entire e-mail message and headers). You don't owe money; they just want to make you think so. When you get **any** e-mail that tells you to give someone money because they say you owe it, don't do it. Trust me, if they want the money bad enough they won't be using e-mail to collect.

Another fraud (Bad English and all) to try and get you to send the spammer your credit card purports: "We have just charged your credit card for money laundry service in amount of \$234.65 (because you are either child pornography webmaster or deal with dirty money, which require us to laundry them and then send to your checking account).

If you feel this transaction was made by our mistake, please press "No".

If you confirm this transaction, please press "Yes" and fill in the form below.

Enter your credit card number here:

Enter your credit card expiration date: "

As always be a cynic when receiving unsolicited e-mails. The frauds are getting more and more complex.

Nigerian Advance Fee Fraud

=====

Robert Heinlein has a saying "TANSTAAFL" (There Ain't No Such Thing As A Free Lunch). If it looks too good, it probably is.

There is a fraud promising you millions of dollars from a "government official" (or Widow, or son of a widow, etc.) in Nigeria (or some other small country) with a "secret" bank account, but all they need to transfer the money to you is:

(a)Your Company's 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).

This is the start of the Nigerian AFF (Advance Fee Fraud). A summary is that they ask for you to "help" pay some fees that are required to get the money out of the country, then they try to get you to go to Nigeria (or a bordering country) to meet.

At this point they try to get you into the country without a visa, promising that they will get you a visa. At that point they have you under their control since you are in Nigeria without a visa (no, they never got you a visa) and they start intimidation (physical or otherwise) trying to get money from you. According to the Department Of State in publication 10465 (release April 1997) "15 foreign businessmen (one American) have been murdered in Nigeria AFF scams".

The Advanced Fee Frauds can also take the form of:

- Disbursement of money from wills
- Contract fraud (C.O.D. of goods or services)
- Purchase of real estate
- Conversion of hard currency
- Transfer of funds from over invoiced contracts
- Sale of crude oil at below market prices

To see the details of this fraud:

<http://www.wired.com/news/culture/0,1284,53818,00.html> - Short Version - Meet the Nigerian E-Mail Grifters

<http://www.state.gov/documents/organization/2189.pdf> - The longer detailed version, Department Of State Publication 10465

Send scams to 419.fcd@ussf.treas.gov (Put No Monetary Loss in the header if you haven't lost any money)

Also see:

<http://www.secretservice.gov/alert419.shtml>

<http://www.fbi.gov/majcases/fraud/fraudschemes.htm>

<http://www.419legal.org/>

<http://www.computerworld.com/softwaretopics/software/story/0,10801,69562,00.html>

<http://www.nigerianfraudwatch.org/>

<http://home.rica.net/alphae/419coal/news1998.htm>

<http://home.rica.net/alphae/419coal/> - How to contact the US Gov't about this scheme

<http://www.scambusters.org/NigerianFee.html> - How the fraud works

<http://www.cbintel.com/nigeriafraud.htm>

<http://www.scamorama.com/> - The Nigerian Scammers - Can you scam a scammer?

<http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,80200,00.html?nas=AM-80200> - The Nigerian Fraud continues to claim victims

<http://www.nwfusion.com/newsletters/sec/2003/0224sec1.html> - Two more scams, one like Nigeria scam, one demanding money you don't owe

<http://www.nwfusion.com/newsletters/sec/2003/1013sec1.html> - M. E. Kabay talks about scams that allege you have won a lottery in Europe. M. E. Kabay mentions "its illegal for a U.S. resident to participate in a foreign lottery". Again, if it looks too good it probably is

Hoaxes

=====

Lat but certainly not least there are many hoaxes circulating around the internet. A hoax is the human version of a computer virus. Instead of convincing the computer to pass the message along to many other computers, the message is written to convince a human to send the message to many other humans. The cleverest hoax wins the prize. 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_1sd_faq.html

A complete Urban Legends listings (It is big) :

<http://www.urbanlegends.com/afu.faq/index.html>

Snopes offers a way to see if a photo is a hoax:

<http://www.snopes.com/photos/>

Some other hoax pages:

<http://www.pfir.org/statements/hoaxes> - Why hoaxes are damaging

<http://www.symantec.com/avcenter/hoax.html> - Symantec Hoax Page

<http://chekware.com/hoax/> - Scams and hoaxes page

<http://kumite.com/myths/myths>

<http://hoaxbusters.ciac.org/> - Hoaxes / Chain Letters

<http://www.snopes.com/inboxer/nothing/billgate.asp> - 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

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.

