

LAFN OUT LOUD

A MESSAGE FROM THE STEERING COMMITTEE

The Steering Committee of the Los Angeles Free-Net would like to take this opportunity to express our sadness for the tragic and horrific attack on the United States, September 11, 2001. Our thoughts and prayers go to the victims of this tragedy. The necessity of good communication capabilities during difficult times as these confirms the value of this goal of the Los Angeles Free-Net. It is our wish that we have in some way risen to the occasion to meet the needs of our users during this crisis. We welcome a response from our users regarding any anecdotes you may have on how LAFN may have been of value during this time. Please e-mail your comments to eartestr@lafn.org so that we may be made aware of your experience. We will consider printing some of the responses in our next edition of LAFN OUT LOUD.

In response to the recent terrorist attack on America, we have established the following links to help people connect with loved ones who might have been affected directly by this attack. These links may be found at:

www.lafn.org/medical/disaster.resources.html.

Web sites for seekers, survivors, and informants

Safe (safe.millennium.berkeley.edu) I believe this is the best site since it incorporates many sites and provides

- Survivor registries
- NY hospital admission search engines
- Friends and Family Status Databases

New York City Bombing Check-in Registry (www.shunn.net/okay)

Prodigy's "OK Message Center" (okay.prodigy.net) - A site where you can list your name and state you are OK. (Included in the Berkeley Safe site)

SeptEleven (bostoncoop.net:8080/SeptEleven), a place for survivors to list their status (by surname) and links to other sites allowing for the communication we are trying to facilitate.

World Trade Center People Locator (tradecenter.cnets.net) Search by first name or last name for status and update.

PRIVACY NOTICE

At the request of our users, we have added a link to our privacy notice on our home page. The Los Angeles Free-Net is concerned about the privacy of our users and encourage them to link to our statement expressing this concern.

(Continued)

GOOGLE SEARCH

We are pleased to inform you that you will soon be able to search the LAFN website via Google. Please click on the appropriate area on our home page.

MEMBERSHIP CONTEST

To maintain or improve our level of service to our users, it is necessary that we increase our user base. To encourage our users to help spread the word about the Los Angeles Free-Net, we are holding a membership contest during the month of October. We will provide more complete details at the end of September regarding the contest. In the meantime, we invite you to give consideration to those you know that could be potential users of the Free-Net.

NEED A GOOD DOSE OF COMMON SENSE?

LAFN Ops frequently receives many notices about the latest viruses and hoaxes. Well, here is a good one for verifying this information:

<http://www.datafellows.com/virus-info/>

Do not pass Go or collect \$200 without first reading that. Thanks to Chuck Wilkinson, az260, for pointing out the need for this reference.

LAFN UPDATING PASSWORD SYSTEM

LAFN will shortly be updating its password system to one that provides more security. The new system will actually use all of the characters in your password rather than only the first 8 as is done as present. This change should have no effect on the users except that we encourage them to go the User Services after the update is complete and change their password.

The system will continue to accept the old passwords so there is no requirement to change yours. However, your password will not gain the additional security from the new system until you do change it. Because passwords are sent in the clear when authenticating using mail, it is recommended that you change your password periodically. Do remember to update your dialer with the new password. Please note that a change to the password does not take effect for up to 7 hours after you make the change.

BYPASSES FOR SPAM BLOCKED E-MAIL

During the last few weeks there have been a number of misconceptions about bypasses for spam blocked email. Hence, we would like to add some clarification about spam blocking. LAFN blocks spam at the lowest possible source. For example, if a spammer is stupid enough to use their real email address then we will only block that address. However, very few do that. Most of them use open relays that have been setup by othr ISPs for their personal use. The problem is that they can also be used by the spammer such that their real identification is removed.

Not all open relays are known at any time. Sometimes they are created for a specific time and then removed. Other times they are created inadvertently. Spammers occasionally find new open relays. Hence you will find that the list of ISPs that are blocked, or partially blocked, changes with time. Blocks come and go as the nature of their use by spammers changes. Some ISPs are very

conscientious about removing open relays and when one is found on their system, they clean it up quickly. It is possible in those cases for a block to last only an hour or two in those situations. Others use the open relays for their purposes and the blocks will remain for many months.

LAFN does not block ISPs per se. We block the IP address of the Mail Transfer Agent (MTA). Many large ISPs have multiple MTAs because the volume of mail they process is too large for just one. LAFN, for example, has two MTAs. MTAs can be shared by multiple ISPs. This is quite common in large ISPs that have been created by various mergers of smaller ISPs. There is no way to tell which domains might use a specific MTA. We can't tell you who is actually being blocked at a user level. In addition, when an ISP has multiple MTAs, a particular user might be assigned to a different MTA each time they connect to the ISP. Sometimes their mail might be blocked and sometimes not.

