

Network Working Group
Request For Comments: 1855
FYI: 28
Category: Informational

S. Hambridge
Intel Corp.
October 1995

Netiquette Guidelines

Status of This Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Abstract

This document provides a minimum set of guidelines for Network Etiquette (Netiquette) which organizations may take and adapt for their own use. As such, it is deliberately written in a bulleted format to make adaptation easier and to make any particular item easy (or easier) to find. It also functions as a minimum set of guidelines for individuals, both users and administrators. This memo is the product of the Responsible Use of the Network (RUN) Working Group of the IETF.

Table of Contents

1.0 Introduction	1
2.0 One-to-One Communication	2
3.0 One-to-Many Communication	7
4.0 Information Services	14
5.0 Selected Bibliography	18
6.0 Security Considerations	21
7.0 Author's Address	21

1.0 Introduction

In the past, the population of people using the Internet had "grown up" with the Internet, were technically minded, and understood the nature of the transport and the protocols. Today, the community of Internet users includes people who are new to the environment. These "Newbies" are unfamiliar with the culture and don't need to know about transport and protocols. In order to bring these new users into the Internet culture quickly, this Guide offers a minimum set of behaviors which organizations and individuals may take and adapt for their own use. Individuals should be aware that no matter who supplies their Internet access, be it an Internet Service Provider through a private account, or a student account at a University, or

an account through a corporation, that those organizations have regulations about ownership of mail and files, about what is proper to post or send, and how to present yourself. Be sure to check with the local authority for specific guidelines.

We've organized this material into three sections: One-to-one communication, which includes mail and talk; One-to-many communications, which includes mailing lists and NetNews; and Information Services, which includes ftp, WWW, Wais, Gopher, MUDs and MOOs. Finally, we have a Selected Bibliography, which may be used for reference.

2.0 One-to-One Communication (electronic mail, talk)

We define one-to-one communications as those in which a person is communicating with another person as if face-to-face: a dialog. In general, rules of common courtesy for interaction with people should be in force for any situation and on the Internet it's doubly important where, for example, body language and tone of voice must be inferred. For more information on Netiquette for communicating via electronic mail and talk, check references [1,23,25,27] in the Selected Bibliography.

2.1 User Guidelines

2.1.1 For mail:

- Unless you have your own Internet access through an Internet provider, be sure to check with your employer about ownership of electronic mail. Laws about the ownership of electronic mail vary from place to place.
- Unless you are using an encryption device (hardware or software), you should assume that mail on the Internet is not secure. Never put in a mail message anything you would not put on a postcard.
- Respect the copyright on material that you reproduce. Almost every country has copyright laws.
- If you are forwarding or re-posting a message you've received, do not change the wording. If the message was a personal message to you and you are re-posting to a group, you should ask permission first. You may shorten the message and quote only relevant parts, but be sure you give proper attribution.
- Never send chain letters via electronic mail. Chain letters are forbidden on the Internet. Your network privileges will be revoked. Notify your local system administrator

if your ever receive one.

- A good rule of thumb: Be conservative in what you send and liberal in what you receive. You should not send heated messages (we call these "flames") even if you are provoked. On the other hand, you shouldn't be surprised if you get flamed and it's prudent not to respond to flames.
- In general, it's a good idea to at least check all your mail subjects before responding to a message. Sometimes a person who asks you for help (or clarification) will send another message which effectively says "Never Mind". Also make sure that any message you respond to was directed to you. You might be cc:ed rather than the primary recipient.
- Make things easy for the recipient. Many mailers strip header information which includes your return address. In order to ensure that people know who you are, be sure to include a line or two at the end of your message with contact information. You can create this file ahead of time and add it to the end of your messages. (Some mailers do this automatically.) In Internet parlance, this is known as a ".sig" or "signature" file. Your .sig file takes the place of your business card. (And you can have more than one to apply in different circumstances.)
- Be careful when addressing mail. There are addresses which may go to a group but the address looks like it is just one person. Know to whom you are sending.
- Watch cc's when replying. Don't continue to include people if the messages have become a 2-way conversation.
- In general, most people who use the Internet don't have time to answer general questions about the Internet and its workings. Don't send unsolicited mail asking for information to people whose names you might have seen in RFCs or on mailing lists.
- Remember that people with whom you communicate are located across the globe. If you send a message to which you want an immediate response, the person receiving it might be at home asleep when it arrives. Give them a chance to wake up, come to work, and login before assuming the mail didn't arrive or that they don't care.
- Verify all addresses before initiating long or personal discourse. It's also a good practice to include the word "Long" in the subject header so the recipient knows the message will take time to read and respond to. Over 100 lines is considered "long".

- Know whom to contact for help. Usually you will have resources close at hand. Check locally for people who can help you with software and system problems. Also, know whom to go to if you receive anything questionable or illegal. Most sites also have "Postmaster" aliased to a knowledgeable user, so you can send mail to this address to get help with mail.
- Remember that the recipient is a human being whose culture, language, and humor have different points of reference from your own. Remember that date formats, measurements, and idioms may not travel well. Be especially careful with sarcasm.
- Use mixed case. UPPER CASE LOOKS AS IF YOU'RE SHOUTING.
- Use symbols for emphasis. That **is** what I meant. Use underscores for underlining. _War and Peace_ is my favorite book.
- Use smileys to indicate tone of voice, but use them sparingly. :-) is an example of a smiley (Look sideways). Don't assume that the inclusion of a smiley will make the recipient happy with what you say or wipe out an otherwise insulting comment.
- Wait overnight to send emotional responses to messages. If you have really strong feelings about a subject, indicate it via FLAME ON/OFF enclosures. For example:
FLAME ON: This type of argument is not worth the bandwidth it takes to send it. It's illogical and poorly reasoned. The rest of the world agrees with me.
FLAME OFF
- Do not include control characters or non-ASCII attachments in messages unless they are MIME attachments or unless your mailer encodes these. If you send encoded messages make sure the recipient can decode them.
- Be brief without being overly terse. When replying to a message, include enough original material to be understood but no more. It is extremely bad form to simply reply to a message by including all the previous message: edit out all the irrelevant material.
- Limit line length to fewer than 65 characters and end a line with a carriage return.
- Mail should have a subject heading which reflects the content of the message.

- If you include a signature keep it short. Rule of thumb is no longer than 4 lines. Remember that many people pay for connectivity by the minute, and the longer your message is, the more they pay.
- Just as mail (today) may not be private, mail (and news) are (today) subject to forgery and spoofing of various degrees of detectability. Apply common sense "reality checks" before assuming a message is valid.
- If you think the importance of a message justifies it, immediately reply briefly to an e-mail message to let the sender know you got it, even if you will send a longer reply later.
- "Reasonable" expectations for conduct via e-mail depend on your relationship to a person and the context of the communication. Norms learned in a particular e-mail environment may not apply in general to your e-mail communication with people across the Internet. Be careful with slang or local acronyms.
- The cost of delivering an e-mail message is, on the average, paid about equally by the sender and the recipient (or their organizations). This is unlike other media such as physical mail, telephone, TV, or radio. Sending someone mail may also cost them in other specific ways like network bandwidth, disk space or CPU usage. This is a fundamental economic reason why unsolicited e-mail advertising is unwelcome (and is forbidden in many contexts).
- Know how large a message you are sending. Including large files such as Postscript files or programs may make your message so large that it cannot be delivered or at least consumes excessive resources. A good rule of thumb would be not to send a file larger than 50 Kilobytes. Consider file transfer as an alternative, or cutting the file into smaller chunks and sending each as a separate message.
- Don't send large amounts of unsolicited information to people.
- If your mail system allows you to forward mail, beware the dreaded forwarding loop. Be sure you haven't set up forwarding on several hosts so that a message sent to you gets into an endless loop from one computer to the next to the next.