Open system spammers love

=====

FormMail is a free program used by many legitimate sites to glean data submitted via online forms. Last year, a vulnerability was discovered in the FormMail.pl gateway that allows external users to run the program. As a result, unsecured FormMail installations have become favored targets with junk emailers.

Many of the viruses circulating now leave "back doors" into the computers that they infect. Armed with the knowledge of the back door, spammers hijack the computer and use the hijacked computer to send out their spam.

Of course open SMTP servers are ALWAYS the computer of choice to blast a few million e-mails out with.

Bottom line, the owner of the computer is responsible for keeping their computer secure. Complain to the upstream provider about their customer and get the computer disconnected from the network until the problems can be corrected.

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://www.jsm-net.demon.co.uk/blackmail/blackmail.html> - Written by Ken Hollis (Not me ...) and

maintained by James Murray

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://www.impsec.org/email-tools/procmail-security.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 filter 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.

Columnist Al Fasoldt suggests a method for filtering your own e-mail:

<http://www.twcny.rr.com/technofile/texts/bit121901.html>

Rejecting E-Mail from domains that continue to Spam

=====
Spamfilter can be found at:

<http://www.samiam.org/spam/index.html>

See Sendmail site: <http://www.sendmail.org/>

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.

=====

Protection for you and your kids on the Internet

=====

The kids have learned the Internet first, and there is a good point made that the Internet may be the first "system" created where kids are teaching parents about ethical use of the Internet.

Learn about it yourself to help your kids use the Internet responsibly. When educating yourself, be **very** sure to read all privacy notices (or anti-privacy policies in this instance). Many of the online contests have "privacy" policies that (basically) say that they can sell any and all information that you submit to anybody that they feel like. That could include selling your e-mail address to spammers. Even when you make an online purchase, scrutinize the privacy policy. An example of a company who's privacy policy allows them to redistribute your information is Ticketmaster. See:

Ticketmaster's Privacy Policy: Opting Out is Not an Option

<http://www.gripe2ed.com/scoop/story/2003/7/24/84435/6284>

<http://www2.norwich.edu/mkabay/cyberwatch/index.htm> - Protecting yourself and your kids on the Internet, teaching your kids about ethical Internet Use

<http://www.ftc.gov/bcp/online/edcams/infosecurity/> - FTC generic information about keeping secure on the Internet. In addition there is a Childs quiz about being a safe cybersurfer.

A company "Alyon Technologies" installed a dialer on home computers and connected / charged the consumers for pornography calls even when they were away on vacation:

<http://www.channel3000.com/technology/2189632/detail.html>

http://www.cheycobb.com/comp_sec_advice.html - Computer security for non geeks

And her book:

<http://www.amazon.com/exec/obidos/ASIN/0764516795/102-0644946-4499357>

I am interested in eliminating spam from my emails, how do I do this?

=====

First off NEVER reply to the "Remove Me" e-mail addresses or sites. This only confirms that you have a live e-mail address and makes *your* e-mail address more valuable to sell to other spammers.

Start off by reading this spam FAQ.

It may take a while to digest all of the new information, but just read it and see what you can get out of it.

Start complaining to the ISP (Internet Service Provider) of where the spam came from. Understanding the "Received:" headers is key to this. Trace back in the Received: header to where it looks like the spam came from and complain to that provider about the spam.

Look in the body of the e-mail. If someone tells you to reply to back to a e-mail address or if they point you to a web site then complain to the ISP owner of that web site or e-mail address (NEVER complain to the spammer, they already know it is wrong and will ignore you).

These steps will help get the spammers accounts eliminated.

Will it stop you from getting spam? Probably not. If spammers have your e-mail address it is already too late. They are selling your address to each other, passing it around. About the only way to do that is to change your e-mail address and give it out to as few people as possible.

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.