When you request spam blocking notification from LAFN, that process will tell you which messages were blocked by the spam blocking. However, because that functionality is not built into the MET but had to be added on, that notification will be a day or two later than the actual receipt of the message. That means that if you request a bypass for an address today, and it's entered today, you may receive notification tomorrow and possibly the next day of blocked mail from that address. All of those messages were actually received prior to the bypass being established.

If you make multiple requests for the same address based on those multiple messages, then it causes significant delays for all bypasses for all users unless I am able to recall that I added that address earlier. Given the volume of requests I receive daily, it's not very likely that it will be recalled. As a result, when the bypass list is updated, the update fails and we have to research where the duplicate is and remove it. This takes time and delays the inclusion of bypasses for all users.

Requests for bypasses in HTML format are very difficult to process. HTML format is when you click on the address and it opens a new message to that address. They usually appear as the address with a line under it in the message. Those addresses cannot be cut and pasted into the bypasses. They have to be retyped. While I think I am a fairly good typist, experience shows that might not be all that accurate. If I don't get it right, you will be disappointed as the bypass you requested did not get entered. The one I did enter probably is useless.

Please note that mail lists pose significant issues for bypassing. For example, at least one popular mail list server uses a sequence number in the from address of each message where the number increases for each new message. Messages from those mail list servers cannot have a bypass opened as the address is never used again. Likewise, there are some common addresses that start with "bounce". Those are almost always open relays that are deliberately there for a specific use. Spammers use those also since they are very effective. We do not establish bypasses for bounce type addresses because it opens a flood of spam for all LAFN users.

A bypass permits a message from anyone on the internet who knows that address to send mail to any LAFN user. That means that if a spammer knows that you have requested a bypass for a specific address, they can use that address and their spam will be delivered to all LAFN users. Generally this does

not happen. However, it has occurred and when we find a spammer using a bypass, we have no choice but to remove the bypass.

When a message is received by LAFN's MTA, the first thing it receives is the envelope, the real from and to addresses established by the originating MTA. These are not the from and to addresses in the message. Those can be anything that is valid or invalid. The spam checks are done with the envelope address. If the message is blocked, the connection to the originating MTA is terminated. The text of the message is never received by LAFN's MTA. We drop the connection because we need to minimize the traffic load on our internet connection. Hence, we cannot give you the message that was blocked. All we received was the envelope. You will need to contact the originator and have the message resent after you have opened a bypass or arranged to have it sent to another address.

In addition to the above, we also have the problem of viruses sent via email. There have been a number of such viruses which cause your computer to send copies of them to other users. Usually they scan your address list and send to those addresses. Aside from this being annoying to those users, frequently they end up sending to invalid addresses. Those messages bounce back to our MTA as non-deliverable. If the return address in the message is correct, it will come back to you. Most developers of viruses know that's not a good idea. You quickly find out that you have a virus, clean it off your computer and effectively stop the distribution. That is not what they want to occur. Hence, they munge the return address so that it will be invalid. The latest set of viruses add one to the second letter of your user id. For example if my computer were to send such, the return address would be bd979 rather than bc979. Thus I will not receive the bounce and my computer will continue to spread the virus.

However, the bounced message to bd979 usually is not delivered because the munged address is not an active account so it goes to our MTA logs. These logs get quite large quickly from these viruses and space that could be used for mail goes to them. A few months ago, the volume of these viruses was so large, that LAFN created filters to identify some of the most frequent of these viruses. Those messages are blocked just like spam messages. However, bypasses will not work for those virus messages. The viruses are blocked before the spam bypasses are checked. If someone sends you a message that does contain one of those viruses we block, there is no way to receive that message until they clean it off their system and out of the message.

One last thing that bears remembering, if you receive email that is not wanted and you are not knowledgeable about the source, do not use the response address to remove yourself from future mailings. Even if it does remove you from them, it also validates that your email is valid and make it valuable for other spammers. We periodically hear about LAFN spamming others. It almost always turns out to be a spammer using the LAFN member's return address. The message never transited the LAFN servers and hence was not from the indicated user. We believe most of those addresses were obtained via the "remove me" mechanism.

Doug Hardie, bc979@lafn.org
System Administrator

Donna Glick, eartestr@lafn.org

Public Relations