



February 2006

Volume 2, Number 2

In This Issue

- Email know how, Part II – Stopping SPAM
- Tips for Reducing Spam
- Blessing joins team
- Meet the Team
- Free Anti-virus

Security Links

Home Security
Information on securing your home pc.

Free Antivirus
McAfee Anti-virus free for the university community

N.U.C.I.A.
Nebraska University Consortium on Information Assurance.

Contact Us

Spider.unomaha.edu
(coming soon)

Unohelpdesk@mail.unomaha.edu

Stopping SPAM (Email know how, Part II)

UNO, like most entities, faces a constant battle with spam. Approximately 75,000 - 100,000 emails come to the campus Lotus Notes system each day. On average, over 75% of these messages are unwanted messages taking the form of mass mailing (spammers) or messages with viruses or phishing. UNO ITS is charged with the protection of the campus e-mail systems as described in section 7 D of the UN Responsible Usage memorandum http://www.nebraska.edu/about/exec_memo16.pdf.

How does ITS Help with SPAM?

Currently, a product called SpamJam is installed on the Lotus Notes server and licensed to cover all faculty/staff. Each user has the option to use SpamJam. If you are not currently using SpamJam, you can go [here](#) to request activation. *(text link at end of document)

Tips for Reducing SPAM

1. Avoiding Unwanted E-mail

Avoid supplying your e-mail address on web sites or to unknown individuals. Many companies (reputable and un reputable) may supply your e-mail address to mailing lists.

If you do need to supply an e-mail address, you may want to give a false e-mail address (you don't owe any web site your real e-mail address unless you want them to send you e-mail). But be sure you don't give another person's e-mail address as that can be considered a form of harassment.

Consider getting a secondary e-mail address you can use for your less important contacts. One of the free Internet web based e-mail systems is a good option and keeps your primary e-mail account less cluttered.

2. How do spammers harvest e-mail addresses?

Visit <http://www.private.org.il/harvest.html> for more information

3. Using Caution with Unwanted e-mail

Many e-mail messages give instructions that tell you to reply or send a message to an address to be removed from their mailing list. Don't

believe it! Don't do it! These options often act as a confirmation that your e-mail address is active and is a good address to pass on to other e-mail lists.

Do not reply to an e-mail address or to the company that the message appears to come from. Many unwanted e-mail messages have forged (fake) "from" information. If you complain to name or address that appears in the "from" area of the message, you may be unwittingly helping to harass an innocent company or individual.

Forwarding the offending message to the IT staff that maintain your e-mail system, is often not going to help because of the fake "from" information in most unwanted e-mail. See the "what to do" section for better options.

Never send multiple messages or messages with questionable content or language to a suspected mail sender. While unwanted e-mail messages can be frustrating and annoying, the aforementioned type of messages may be considered illegal activity.

If an unwanted e-mail message has an attachment, do not open the attachment. It is not uncommon for such attachments to contain a virus or other destructive program. UNO students, faculty and staff should contact the UNO Helpdesk (554-3282 or unohelpdesk@mail.unomaha.edu) for information on free virus protection software.

4. What to do if you get unwanted e-mail.

The easiest thing to do is to just delete the unwanted e-mail messages. If you're comfortable with that solution then read no further. If you are using Lotus Notes via a web browser, that is the only option. If you are a Lotus Notes client (version 6.x or higher) user and you want to combat unwanted e-mail, and are willing to spend a few minutes per message doing so, here are some effective steps:

- **Unwanted email from a UN Lotus Notes account:**

- 1) When you get an unwanted e-mail message sent to your Lotus Notes client account from another Lotus Notes user, close the message so you are again viewing your inbox of messages.
- 2) Right-click on the unwanted message and in the menu that pops up, select "document properties". This will give you a display box of information about this document (message).
- 3) In the "Document Information" window there are a series of tabs near the top of the box. Click on the "fields" tab.
- 4) You will see multiple fields of information. Look for fields called "Additional Headers" or "Received". Click on each in your listing and look on the right side to see which one has the most information. You are looking for information about IP (Internet) numbers, sets of four numbers with dot (.) separators. (000.000.000.000). Each set might be one, two, or three digits.
- 5) Use your cursor to select all of the information in the right

side of the document box (you may need to scroll to get all of it selected). Right-click for options, and select "copy". Now that you have all of the source information for this message. Close the document information box.