2.1.2 For talk:

Talk is a set of protocols which allow two people to have an interactive dialogue via computer.

- Use mixed case and proper punctuation, as though you were typing a letter or sending mail.
- Don't run off the end of a line and simply let the terminal wrap; use a Carriage Return (CR) at the end of the line. Also, don't assume your screen size is the same as everyone else's. A good rule of thumb is to write out no more than 70 characters, and no more than 12 lines (since you're using a split screen).
- Leave some margin; don't write to the edge of the screen.
- Use two CRs to indicate that you are done and the other person may start typing. (blank line).
- Always say goodbye, or some other farewell, and wait to see a farewell from the other person before killing the session. This is especially important when you are communicating with someone a long way away. Remember that your communication relies on both bandwidth (the size of the pipe) and latency (the speed of light).
- Remember that talk is an interruption to the other person. Only use as appropriate. And never talk to strangers.
- The reasons for not getting a reply are many. Don't assume that everything is working correctly. Not all versions of talk are compatible.
- If left on its own, talk re-rings the recipient. Let it ring one or two times, then kill it.
- If a person doesn't respond you might try another tty. Use finger to determine which are open. If the person still doesn't respond, do not continue to send.
- Talk shows your typing ability. If you type slowly and make mistakes when typing it is often not worth the time of trying to correct, as the other person can usually see what you meant.
- Be careful if you have more than one talk session going!

2.2 Administrator Issues

- Be sure you have established written guidelines for dealing with situations especially illegal, improper, or forged traffic.
- Handle requests in a timely fashion - by the next business day.
- Respond promptly to people who have concerns about receiving improper or illegal messages. Requests concerning chain letters should be handled immediately.
- Explain any system rules, such as disk quotas, to your users. Make sure they understand implications of requesting files by mail such as: Filling up disks; running up phone bills, delaying mail, etc.
- Make sure you have "Postmaster" aliased. Make sure you have "Root" aliased. Make sure someone reads that mail.
- Investigate complaints about your users with an open mind. Remember that addresses may be forged and spoofed.

3.0 One-to-Many Communication (Mailing Lists, NetNews)

Any time you engage in One-to-Many communications, all the rules for mail should also apply. After all, communicating with many people via one mail message or post is quite analogous to communicating with one person with the exception of possibly offending a great many more people than in one-to-one communication. Therefore, it's quite important to know as much as you can about the audience of your message.

3.1 User Guidelines

3.1.1 General Guidelines for mailing lists and NetNews

- Read both mailing lists and newsgroups for one to two months before you post anything. This helps you to get an understanding of the culture of the group.
- Do not blame the system administrator for the behavior of the system users.
- Consider that a large audience will see your posts. That may include your present or your next boss. Take care in what you write. Remember too, that mailing lists and Newsgroups are frequently archived, and that your words may be

stored for a very long time in a place to which many people have access.

- Assume that individuals speak for themselves, and what they say does not represent their organization (unless stated explicitly).
- Remember that both mail and news take system resources. Pay attention to any specific rules covering their uses your organization may have.
- Messages and articles should be brief and to the point. Don't wander off-topic, don't ramble and don't send mail or post messages solely to point out other people's errors in typing or spelling. These, more than any other behavior, mark you as an immature beginner.
- Subject lines should follow the conventions of the group.
- Forgeries and spoofing are not approved behavior.
- Advertising is welcomed on some lists and Newsgroups, and abhorred on others! This is another example of knowing your audience before you post. Unsolicited advertising which is completely off-topic will most certainly guarantee that you get a lot of hate mail.
- If you are sending a reply to a message or a posting be sure you summarize the original at the top of the message, or include just enough text of the original to give a context. This will make sure readers understand when they start to read your response. Since NetNews, especially, is proliferated by distributing the postings from one host to another, it is possible to see a response to a message before seeing the original. Giving context helps everyone. But do not include the entire original!
- Again, be sure to have a signature which you attach to your message. This will guarantee that any peculiarities of mailers or newsreaders which strip header information will not delete the only reference in the message of how people may reach you.
- Be careful when you reply to messages or postings. Frequently replies are sent back to the address which originated the post - which in many cases is the address of a list or group! You may accidentally send a personal response to a great many people, embarrassing all involved. It's best to type in the address instead of relying on "reply."

- Delivery receipts, non-delivery notices, and vacation programs are neither totally standardized nor totally reliable across the range of systems connected to Internet mail. They are invasive when sent to mailing lists, and some people consider delivery receipts an invasion of privacy. In short, do not use them.
- If you find a personal message has gone to a list or group, send an apology to the person and to the group.
- If you should find yourself in a disagreement with one person, make your responses to each other via mail rather than continue to send messages to the list or the group. If you are debating a point on which the group might have some interest, you may summarize for them later.
- Don't get involved in flame wars. Neither post nor respond to incendiary material.
- Avoid sending messages or posting articles which are no more than gratuitous replies to replies.
- Be careful with monospacing fonts and diagrams. These will display differently on different systems, and with different mailers on the same system.
- There are Newsgroups and Mailing Lists which discuss topics of wide varieties of interests. These represent a diversity of lifestyles, religions, and cultures. Posting articles or sending messages to a group whose point of view is offensive to you simply to tell them they are offensive is not acceptable. Sexually and racially harassing messages may also have legal implications. There is software available to filter items you might find objectionable.

3.1.2 Mailing List Guidelines

There are several ways to find information about what mailing lists exist on the Internet and how to join them. Make sure you understand your organization's policy about joining these lists and posting to them. In general it is always better to check local resources first before trying to find information via the Internet. Nevertheless, there are a set of files posted periodically to news.answers which list the Internet mailing lists and how to subscribe to them. This is an invaluable resource for finding lists on any topic. See also references [9,13,15] in the Selected Bibliography.

- Send subscribe and unsubscribe messages to the appropriate address. Although some mailing list software is smart enough

to catch these, not all can ferret these out. It is your responsibility to learn how the lists work, and to send the correct mail to the correct place. Although many many mailing lists adhere to the convention of having a "-request" alias for sending subscribe and unsubscribe messages, not all do. Be sure you know the conventions used by the lists to which you subscribe.

- Save the subscription messages for any lists you join. These usually tell you how to unsubscribe as well.
- In general, it's not possible to retrieve messages once you have sent them. Even your system administrator will not be able to get a message back once you have sent it. This means you must make sure you really want the message to go as you have written it.
- The auto-reply feature of many mailers is useful for in-house communication, but quite annoying when sent to entire mailing lists. Examine "Reply-To" addresses when replying to messages from lists. Most auto-replies will go to all members of the list.
- Don't send large files to mailing lists when Uniform Resource Locators (URLs) or pointers to ftp-able versions will do. If you want to send it as multiple files, be sure to follow the culture of the group. If you don't know what that is, ask.
- Consider unsubscribing or setting a "nomail" option (when it's available) when you cannot check your mail for an extended period.
- When sending a message to more than one mailing list, especially if the lists are closely related, apologize for cross-posting.
- If you ask a question, be sure to post a summary. When doing so, truly summarize rather than send a cumulation of the messages you receive.
- Some mailing lists are private. Do not send mail to these lists uninvited. Do not report mail from these lists to a wider audience.
- If you are caught in an argument, keep the discussion focused on issues rather than the personalities involved.