The very first spam was on 2 May 1978 from Digital Equipment Corporation (DEC):

<http://www.templetons.com/brad/spamreact.html>

The different kinds of "spam":

spam – Unsolicited (Commercial Or Bulk) E-Mail

SPIM or spIM - IM Spam, Cell Phone SMS spam

SPIT - Spam over Internet Telephony

Geek cartoons, some anti-spam cartoons mixed in:

<http://www.userfriendly.org/cartoons/archives/> - Type "spam" and click "Submit Query"

<http://ars.userfriendly.org/cartoons/?id=19990226> - :-)

The Spammers Rules (and their lies):

<http://bruce.pennypacker.org/spamrules.html>

<http://groups.google.com/groups?q=Rules+of+Spam>

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]

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 100zer" 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://www.spamgift.com/>

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://www.spamhaiku.com/> - SPAM Haiku
<http://www.go2net.com/internet/useless/useless/spam.html>
<http://www.vivalasvegastamps.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://petemoss.com/spamflames/ShifmanIsAMoronSpammer.html>

Just keep the spammer in a conversation - <http://www.thespamletters.com/>

A Spammers Soliloquy. I had to keep this one because it was actually very creative (unexpected from a spammer) :

<http://digital.net/~gandalf/spammersoliloquy.html>

And if you cannot get enough Unsolicited Commercial E-Mail, you can listen to it coming from your speakers:

<http://spamradio.com/html/listen.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://gamesbyemail.com/Documentation/AntiSpamEmailLinks/> - Examples of disguising your e-mail.

<http://www.applelinks.com/articles/2001/07/20010730122944.shtml> - converting email addresses to "digital entities"

<http://www.inter-linked.com/content/spiderbait.php3> - A Java script to encode your e-mail address on a web page

Larry suggests making your e-mail address into a JPEG (picture). You can't click on it and send a e-mail, but the spammers can't harvest your e-mail address either.

Do Not ever reply to the "unsubscribe" option in a spam. That only confirms your e-mail as "real" and gets your e-mail address sold to others. More spam for you.

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>

Greg tells us of yet another clever trick. The spammer imbeds a unique image (Web Bug) in a spam e-mail so that just the act of opening the e-mail tells the spammer that your address is "live":

```
img src="http://209.73.247.130/cgi-bin/loadbalance/load.cgi?servers=clusters_1-9 &
image=39E218DC0DE2341934ED231E203E382D2193A7B975B23CA8EA-3.jpeg" border=0
```

I have seen yet another trick that spammers use, they make the URL a web bug. When you have a link like <http://NAIOKWDVDISY.adwarebde.com/?id=02025> the "name" of the web site NAIOKWDVDISY can uniquely identify what e-mail address that spam was sent to. Just doing a NSLookup of the name will point out the e-mail address of the person that the spam was sent to thus identifying a "live" person.

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.

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<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 <https://ssl.dizum.com/help/mail2news.html> for mail to news gateways.

A [HREF="mailto:news.admin.net-abuse.email@myriad.alias.net"/a](mailto:news.admin.net-abuse.email@myriad.alias.net)

Or

A [HREF="mailto:news.admin.net-abuse.misc@myriad.alias.net"/a](mailto:news.admin.net-abuse.misc@myriad.alias.net)

Or

A [HREF="mailto:news.admin.net-abuse.usenet@myriad.alias.net"/a](mailto:news.admin.net-abuse.usenet@myriad.alias.net)

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@\[127.0.0.1\]](mailto:root@[127.0.0.1]) with any of the following :

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](mailto`;cat /dev/zero /tmp/...;`@localhost)

`umount /tmp`@localhost

[;umount /tmp;`@localhost](mailto`;umount /tmp;`@localhost)

`halt`@localhost

[;halt;`@localhost](mailto`;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 definitively 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 warrant 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 follow-up 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 follow-up 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 canceled, or Chris Lewis is on vacation in the Seychelles Islands. If all three conditions are met, a follow-up 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 hackers out.

You have no excuse for not installing virus and firewall software on your computer. There is always someone out there offering free or low priced antivirus or firewall software. See <http://www.google.com/search?q=free+antivirus+firewall>

For example:

<http://www.my-etrust.com/microsoft/>

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 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://ntbugtraq.ntadvice.com/> - Click on the FAQ link and there is a link to a page with a very extensive list of firewalls.