3.1.3 NetNews Guidelines

NetNews is a globally distributed system which allows people to communicate on topics of specific interest. It is divided into hierarchies, with the major divisions being: sci - science related discussions; comp - computer related discussions; news - for discussions which center around NetNews itself; rec - recreational activities; soc - social issues; talk - long-winded never-ending discussions; biz - business related postings; and alt - the alternate hierarchy. Alt is so named because creating an alt group does not go through the same process as creating a group in the other parts of the hierarchy. There are also regional hierarchies, hierarchies which are widely distributed such as Bionet, and your place of business may have its own groups as well. Recently, a "humanities" hierarchy was added, and as time goes on its likely more will be added. For longer discussions on News see references [2,8,22,23] in the Selected Bibliography.

- In NetNews parlance, "Posting" refers to posting a new article to a group, or responding to a post someone else has posted. "Cross-Posting" refers to posting a message to more than one group. If you introduce Cross-Posting to a group, or if you direct "Followup-To:" in the header of your posting, warn readers! Readers will usually assume that the message was posted to a specific group and that followups will go to that group. Headers change this behavior.
- Read all of a discussion in progress (we call this a thread) before posting replies. Avoid posting "Me Too" messages, where content is limited to agreement with previous posts. Content of a follow-up post should exceed quoted content.
- Send mail when an answer to a question is for one person only. Remember that News has global distribution and the whole world probably is NOT interested in a personal response. However, don't hesitate to post when something will be of general interest to the Newsgroup participants.
- Check the "Distribution" section of the header, but don't depend on it. Due to the complex method by which News is delivered, Distribution headers are unreliable. But, if you are posting something which will be of interest to a limited number of readers, use a distribution line that attempts to limit the distribution of your article to those people. For example, set the Distribution to be "nj" if you are posting an article that will be of interest only to New Jersey readers.

- If you feel an article will be of interest to more than one Newsgroup, be sure to CROSSPOST the article rather than individually post it to those groups. In general, probably only five-to-six groups will have similar enough interests to warrant this.
- Consider using Reference sources (Computer Manuals, Newspapers, help files) before posting a question. Asking a Newsgroup where answers are readily available elsewhere generates grumpy "RTFM" (read the fine manual - although a more vulgar meaning of the word beginning with "f" is usually implied) messages.
- Although there are Newsgroups which welcome advertising, in general it is considered nothing less than criminal to advertise off-topic products. Sending an advertisement to each and every group will pretty much guarantee your loss of connectivity.
- If you discover an error in your post, cancel it as soon as possible.
- DO NOT attempt to cancel any articles but your own. Contact your administrator if you don't know how to cancel your post, or if some other post, such as a chain letter, needs canceling.
- If you've posted something and don't see it immediately, don't assume it's failed and re-post it.
- Some groups permit (and some welcome) posts which in other circumstances would be considered to be in questionable taste. Still, there is no guarantee that all people reading the group will appreciate the material as much as you do. Use the Rotate utility (which rotates all the characters in your post by 13 positions in the alphabet) to avoid giving offense. The Rot13 utility for Unix is an example.
- In groups which discuss movies or books it is considered essential to mark posts which disclose significant content as "Spoilers". Put this word in your Subject: line. You may add blank lines to the beginning of your post to keep content out of sight, or you may Rotate it.
- Forging of news articles is generally censured. You can protect yourself from forgeries by using software which generates a manipulation detection "fingerprint", such as PGP (in the US).
- Postings via anonymous servers are accepted in some Newsgroups and disliked in others. Material which is inappropriate when posted under one's own name is still inappropriate when posted

anonymously.

- Expect a slight delay in seeing your post when posting to a moderated group. The moderator may change your subject line to have your post conform to a particular thread.
- Don't get involved in flame wars. Neither post nor respond to incendiary material.

3.2 Administrator Guidelines

3.2.1 General Issues

- Clarify any policies your site has regarding its subscription to NetNews groups and about subscribing to mailing lists.
- Clarify any policies your site has about posting to NetNews groups or to mailing lists, including use of disclaimers in .sigs.
- Clarify and publicize archive policy. (How long are articles kept?)
- Investigate accusations about your users promptly and with an open mind.
- Be sure to monitor the health of your system.
- Consider how long to archive system logs, and publicize your policy on logging.

3.2.2 Mailing Lists

- Keep mailing lists up to date to avoid the "bouncing mail" problem.
- Help list owners when problems arise.
- Inform list owners of any maintenance windows or planned downtime.
- Be sure to have "-request" aliases for list subscription and administration.
- Make sure all mail gateways operate smoothly.

3.2.3. NetNews

- Publicize the nature of the feed you receive. If you do not get a full feed, people may want to know why not.

- Be aware that the multiplicity of News Reader clients may cause the News Server being blamed for problems in the clients.
- Honor requests from users immediately if they request cancellation of their own posts or invalid posts, such as chain letters.
- Have "Usenet", "Netnews" and "News" aliased and make sure someone reads the mail.

3.3 Moderator Guidelines

3.3.1 General Guidelines

- Make sure your Frequently Asked Questions (FAQ) is posted at regular intervals. Include your guidelines for articles/messages. If you are not the FAQ maintainer, make sure they do so.
- Make sure you maintain a good welcome message, which contains subscribe and unsubscribe information.
- Newsgroups should have their charter/guidelines posted regularly.
- Keep mailing lists and Newsgroups up to date. Post messages in a timely fashion. Designate a substitute when you go on vacation or out of town.

4.0 Information Services (Gopher, Wais, WWW, ftp, telnet)

In recent Internet history, the 'Net has exploded with new and varied Information services. Gopher, Wais, World Wide Web (WWW), Multi-User Dimensions (MUDs) Multi-User Dimensions which are Object Oriented (MOOs) are a few of these new areas. Although the ability to find information is exploding, "Caveat Emptor" remains constant. For more information on these services, check references [14,28] in the Selected Bibliography.

4.1 User Guidelines

4.1.1. General guidelines

- Remember that all these services belong to someone else. The people who pay the bills get to make the rules governing usage. Information may be free - or it may not be! Be sure you check.
- If you have problems with any form of information service, start problem solving by checking locally: Check file configurations, software setup, network connections, etc. Do this before assuming

the problem is at the provider's end and/or is the provider's fault.

- Although there are naming conventions for file-types used, don't depend on these file naming conventions to be enforced. For example, a ".doc" file is not always a Word file.
- Information services also use conventions, such as www.xyz.com. While it is useful to know these conventions, again, don't necessarily rely on them.
- Know how file names work on your own system.
- Be aware of conventions used for providing information during sessions. FTP sites usually have files named README in a top level directory which have information about the files available. But, don't assume that these files are necessarily up-to-date and/or accurate.
- Do NOT assume that ANY information you find is up-to-date and/or accurate. Remember that new technologies allow just about anyone to be a publisher, but not all people have discovered the responsibilities which accompany publishing.
- Remember that unless you are sure that security and authentication technology is in use, that any information you submit to a system is being transmitted over the Internet "in the clear", with no protection from "sniffers" or forgers.
- Since the Internet spans the globe, remember that Information Services might reflect culture and life-style markedly different from your own community. Materials you find offensive may originate in a geography which finds them acceptable. Keep an open mind.
- When wanting information from a popular server, be sure to use a mirror server that's close if a list is provided.
- Do not use someone else's FTP site to deposit materials you wish other people to pick up. This is called "dumping" and is not generally acceptable behavior.
- When you have trouble with a site and ask for help, be sure to provide as much information as possible in order to help debug the problem.

- When bringing up your own information service, such as a homepage, be sure to check with your local system administrator to find what the local guidelines are in affect.
- Consider spreading out the system load on popular sites by avoiding "rush hour" and logging in during off-peak times.