<http://www.google.com/search?q=Personal+Firewall> - Google search for personal firewalls

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. ZoneAlarm by Zonelabs and 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 do to our quiet little corner of the Universe known as the Internet, Spam is not illegal worldwide (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, just search in Google. Jeff mentions that some people cross enter 800 numbers, phone numbers and addresses of spammers onto other spammers' sites. He says the least we can do is introduce like minded individuals to each other. Just being neighborly. ;-)

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://ag.state.nv.us/> - 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@ag.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?](http://sandgate.co.clark.nv.us:8498/servlet/BusinessLicense?instance=blotdetl&license_number=1000144-533)

[instance=blotdetl&license_number=1000144-533](http://sandgate.co.clark.nv.us:8498/servlet/BusinessLicense?instance=blotdetl&license_number=1000144-533)

And see if they are paying the correct taxes:

<http://tax.state.nv.us/>

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. Of course calling from a pay phone takes care of all of these problems :-) ...

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://www.infospace.com/info.zip/>

<http://www.bigbook.com/>

<http://www.switchboard.com/>

<http://decoder.americom.com/> - Look up location by area code.

http://www.nanpa.com/area_codes/index.html - North American Numbering Area Code Lookup

<http://www.aegisbooks.com/download.html> - Map of the Area Codes

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 in the U.S.

=====

<http://www.ftc.gov/bcp/online/pubs/tmarkg/nine.htm> - 1-900 explained

<http://www.ftc.gov/bcp/online/pubs/services/cramming.htm> - Mysterious Phone charges

http://www.theregister.co.uk/2004/09/22/ireland_rogue_dialler_crackdown - Long distance charges on your phone bill from your modem

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 in the United States. Ozzy tells us that in Canada, ALL 1-800, 866,877, & 888 numbers ARE toll free. In the U.S 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://docs.nanpa.com/cgi-bin/npa_reports/nanpa?function=list_npa_geo_number)

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/online/edcams/telemarketing/index.html> - Telemarketing information / scams

<http://www.ftc.gov/bcp/online/edcams/telemarketing/fileacomplaint.htm> File a complaint

http://www.infoworld.com/article/04/09/07/HNspamspit_1.html - Spam over Internet Telephony (SPIT)

Junk Mail - The Law

=====

<http://www.jmls.edu/cyber/index/spam.html> - Collection of legal spam items

<http://www.lectlaw.com/> - '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 organization, 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)

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 <http://groups.google.com/> 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>

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 clicking "All" and entering "17538" into:

<http://www.leginfo.ca.gov/calaw.html> (A pretty authoritative source) then click on "BUSINESS AND PROFESSIONS CODE"

Also see:

<http://www.netatty.com/spam.html> - Sue a California spammer

The Virginia law : <http://www.spamlaws.com/state/va.html>

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

=====

The latest & greatest version of the Spam FAQ is found at:

<http://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/>

<http://samspade.org/d/nanaefaq.html> - news.admin.net-abuse.email FAQ

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

<http://www.spamfaq.net/terminology.shtml> - spam terminology

<http://www.cm.org> for info on NoCeM

<http://www.killfile.org/faqs/spam.html>

Net abuse jargon:

<http://www.ncf.carleton.ca/ip/freenet/subs/complaints/spam/jargon.txt>

<http://groups.google.com/groups?selm=6tk5th%24497%40freenet-news.carleton.ca>

Software to track the headers / eliminate Spam for you :

<http://www.antisipam-software.net/> - Anti-Spam software for Outlook and AOL

<http://allmacintosh.forthnet.gr/macintosh.html> - Mac software

<http://samspade.org/> - Sam Spade WWW Spam tools - Excellent!

<http://www.spamulor.net/> - Software to identify / classify and funnel spam to a location out of your way

<http://www.exit109.com/~jeremy/news/cleanfeed.html>

<http://www.julianhaight.com/spamcop.shtml> - Spam Cop - Does the header analysis for you.

<http://www.netdemon.net/> - 30+ spam tools ...

<http://www.spamhippo.com/>

<http://www.spammerslammer.com> - Works with windows e-mail programs that uses pop mail

<http://www.vicomsoft.com/knowledge/reference/spam.html> - Vicomsoft document to raise awareness about Spam and offer practical solutions to email users

<http://www.vipul.net/ricochet/> - automated spam tracing and reporting agent

<http://andrew.triumf.ca/pub/security/> - UNIX Tools

Your Daily Spam News:

<http://www.spam-news.com>

<http://www.newsadmin.com/cgi-bin/newsspam1> - Top Spam Hosts

<http://www.newsadmin.com/cgi-bin/newsspam2> - Top Spam Sites

Spammers and how to stop them :