4.1.2 Real Time Interactive Services Guidelines (MUDs MOOs IRC)

- As in other environments, it is wise to "listen" first to get to know the culture of the group.
- It's not necessary to greet everyone on a channel or room personally. Usually one "Hello" or the equivalent is enough. Using the automation features of your client to greet people is not acceptable behavior.
- Warn the participants if you intend to ship large quantities of information. If all consent to receiving it, you may send, but sending unwanted information without a warning is considered bad form just as it is in mail.
- Don't assume that people who you don't know will want to talk to you. If you feel compelled to send private messages to people you don't know, then be willing to accept gracefully the fact that they might be busy or simply not want to chat with you.
- Respect the guidelines of the group. Look for introductory materials for the group. These may be on a related ftp site.
- Don't badger other users for personal information such as sex, age, or location. After you have built an acquaintance with another user, these questions may be more appropriate, but many people hesitate to give this information to people with whom they are not familiar.
- If a user is using a nickname alias or pseudonym, respect that user's desire for anonymity. Even if you and that person are close friends, it is more courteous to use his nickname. Do not use that person's real name online without permission.

4.2 Administrator Guidelines

4.2.1 General Guidelines

- Make clear what's available for copying and what is not.
- Describe what's available on your site, and your organization. Be sure any general policies are clear.
- Keep information, especially READMEs, up-to-date. Provide READMEs in plain ascii text.
- Present a list of mirrors of your site if you know them. Make sure you include a statement of copyright applicable to your mirrors. List their update schedule if possible.
- Make sure that popular (and massive) information has the bandwidth to support it.
- Use conventions for file extensions - .txt for ascii text; .html or .htm for HTML; .ps for Postscript; .pdf for Portable Document Format; .sgml or .sgm for SGML; .exe for non-Unix executables, etc.
- For files being transferred, try to make filenames unique in the first eight characters.
- When providing information, make sure your site has something unique to offer. Avoid bringing up an information service which simply points to other services on the Internet.
- Don't point to other sites without asking first.
- Remember that setting up an information service is more than just design and implementation. It's also maintenance.
- Make sure your posted materials are appropriate for the supporting organization.
- Test applications with a variety of tools. Don't assume everything works if you've tested with only one client. Also, assume the low end of technology for clients and don't create applications which can only be used by Graphical User Interfaces.
- Have a consistent view of your information. Make sure the look and feel stays the same throughout your applications.

- Be sensitive to the longevity of your information. Be sure to date time-sensitive materials, and be vigilant about keeping this information well maintained.
- Export restrictions vary from country to country. Be sure you understand the implications of export restrictions when you post.
- Tell users what you plan to do with any information you collect, such as WWW feedback. You need to warn people if you plan to publish any of their statements, even passively by just making it available to other users.
- Make sure your policy on user information services, such as homepages, is well known.

5.0 Selected Bibliography

This bibliography was used to gather most of the information in the sections above as well as for general reference. Items not specifically found in these works were gathered from the IETF-RUN Working Group's experience.

- [1] Angell, D., and B. Heslop, "The Elements of E-mail Style", New York: Addison-Wesley, 1994.
- [2] "Answers to Frequently Asked Questions about Usenet"
Original author: jerry@eagle.UUCP (Jerry Schwarz)
Maintained by: netannounce@deshaw.com (Mark Moraes)
Archive-name: usenet-faq/part1
- [3] Cerf, V., "Guidelines for Conduct on and Use of Internet", at: <URL://http://www.isoc.org/proceedings/conduct/cerf-Aug-draft.html>
- [4] Dern, D., "The Internet Guide for New Users", New York: McGraw-Hill, 1994.
- [5] "Emily Postnews Answers Your Questions on Netiquette"
Original author: brad@looking.on.ca (Brad Templeton)
Maintained by: netannounce@deshaw.com (Mark Moraes)
Archive-name: emily-postnews/part1
- [6] Gaffin, A., "Everybody's Guide to the Internet", Cambridge, Mass., MIT Press, 1994.

- [7] "Guidelines for Responsible Use of the Internet" from the US house of Representatives gopher, at: <URL:gopher://gopher.house.gov:70/OF-1%3a208%3aInternet%20Etiquette>
- [8] How to find the right place to post (FAQ) by buglady@bronze.lcs.mit.edu (Aliza R. Panitz) Archive-name: finding-groups/general
- [9] Hambridge, S., and J. Sedayao, "Horses and Barn Doors: Evolution of Corporate Guidelines for Internet Usage", LISA VII, Usenix, November 1-5, 1993, pp. 9-16. <URL: ftp://ftp.intel.com/pub/papers/horses.ps or horses.ascii>
- [10] Heslop, B., and D. Angell, "The Instant Internet guide : Hands-on Global Networking", Reading, Mass., Addison-Wesley, 1994.
- [11] Horwitz, S., "Internet Etiquette Tips", <ftp://ftp.temple.edu/pub/info/help-net/netiquette.infohn>
- [12] Internet Activities Board, "Ethics and the Internet", RFC 1087, IAB, January 1989. <URL: ftp://ds.internic.net/rfc/rfc1087.txt>
- [13] Kehoe, B., "Zen and the Art of the Internet: A Beginner's Guide", Netiquette information is spread through the chapters of this work. 3rd ed. Englewood Cliffs, NJ., Prentice-Hall, 1994.
- [14] Kochmer, J., "Internet Passport: NorthWestNet's Guide to our World Online", 4th ed. Bellevue, Wash., NorthWestNet, Northwest Academic Computing Consortium, 1993.
- [15] Krol, Ed, "The Whole Internet: User's Guide and Catalog", Sebastopol, CA, O'Reilly & Associates, 1992.
- [16] Lane, E. and C. Summerhill, "Internet Primer for Information Professionals: a basic guide to Internet networking technology", Westport, CT, Meckler, 1993.
- [17] LaQuey, T., and J. Ryer, "The Internet Companion", Chapter 3 "Communicating with People", pp 41-74. Reading, MA, Addison-Wesley, 1993.

- [18] Mandel, T., "Surfing the Wild Internet", SRI International Business Intelligence Program, Scan No. 2109. March, 1993.
<URL: gopher://gopher.well.sf.ca.us:70/00/Communications/surf-wild>
- [19] Martin, J., "There's Gold in them thar Networks! or Searching for Treasure in all the Wrong Places", FYI 10, RFC 1402, January 1993. <URL: ftp://ds.internic.net/rfc/rfc1402.txt>
- [20] Pioch, N., "A Short IRC Primer", Text conversion by Owe Rasmussen. Edition 1.1b, February 28, 1993.
<URL: http://www.kei.com/irc/IRCprimer1.1.txt>
- [21] Polly, J., "Surfing the Internet: an Introduction", Version 2.0.3. Revised May 15, 1993.
<URL: gopher://nysernet.org:70/00/ftp%20archives/pub/resources/guides/surfing.2.0.3.txt>
<URL: ftp://ftp.nysernet.org/pub/resources/guides/surfing.2.0.3.txt>
- [22] "A Primer on How to Work With the Usenet Community"
Original author: chuq@apple.com (Chuq Von Rospach)
Maintained by: netannounce@deshaw.com (Mark Moraes)
Archive-name: usenet-primer/part1
- [23] Rinaldi, A., "The Net: User Guidelines and Netiquette", September 3, 1992.
<URL: http://www.fau.edu/rinaldi/net/index.htm>
- [24] "Rules for posting to Usenet"
Original author: spaf@cs.purdue.edu (Gene Spafford)
Maintained by: netannounce@deshaw.com (Mark Moraes)
Archive-name: posting-rules/part1
- [25] Shea, V., "Netiquette", San Francisco: Albion Books, 1994?.
- [26] Strangelove, M., with A. Bosley, "How to Advertise on the Internet", ISSN 1201-0758.
- [27] Tenant, R., "Internet Basics", ERIC Clearinghouse of Information Resources, EDO-IR-92-7. September, 1992.
<URL: gopher://nic.merit.edu:7043/00/introducing.the.internet/internet.basics.eric-digest>
<URL: gopher://vega.lib.ncsu.edu:70/00/library/reference/guides/tennet>

[28] Wiggins, R., "The Internet for everyone: a guide for users and providers", New York, McGraw-Hill, 1995.

6.0 Security Considerations

Security issues are not discussed in this memo.

7.0 Author's Address

Sally Hambridge
Intel Corporation
2880 Northwestern Parkway
SC3-15
Santa Clara, CA 95052

Phone: 408-765-2931
Fax: 408-765-3679
EMail: sallyh@ludwig.sc.intel.com

Network Working Group
Request for Comments: 2635
FYI: 35
Category: Informational

S. Hambridge
INTEL
A. Lunde
Northwestern University
June 1999

DON'T SPEW
A Set of Guidelines for Mass Unsolicited
Mailings and Postings (spam*)

Status of this Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (1999). All Rights Reserved.

Abstract

This document explains why mass unsolicited electronic mail messages are harmful in the Internetworking community. It gives a set of guidelines for dealing with unsolicited mail for users, for system administrators, news administrators, and mailing list managers. It also makes suggestions Internet Service Providers might follow.

1. Introduction

The Internet's origins in the Research and Education communities played an important role in the foundation and formation of Internet culture. This culture defined rules for network etiquette (netiquette) and communication based on the Internet's being relatively off-limits to commercial enterprise.

This all changed when U.S. Government was no longer the primary funding body for the U.S. Internet, when the Internet truly went global, and when all commercial enterprises were allowed to join what had been strictly research networks. Internet culture had become deeply embedded in the protocols the network used. Although the social context has changed, the technical limits of the Internet protocols still require a person to enforce certain limits on resource usage for the 'Net to function effectively. Strong authentication was not built into the News and Mail protocols. The only thing that is saving the Internet from congestion collapse is the voluntary inclusion of TCP backoff in almost all of the TCP/IP

driver code on the Internet. There is no end-to-end cost accounting and/or cost recovery. Bandwidth is shared among all traffic without resource reservation (although this is changing).

Unfortunately for all of us, the culture so carefully nurtured through the early years of the Internet was not fully transferred to all those new entities hooking into the bandwidth. Many of those entities believe they have found a paradise of thousands of potential customers each of whom is desperate to learn about stunning new business opportunities. Alternatively, some of the new netizens believe all people should at least hear about the one true religion or political party or process. And some of them know that almost no one wants to hear their message but just can't resist how inexpensive the net can be to use. While there may be thousands of folks desperate for any potential message, mass mailings or Netnews postings are not at all appropriate on the 'Net.

This document explains why mass unsolicited email and Netnews posting (aka spam) is bad, what to do if you get it, what webmasters, postmasters, and news admins can do about it, and how an Internet Service Provider might respond to it.

2. What is Spam*?

The term "spam" as it is used to denote mass unsolicited mailings or netnews postings is derived from a Monty Python sketch set in a movie/tv studio cafeteria. During that sketch, the word "spam" takes over each item offered on the menu until the entire dialogue consists of nothing but "spam spam spam spam spam spam and spam." This so closely resembles what happens when mass unsolicited mail and posts take over mailing lists and netnews groups that the term has been pushed into common usage in the Internet community.

When unsolicited mail is sent to a mailing list and/or news group it frequently generates more hate mail to the list or group or apparent sender by people who do not realize the true source of the message. If the mailing contains suggestions for removing your name from a mailing list, 10s to 100s of people will respond to the list with "remove" messages meant for the originator. So, the original message (spam) creates more unwanted mail (spam spam spam spam), which generates more unwanted mail (spam spam spam spam spam and spam). Similar occurrences are perpetrated in newsgroups, but this is held somewhat in check by "cancelbots" (programs which cancel postings) triggered by mass posting. Recently, cancelbots have grown less in favor with those administering News servers since the cancelbots are now generating the same amount of traffic as spam. Even News admins are beginning to use filters, demonstrating that spam spam spam spam spam spam and spam is a monumental problem.

3. Why Mass Mailing is Bad

In the world of paper mail we're all used to receiving unsolicited circulars, advertisements, and catalogs. Generally we don't object to this - we look at what we find of interest, and we discard/recycle the rest. Why should receiving unsolicited email be any different?

The answer is that the cost model is different. In the paper world, the cost of mailing is borne by the sender. The sender must pay for the privilege of creating the ad and the cost of mailing it to the recipient. An average paper commercial mailing in the U.S. ends up costing about \$1.00 per addressee. In the world of electronic communications, the recipient bears the majority of the cost. Yes, the sender still has to compose the message and the sender has to pay for Internet connectivity. However, the recipient ALSO has to pay for Internet connectivity and possibly also connect time charges and for disk space. For electronic mailings the recipient is expected to help share the cost of the mailing. Bulk Internet mail from the U.S. ends up costing the sender only about 1/100th of a cent per address; or FOUR ORDERS of magnitude LESS than bulk paper mailings!

Of course, this cost model is very popular with those looking for cheap methods to get their message out. By the same token, it's very unpopular with people who have to pay for their messages just to find that their mailbox is full of junk mail. Neither do they appreciate being forced to spend time learning how to filter out unwanted messages. Consider this: if you had to pay for receiving paper mail would you pay for junk mail?

Another consideration is that the increase in volume of spam will have an impact on the viability of electronic mail as a communications medium. If, when you went to your postal mail box you found four crates of mail, would you be willing to search through the crates for the one or two pieces of mail which were not advertising? Spam has a tremendous potential to create this scenario in the electronic world.

Frequently spammers indulge in unethical behavior such as using mail servers which allow mail to be relayed to send huge amounts of electronic solicitations. Or they forge their headers to make it look as if the mail originates from a different domain. These people don't care that they're intruding into a personal or business mailbox nor do they care that they are using other people's resources without compensating them.

The huge cost difference has other bad effects. Since even a very cheap paper mailing is going to cost tens of (U.S.) cents there is a real incentive to send only to those really likely to be interested.

So paper bulk mailers frequently pay a premium to get high quality mailing lists, carefully prune out bad addresses and pay for services to update old addresses. Bulk email is so cheap that hardly anyone sending it bothers to do any of this. As a result, the chance that the receiver is actually interested in the mail is very, very, very low.

As of the date of this document, it is a daily event on the Internet for a mail service to melt-down due to an overload of spam. Every few months this happens to a large/major/regional/national/international service provider resulting in denial of or severe degradation of service to hundreds of thousands of users. Such service degradations usually prompt the providers to spend hundreds of thousands of dollars upgrading their mail service equipment just because of the volume of spam. Service providers pass those costs on to customers.

Doesn't the U.S. Constitution guarantee the ability to say whatever one likes? First, the U.S. Constitution is law only in the U.S., and the Internet is global. There are places your mail will reach where free speech is not a given. Second, the U.S. Constitution does NOT guarantee one the right to say whatever one likes. In general, the U.S. Constitution refers to political freedom of speech and not to commercial freedom of speech. Finally, and most importantly, the U.S. Constitution DOES NOT guarantee the right to seize the private property of others in order to broadcast your speech. The Internet consists of a vast number of privately owned networks in voluntary cooperation. There are laws which govern other areas of electronic communication, namely the "junk fax" laws. Although these have yet to be applied to electronic mail they are still an example of the "curbing" of "free speech." Free speech does not, in general, require other people to spend their money and resources to deliver or accept your message.