<http://abuse.sourceforge.net/> <http://spam.sourceforge.net/> - Anti-spam support site

http://livinginternet.com/e/et_spam.htm - a discussion on the origins of spam

<http://spamhaus.org> - spam havens listing

<http://lumbercartel.freeyellow.com/> - <http://www.cafeshops.com/tinlc> - TINLC - There Is No Lumber Cartel - CafeShops has the TINLC Tee-Shirt.

http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Email/

http://dir.yahoo.com/Computers_and_Internet/Communications_and_Networking/Email/Spam/

<http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,75737,00.html> - Spam wars

<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://www.jahitchcock.com/cyberstalked/> - Maryland Anti-Harassment bill

<http://morehouse.org/hin> - Internet Security

<http://persona.www.media.mit.edu/judith/Identity/IdentityDeception.html>

<http://www.cromwell-intl.com/security/> - Internet Security

<http://slashdot.org/articles/99/08/02/129213.shtml> - ISP sues spammer

<http://spam.abuse.net/spam/>

<http://viper.law.miami.edu/~froomkin/articles/oceanf.htm> Regulation of Computing and Information Technology

<http://www.atnewyork.com/news/article.php/1557541> - AOL wins against Spammers

<http://www.abuse.net/lookup.phtml> - Complaint lookup

<http://www.antonline.com/> - Internet Security

<http://www.cabal.net/jason/index.html> - A spammer tries to sue the Cabal (TINC)

<http://www.cabal.net/> - 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-1/> - Improve your spam-fighting skills

<http://www.claws-and-paws.com/spam-1/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://eioMAIL.com/> Spam free web- and POP3-based e-mail account for individual users

<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?!&igv&> - Spam link list

<http://www.nags.org/>

<http://groups.yahoo.com/group/anti-spam/join> - Anti-Spam mailing list

<http://www.petemoss.com/>

<http://fravia.anticrack.de/enemy.htm> - Stalking the spammer Enemy

<http://www.robertgraham.com/> - Infosec / computer security page

<http://spamsites.org> - Where spammers get their software

<http://ars.userfriendly.org/cartoons/?id=19990226> - 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.stopspam.org/email/headers/headers.html> - More Reading Headers

<http://www.usenet2.org/> - A Usenet with no Spam

http://www4.zdnet.com/anchordesk/story/story_index_19970819.html - Special Spam Fighting Edition

<http://crash.ihug.co.nz/~bryanc/> - Mac WhatRoute

<http://eddie.cis.uoguelph.ca/~tburgess/local/spam.html>

<http://members.aol.com/emailfaq/emailfaq.html>

<http://members.aol.com/emailfaq/resource-list.html>

<http://www.private.org.il/yanig.html> - Also yet another newbie guide

<http://groups.google.com/groups?selm=36811bc9.1386301459%40news.alt.net> - Forgery FAQ

<http://www.private.org.il/harvest.html> - 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://donotcall.gov/> - or call 1-888-382-1222 - Put yourself on the national "Do Not Call" list

<http://www.rahul.net/falk/index.html#howtos>

<http://www.river.com/users/share/cluetrain/> - My mailbox. My property. My personal space. My rules. Deal with it.

<http://www.spam-archive.org/> - A collection of email-Spams.

<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://member.nifty.ne.jp/usr/negi/news.html> - Japan

<http://member.nifty.ne.jp/usr/negi/newsgroup0.html> - Japan

<http://perso.magic.fr/roumazeilles/spamantf.htm> - Spam Anti! French

<http://portale.web.de/Internet/Spam/> - German Anti-Spam

<http://www.despaml.interrob.de/> - German Anti-Spam Mailing List

<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.snafu.de/~laura/de.admin.net-abuse.mail.txt> - German net abuse FAQ

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://digital.net/~gandalf/spamfaq.html>

English to German:

<http://translate.google.com/translate?hl=de&sl=en&u=http://digital.net/~gandalf/spamfaq.html>

English to Italian:

<http://translate.google.com/translate?hl=it&sl=en&u=http://digital.net/~gandalf/spamfaq.html>

English to Spanish:

<http://translate.google.com/translate?hl=es&sl=en&u=http://digital.net/~gandalf/spamfaq.html>

Or why Netabuse is bad :

<http://cnn.com/TECH/computing/9808/10/tastyspam.idg/>

<http://www.csoonline.com/alarmed/06192003.html> - Is someone watching everything you type?