Most responsible Internet citizens have come to regard unsolicited mail/posts as "theft of service". Since the recipient must pay for the service and for the most part the mail/posts are advertisements of unsolicited "stuff" (products, services, information) those receiving it believe that the practice of making the recipient pay constitutes theft.

The crux of sending large amounts of unsolicited mail and news is not a legal issue so much as an ethical one. If you are tempted to send unsolicited "information" ask yourself these questions: "Whose resources is this using?" "Did they consent in advance?" "What would happen if everybody (or a very large number of people) did this?" "How would you feel if 90% of the mail you received was advertisements for stuff you didn't want?" "How would you feel if 95%

of the mail you received was advertisements for stuff you didn't want?" "How would you feel if 99% of the mail you received was advertisements for stuff you didn't want?"

Although numbers on the volume and rate of increase of spam are not easy to find, seat-of-the-pants estimates from the people on spam discussion mailing lists [1] indicate that unsolicited mail/posts seems to be following the same path of exponential growth as the Internet as a whole [2]. This is NOT encouraging, as this kind of increase puts a strain on servers, connections, routers, and the bandwidth of the Internet as a whole. On a per person basis, unsolicited mail is also on the increase, and individuals also have to bear the increasing cost of increasing numbers of unsolicited and unwanted mail. People interested in hard numbers may want to point their web browsers to <http://www.techweb.com/se/directlink.cgi?INW19980504S0003> where Internet Week reports what spam costs.

Finally, sending large volumes of unsolicited email or posting voluminous numbers of Netnews postings is just plain rude. Consider the following analogy: Suppose you discovered a large party going on in a house on your block. Uninvited, you appear, then join each group in conversation, force your way in, SHOUT YOUR OPINION (with a megaphone) of whatever you happen to be thinking about at the time, drown out all other conversation, then scream "discrimination" when folks tell you you're being rude.

To continue the party analogy, suppose instead of forcing your way into each group you stood on the outskirts a while and listened to the conversation. Then you gradually began to add comments relevant to the discussion. Then you began to tell people your opinion of the issues they were discussing; they would probably be less inclined to look badly on your intrusion. Note that you are still intruding. And that it would still be considered rude to offer to sell products or services to the guests even if the products and services were relevant to the discussion. You are in the wrong venue and you need to find the right one.

Lots of spammers act as if their behavior can be forgiven by beginning their messages with an apology, or by personalizing their messages with the recipient's real name, or by using a number of ingratiating techniques. But much like the techniques used by Uriah Heep in Dickens' David Copperfield, these usually have an effect opposite to the one intended. Poor excuses ("It's not illegal," "This will be the only message you receive," "This is an ad," "It's easy to REMOVE yourself from our list") are still excuses. Moreover, they are likely to make the recipient MORE aggravated rather than

less aggravated.

In particular, there are two very severe problems with believing that a "remove" feature to stop future mail helps: (1) Careful tests have been done with sending remove requests for "virgin" email accounts (that have never been used anywhere else). In over 80% of the cases, this resulted in a deluge of unsolicited email, although usually from other sources than the one the remove was sent to. In other words, if you don't like unsolicited mail, you should think carefully before using a remove feature because the evidence is that it will result in more mail not less. (2) Even if it did work, it would not stop lots of new unsolicited email every day from new businesses that hadn't mailed before.

4a. ACK! I've Been Spammed - Now What?

It's unpleasant to receive mail which you do not want. It's even more unpleasant if you're paying for connect time to download it. And it's really unpleasant to receive mail on topics which you find offensive. Now that you're good and mad, what's an appropriate response?

First, you always have the option to delete it and get on with your life. This is the easiest and safest response. It does not guarantee you won't get more of the same in the future, but it does take care of the current problem. Also, if you do not read your mail on a regular basis it is possible that your complaint is much too late to do any good.

Second, consider strategies that take advantage of screening technology. You might investigate technologies that allow you to filter unwanted mail before you see it. Some software allows you to scan subject lines and delete unwanted messages before you download them. Other programs can be configured to download portions of messages, check them to see if they are advertising (for example) and delete them before the whole message is downloaded.

Also, your organization or your local Internet Service Provider may have the ability to block unwanted mail at their mail relay machines and thus spare you the hassle of dealing with it at all. It is worth inquiring about this possibility if you are the victim of frequent spam.

Your personal mailer software may allow you to write rules defining what you do and do not wish to read. If so, write a rule which sends mail from the originator of the unwanted mail to the trash. This will work if one sender or site repeatedly bothers you. You may also consider writing other rules based on other headers if you are sure

the probability of them being activated for non-spam is low enough.

That way, although you may still have to pay to download it, you won't have to read it!

Third, you may consider sending the mail back to the originator objecting to your being on the mailing-list; however, we recommend against this. First, a lot of spammers disguise who they are and where their mail comes from by forging the mail headers. Unless you are very experienced at reading headers discovering the true origin of the mail will probably prove difficult. Although you can engage your local support staff to help you with this, they may have much higher priorities (such as setting up site-wide filters to prevent spam from entering the site). Second, responding to this email will simply verify your address as valid and make your address more valuable for other (ab)uses (as was mentioned above in Section 3). Third, even if the two previous things do not happen, very probably your mail will be directed to the computer equivalent of a black hole (the bit-bucket).

As of the writing of this document, there are several pieces of pending legislation in several jurisdictions about the sending of unsolicited mail and also about forging headers. If forging of headers should become illegal, then responding to the sender is less risky and may be useful.

Certainly we advocate communicating to the originator (as best as you can tell) to let them know you will NOT be buying any products from them as you object to the method they have chosen to conduct their business (aka spam). Most responses through media other than electronic mail (mostly by those who take the time to phone included "800" (free to calling party in the U.S.) phone numbers) have proved somewhat effective. You can also call the business the advertisement is for, ask to speak to someone in authority, and then tell them you will never buy their products or use their services because their advertising mechanism is spam.

Next, you can carbon copy or forward the questionable mail messages or news postings to your postmaster. You can do this by sending mail "To: Postmaster@your-site.example." Your postmaster should be an expert at reading mail headers and will be able to tell if the originating address is forged. He or she may be able to pinpoint the real culprit and help close down the site. If your postmaster wants to know about unsolicited mail, be sure s/he gets a copy, including headers. You will need to find out the local policy and comply.

Wherever you send a complaint, be sure to include the full headers (most mail and news programs don't display the full headers by default). For mail it is especially important to show the "Received:" headers. For Usenet news, it is the "Path:" header. These normally show the route by which the mail or news was delivered. Without them, it's impossible to even begin to tell where the message originated. See the appendix for an example of a mail header.

There is lively and ongoing debate about the validity of changing one's email address in a Web Browser in order to have Netnews posts and email look as if it is originating from some spot other than where it does originate. The reasoning behind this is that web email address harvesters will not be getting a real address when it encounters these. There is reason on both sides of this debate: If you change your address, you will not be as visible to the harvesters, but if you change your address, real people who need to contact you will be cut off as well. Also, if you are using the Internet through an organization such as a company, the company may have policies about "forging" addresses - even your own! Most people agree that the consequences of changing your email address on your browser or even in your mail headers is fairly dangerous and will nearly guarantee your mail goes into a black hole unless you are very sure you know what you are doing.

Finally, DO NOT respond by sending back large volumes of unsolicited mail. Two wrongs do not make a right; do not become your enemy; and take it easy on the network. While the legal status of spam is uncertain, the legal status (at least in the U.S.) of a "mail bomb" (large numbers and/or sizes of messages to the site with the intent of disabling or injuring the site) is pretty clear: it is criminal.

There is a web site called "www.abuse.net" which allows you to register, then send your message to the name of the "offending-domain@abuse.net," which will re-mail your message to the best reporting address for the offending domain. The site contains good tips for reporting abuse netnews or email messages. It also has some automated tools that you may download to help you filter your messages. Also check CIAC bulletin I-005 at:

<http://ciac.llnl.gov/ciac/bulletins/i-005c.shtml>

or at:

<http://spam.abuse.net/spam/tools/mailblock.html>.

Check the Appendix for a detailed explanation of tools and methodology to use when trying to chase down a spammer.

4b. There's a Spam in My Group!

Netnews is also subject to spamming. Here several factors help to mitigate against the propagation of spam in news, although they don't entirely solve the problem. Newsgroups and mailing lists may be moderated, which means that a moderator approves all mail/posts. If this is the case, the moderator usually acts as a filter to remove unwanted and off-topic posts/mail.

In Netnews there are programs which detect posts which have been sent to multiple groups or which detect multiple posts from the same source to one group. These programs cancel the posts. While these work and keep unsolicited posts down, they are not 100% effective and spam in newsgroups seems to be growing at an even faster rate than spam in mail or on mailing lists. After all, it's much easier to post to a newsgroup for which there are thousands of readers than it is to find individual email addresses for all those folks. Hence the development of the "cancelbots" (sometimes called "cancelmoose") for Netnews groups. Cancelbots are triggered when one message is sent to a large number of newsgroups or when many small messages are sent (from one sender) to the same newsgroup. In general these are tuned to the "Breidbart Index" [3] which is a somewhat fuzzy measure of the interactions of the number of posts and number of groups. This is fuzzy purposefully, so that people will not post a number of messages just under the index and still "get away with it." And as noted above, the cancel messages have reached such a volume now that a lot of News administrators are beginning to write filters rather than send cancels. Still spam gets through, so what can a concerned netizen do?

If there is a group moderator, make sure s/he knows that off-topic posts are slipping into the group. If there is no moderator, you could take the same steps for dealing with news as are recommended for mail with all the same caveats.

A reasonable printed reference one might obtain has been published by O'Reilly and Associates, Stopping Spam, by Alan Schwartz and Simson Garfinkel [4]. This book also has interesting histories of spammers such as Cantor and Siegel, and Jeff Slaton. It gives fairly clear instructions for filtering mail and news.

5. Help for Beleaguered Admins

As a system administrator, news administrator, local Postmaster, or mailing-list administrator, your users will come to you for help in dealing with unwanted mail and posts. First, find out what your institution's policy is regarding unwanted/unsolicited mail. It is possible that it won't do anything for you, but it is also possible to use it to justify blocking a domain which is sending particularly offensive mail to your users. If you don't have a clear policy, it would be really useful to create one. If you are a mailing-list administrator, make sure your mailing-list charter forbids off-topic posts. If your internal-only newsgroups are getting spammed from the outside of your institution, you probably have bigger security problems than just spam.

Make sure that your mail and news transports are configured to reject messages injected by parties outside your domain. Recently misconfigured Netnews servers have become subject to hijacking by spammers. SMTP source routing <relay.host:user@dest.host> is becoming deprecated due to its overwhelming abuse by spammers. You should configure your mail transport to reject relayed messages (when neither the sender nor the recipient are within your domain). Check:

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

under the "Anti-Spam" heading.

If you run a firewall at your site, it can be configured in ways to discourage spam. For example, if your firewall is a gateway host that itself contains an NNTP server, ensure that it is configured so it does not allow access from external sites except your news feeds. If your firewall acts as a proxy for an external news-server, ensure that it does not accept NNTP connections other than from your internal network. Both these potential holes have recently been exploited by spammers. Ensure that email messages generated within your domain have proper identity information in the headers, and that users cannot forge headers. Be sure your headers have all the correct information as stipulated by RFC 822 [5] and RFC 1123 [6].

If you are running a mailing-list, allowing postings only by subscribers means a spammer would actually have to join your list before sending spam messages, which is unlikely. Make sure your charter forbids any off-topic posts. There is another spam-related problem with mailing-lists which is that spammers like to retaliate on those who work against them by mass-subscribing their enemies to mailing-lists. Your mailing-list software should require confirmation of the subscription, and only then should the address be subscribed.

It is possible, if you are running a mail transfer agent that allows it, to block persistent offending sites from ever getting mail into your site. However, careful consideration should be taken before taking that step. For example, be careful not to block out sites for which you run MX records! In the long run, it may be most useful to

help your users learn enough about their mailers so that they can write rules to filter their own mail, or provide rules and kill files for them to use, if they so choose.

There is information about how to configure sendmail available at "www.sendmail.org." Help is also available at "spam.abuse.net."

Another good strategy is to use Internet tools such as whois and traceroute to find which ISP is serving your problem site. Notify the postmaster or abuse (abuse@offending-domain.example) address that they have an offender. Be sure to pass on all header information in your messages to help them with tracking down the offender. If they have a policy against using their service to post unsolicited mail they will need more than just your say-so that there is a problem. Also, the "originating" site may be a victim of the offender as well. It's not unknown for those sending this kind of mail to bounce their mail through dial-up accounts, or off unprotected mail servers at other sites. Use caution and courtesy in your approach to those who look like the offender.

News spammers use similar techniques for sending spam to the groups. They have been known to forge headers and bounce posts off "open" news machines and remailers to cover their tracks. During the height of the infamous David Rhodes "Make Money Fast" posts, it was not unheard of for students to walk away from terminals which were logged in, and for sneaky folks to then use their accounts to forge posts, much to the later embarrassment of both the student and the institution.

One way to lessen problems is to avoid using mail-to URLs on your web pages. They allow email addresses to be easily harvested by those institutions grabbing email addresses off the web. If you need to have an email address prevalent on a web page, consider using a cgi script to generate the mailto address.

Participate in mailing lists and news groups which discuss unsolicited mail/posts and the problems associated with it. News.admin.net-abuse.misc is probably the most well-known of these.

6. What's an ISP to Do

As an Internet Service Provider, you first and foremost should decide what your stance against unsolicited mail and posts will be. If you decide not to tolerate unsolicited mail, write a clear Acceptable Use Policy which states your position and delineates consequences for abuse. If you state that you will not tolerate use of your resource for unsolicited mail/posts, and that the consequence will be loss of service, you should be able to cancel offending accounts relatively quickly (after verifying that the account really IS being mis-used). If you have downstreaming arrangements with other providers, you should make sure they are aware of any policy you set. Likewise, you should be aware of your upstream providers' policies.

Consider limiting access for dialup accounts so they cannot be used by those who spew. Make sure your mail servers aren't open for mail to be bounced off them (except for legitimate users). Make sure your mail transfer agents are the most up-to-date version (which pass security audits) of the software.

Educate your users about how to react to spew and spewers. Make sure instructions for writing rules for mailers are clear and available. Support their efforts to deal with unwanted mail at the local level - taking some of the burden from your system administrators.

Make sure you have an address for abuse complaints. If complainers can routinely send mail to "abuse@BigISP.example" and you have someone assigned to read that mail, workflow will be much smoother. Don't require people complaining about spam to use some unique local address for complaints. Read and use 'postmaster' and 'abuse'. We recommend adherence to RFC 2142, *_Mailbox Names for Common Services, Roles and Functions_* [7].