<http://www.fraudbureau.com/articles/consumer/article14.html> - The cost of spam

<http://www.honet.com/Nadine/permission.htm> - Why permission is needed to send e-mail

<http://www.honet.com/Nadine/default.htm> - Someone types in a bad e-mail address and an innocent party starts getting spam

<http://www.honet.com/Nadine/Unsubscribe.htm> - Why Unsubscribe doesn't work

http://www.infoworld.com/article/03/03/14/11winman_1.html - Microsoft Update --> Watch what your computer sends out

http://www.infoworld.com/article/03/04/15/HNaolspammers_1.html - AOL takes spammers to court

http://www.infoworld.com/article/03/04/10/hnspamgov_1.html - US Government "Can spam" bill.

<http://www.nwfusion.com/news/2001/0104spamspace.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

<http://www.nwfusion.com/research/2002/0513spam.html> - How spam brings down servers

<http://www.nwfusion.com/research/2002/0513spamside4.html> - How spammers get your e-mail address

<http://www.nwfusion.com/newsletters/sec/2002/01331360.html> - Scumware, unauthorized software additions to your computer

<http://www.nwfusion.com/newsletters/sec/2002/01366115.html> - Scumware prevention and removal

<http://www.nwfusion.com/news/2003/0224spammers.html?net> - Spammers using students to send spam

<http://www.nwfusion.com/news/2003/0224spammerside.html> - Spam driving - Why wireless is bad

<http://www.nwfusion.com/news/2003/0227spamspam.html?net> - Corporate spam tools

<http://www.nwfusion.com/newsletters/sec/2003/0303sec2.html> - Security for those that aren't computer security geeks

<http://www.nwfusion.com/columnists/2003/0630backspin.html> - What spam really costs Part I

<http://www.nwfusion.com/columnists/2003/0707backspin.html> - What spam really costs Part II

<http://enterprisesecurity.symantec.com/content.cfm?articleID=1369> - The cost of Spam (at bottom of article) and how spammers are trying to fight back

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"

<http://www.nwfusion.com/news/2003/0415aolwield.html?net> - AOL wields legal, technical weapons in spam war

Spammers / Spyware Convictions:

<http://www.informationweek.com/shared/printableArticle.jhtml?articleID=52601698>

<http://australianit.news.com.au/articles/0,7204,11319598%5E15331%5E%5Enbv%5E15306%2D15318,00.html>

http://www.infoworld.com/article/04/10/08/HNftcspyware_1.html

<http://www.reuters.com/newsArticle.jhtml?storyID=6455433>

<http://www.computerworld.com/newsletter/0,4902,96528,00.html?nlid=PM>

<http://www.securityfocus.com/news/4217> - Spammers sending out Trojan Programs to turn home computers into spamming machines

<http://www.nwfusion.com/news/2005/0125spambust.html?net> - Spam busters go on the offensive

First register at: http://www.sensepost.com/garage_portal.html to look at: http://www.sensepost.com/restricted/ISSA2004_spam_paper.pdf - How Spammers Work

Listen to The Spam Avenger abuse spammers - <http://www.thespamavenger.com/>

Equal time, The spammer's viewpoint (Why Spam is good):

<http://www.juicycerebellum.com/spam.htm>

<http://listen.to/spammers> - Spammers Speak

<http://groups.google.com/groups?selm=7iviu5%2475g%241%40bgtnsc03.worldnet.att.net> - 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.freep.com/money/tech/mwend6_20021206.htm - Spammers don't like spam :-)

<http://www.marketing-2000.net/legal.htm> - Bulk E-Mail - Is It Legal? This page *used* to say "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.htm> - Bulk E-Mail Marketing guide

<http://www.marketing-2000.net/testimonials.htm> - 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>

And the Alt.Gothic Special Forces:

<http://thingy.apana.org.au/~fun/agsf/>

<http://www.izzy.net/~jfron/agsf/tools/>

AGSF FAQ:

<http://www.legendsmagazine.net/pan/panstuff/agsffaq.htm>

Disclaimer :

I am not a lawyer and this is not legal advice. For legal advice, consult an attorney with appropriate expertise in this area of the law who is licensed to practice in your jurisdiction.

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://gandalf.home.digital.net/>

Trace E-Mail forgery - <http://gandalf.home.digital.net/spamfaq.html>

Trolls crossposts - <http://gandalf.home.digital.net/trollfaq.html>