Finally, write your contracts and terms and conditions in such language that allows you to suspend service for offenders, and so that you can impose a charge on them for your costs in handling the complaints their abuse generates and/or terminating their account and cleaning up the mess they make. Some large ISPs have found that they can fund much of their abuse prevention staff by imposing such charges. Make sure all your customers sign the agreement before their accounts are activated. There is a list of "good" Acceptable Use Policies and Terms of Service at:

<http://spam.abuse.net/goodsites/index.html>.

Legally, you may be able to stop spammers and spam relayers, but this is certainly dependent on the jurisdictions involved. Potentially, the passing of spam via third party computers, especially if the

headers are forged, could be a criminal action depending on the laws of the particular jurisdiction(s) involved. If your site is being used as a spam relay, be sure to contact local and national criminal law enforcement agencies. Site operators may also want to consider bringing civil actions against the spammer for expropriation of property, in particular the computer time and network bandwidth. In addition, when a mailing list is involved, there is a potential intellectual property rights violation.

There are a few law suits in the courts now which claim spammers interfered with and endangered network connectivity. At least one company is attempting to charge spammers for the use of its networks (www.kclink.com/spam/).

7. Security Considerations

Certain actions to stop spamming may cause problems to legitimate users of the net. There is a risk that filters to stop spamming will unintentionally stop legitimate mail too. Overloading postmasters with complaints about spamming may cause trouble to the wrong person, someone who is not responsible for and cannot do anything to avoid the spamming activity, or it may cause trouble out of proportion to the abuse you are complaining about. Be sure to exercise discretion and good judgment in all these cases. Check your local escalation procedure. The Site Security Handbook [2] can help define an escalation procedure if your site does not have one defined.

Lower levels of network security interact with the ability to trace spam via logs or message headers. Measures to stop various sorts of DNS and IP spoofing can make this information more reliable. Spammers can and will exploit obvious security weaknesses, especially in NNTP servers. This can lead to denial of service, either from the sheer volume of posts, or as a result of action taken by upstream providers.

8. Acknowledgments

Thanks for help from the IETF-RUN working group, and also to all the spew-fighters. Specific thanks are due to J.D. Falk, whose very helpful Anti-spam FAQ proved valuable. Thanks are also due to the vigilance of Scott Hazen Mueller and Paul Vixie, who run spam.abuse.net, the Anti-spam web site. Thanks also to Jacob Palme, Chip Rosenthal, Karl Auerbach for specific text: Jacob for the Security Considerations section, Chip for the configuration suggestions in section 5, Karl for the legal considerations. Andrew Gierth was very helpful with Netnews spam considerations. And thanks to Gary Malkin for proofing and formatting.

9. References

- [1] See for example `spam-l@peach.ease.lsoft.com`
 - [2] Fraser, B., "Site Security Handbook", FYI 8, RFC 2196, September 1997.
 - [3] "Current Spam thresholds and guidelines," Lewis, Chris and Tim Skirvin, <http://www.killfile.org/~tskirvin/faqs/spam.html>.
 - [4] Schwartz, Alan and Simson Garfinkel, "Stopping Spam," O'Reilly and Associates, 1998.
 - [5] Crocker, D., "Standard for the format of ARPA Internet text messages", STD 11, RFC 822, August 1982.
 - [6] Braden, R., "Requirements for Internet hosts - application and support", STD 3, RFC 1123, October 1989.
 - [7] Crocker, D., "Mailbox Names for Common Services, Roles and Functions", RFC 2142, May 1997.
- * Spam is a name of a meat product made by Hormel. "spam" (no capitalization) is routinely used to describe unsolicited bulk email and netnews posts.

10. Appendix - How to Track Down Spammers

In a large proportion of spams today, complaining to the postmaster of the site that is the apparent sender of a message will have little effect because either the headers are forged to disguise the source of the message, or the senders of the message run their own system/domain, or both.

As a result, it may be necessary to look carefully at the headers of a message to see what parts are most reliable, and/or to complain to the second or third-level Internet providers who provide Internet service to a problem domain.

In many cases, getting reports with full headers from various recipients of a spam can help locate the source. In extreme cases of header forgery, only examination of logs on multiple systems can trace the source of a message.

With only one message in hand, one has to make an educated guess as to the source. The following are only rough guidelines.

In the case of mail messages, "Received:" headers added by systems under control of the destination organization are most likely to be reliable. You can't trust what the source domain calls itself, but you can usually use the source IP address since that is determined by the destination domain's server.

In naive mail forgeries, the "Message-ID:" header may show the first SMTP server to handle the message and/or the "Received:" headers may all be accurate, but neither can be relied on. Be especially wary when the Received: headers have other headers intermixed. Normally, Received: headers are all together in a block, and when split up, one or the other blocks is probably forged.

In the case of news messages, some part of the Path: header may be a forgery; only reports from multiple sites can make this clear. In naive news forgeries, the "NNTP-Posting-Host:" header shows the actual source, but this can be forged too.

If a spam message advertises an Internet server like a WWW site, that server must be connected to the network to be usable. Therefore that address can be traced. It is appropriate to complain to the ISP hosting a web site advertised in a SPAM, even if the origin of the spam seems to be elsewhere. Be aware that the spam could be an attack on the advertised site; the perpetrator knows the site will be deluged with complaints and their reputation will be damaged. Any spam with an electronic address in it is suspect because most spammers know they're unwelcome and won't make themselves accessible.

Here is an example mail header:

```
-----
From friendlymail@209.214.12.258.com Thu Feb 26 20:32:47 1998
Received: from clio.sc.intel.com by Ludwig.sc.intel.com (4.1/SMI-4.1)
       id AA05377; Thu, 26 Feb 98 20:32:46 PST
Received: from 209.214.12.258.com (209.214.12.258.com [208.26.102.16])
       by clio.sc.intel.com (8.8.6/8.8.5) with ESMTMP id UAA29637
       for <sallyh@intel.com>; Thu, 26 Feb 1998 20:33:30 -0800 (PST)
Received: ok
X-Sender: promol@gotosportsbook.com
X-Advertisement: <a href="http://www.opt-out.com">
Click here to be removed.
Date: Thu, 26 Feb 1998 23:23:03 -0500
From: Sent By <promol@gotosportsbook.com>
Reply-To: Sent By <promol@gotosportsbook.com>
To: friend@bulkmailer
Subject: Ad: FREE $50 in Sportsbook & Casino
X-Mailer: AK-Mail 3.0b [eng] (unregistered)
Mime-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Transfer-Encoding: 7bit
Sender: friendlymail@aqua.258.com
Message-Id: <bulk.6508.19980226232535@aqua.258.com>
Status: R
-----
```

Doing a traceroute on an IP address or DNS address will show what domains provide IP connectivity from you to that address.

Using whois and nslookup, one can try to determine who is administratively responsible for a domain.

In simple cases, a user of a responsible site may be exploiting an account or a weakness in dial-up security; in those cases a complaint to a single site may be sufficient. However, it may be appropriate to complain to more than one domain, especially when it looks like the spammers run their own system.

If you look at the traceroute to an address, you will normally see a series of domains between you and that address, with one or more wide-area/national Internet Service Providers in the middle and "smaller" networks/domains on either end. It may be appropriate to complain to the domains nearer the source, up to and including the closest wide-area ISP. However, this is a judgement call.

If an intermediate site appears to be a known, responsible domain, stopping your complaints at this point makes sense.

Authors' Information

Sally Hambridge
Intel Corp, SC11-321
2200 Mission College blvd
Santa Clara, CA 95052

EMail: sallyh@ludwig.sc.intel.com

Albert Lunde
Northwestern University
Suite 1400
1603 Orrington Avenue
Evanston, IL 60201

EMail: Albert-Lunde@nwu.edu

Full Copyright Statement

Copyright (C) The Internet Society (1999). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.