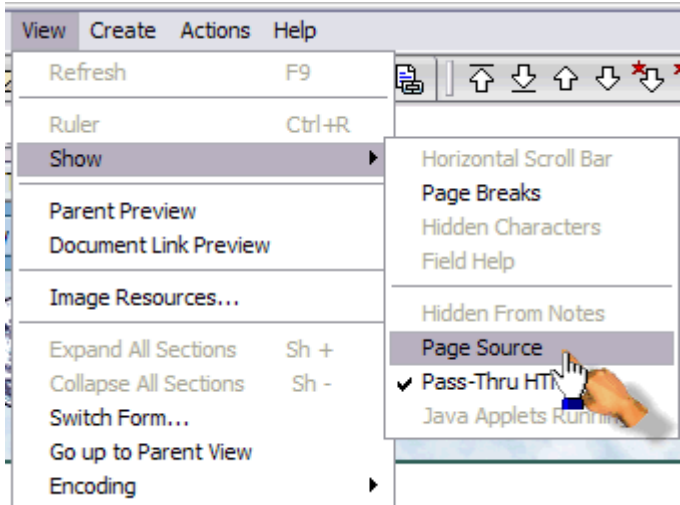
- 6) Re-open the same unwanted e-mail message and then click the "forward" button. Don't fill out the "To:" field information yet. Place your cursor at the top of the body of the new message and click on the "Edit>Paste" options in the tool bar at the top of the screen. This will put all of the routing information (where it came from) that you copied into the body of the memo.
- 7) Open up a web browser and go to this address: <http://www.arin.net/whois/index.html>. In the "whois" search box, enter one of the IP numbers you have in the body of your Lotus Notes forwarded message screen and click on the whois search button.
- 8) You should now have a screen on your web browser with whois information about the company that owns this computer system. There should also be one or more e-mail addresses on this screen. Copy these e-mail addresses into the To: field of the Lotus Notes message you are forwarding.
- 9) Repeat the steps for each of the IP numbers you have at the top of the message you are forwarding.
- 10) For each of the addresses you are sending to, also cc: the message to abuse@companyname.com. For example, if one of the e-mail addresses is jdoe@abcxyz.com, then in the cc: field of your message also send it to abuse@abcxyz.com. For the final address in your message, send it to abuse@unomaha.edu as one of your cc: addresses.
- 11) You are almost ready to report the unwanted message with the relevant information to the proper contacts. As a final step you should include some clear and direct but not abusive information about why you are sending them this message. Here is a suggested paragraph you can include at the top of your message:

"Below is an unsolicited message that was sent either from or through your computer system. You should be aware that your system is being used to either send or relay e-mail that may be in violation of your acceptable use policy or may be in violation of state or federal laws. As the officially listed contact for these systems we are sending you the content of this message as well as the header and routing information. This supplies you with all of the information you need to be able to take action on this problem."

- **Unwanted email from an Internet site:**

If you have received an unwanted e-mail in your Lotus Notes account through the Internet and NOT through another Lotus Notes client, you can still determine the sender of that e-mail to report them to authorities:

- 1) With the message open, click on "View>Show>Page Source":



- 2) Once the source code is visible, you can right-click on the page to print the source information or to forward it to proper authorities (<http://www.arin.net/whois/index.html>).

Blessing joins IA team

George Blessing

George began working as a PTSW for UNO Computing & Data Communications in late 1993 at the Training and Computer Information Center (TCIC). At the TCIC, and later the Computer Helpdesk, George assisted those in need of computer-related help, in-person, over the telephone, on, and off campus. In the Fall of 1999, George joined Steve Lendt and Aaron Murray in the Network department and was instrumental in deploying our current QIP DNS/DHCP systems. In September of 2000 and after much arm-twisting, George hired on full-time with ITS and began his current role as System Administrator II. This allowed him to increase his server management and enterprise systems experience. George worked with others to deploy the current UNOMAHA.EDU Active Directory, which serves various departments on-campus with file-sharing capabilities, as well as back-end authentication for a number of websites that make file storage over the internet a reality. George has steadily increased his knowledge of server technology and management practices over the years, especially in the area of secure server operation, and will continue to study and improve his skills to help others on-campus in their quest to provide a secure information environment at UNO.

George will be assisting the campus in the area of server security, including the creation and maintenance of policies that will help existing and new server managers to properly secure their servers. In the case of server-related security issues, George will also work with the appropriate server administrator(s) to examine and investigate the extent of damage caused by any breach in security.

Some of the server-related areas that George will be involved with are:

- Initial installation
- Installation of O/S

Configuration of common items
Securing the installation
Filesystem configuration
Antivirus and Antispyware software
Firewall configuration
Documentation of configuration
IIS configuration

Ongoing

Change documentation
System monitoring
OS/software/application updates

Incident response

Respond to reported incidents
Investigate incidents to determine extent of compromise
Repair work to affected server

This newsletter will be distributed via eNotes and our website at
<http://spider.unomaha.edu>

Meet the SPIDER team...

Bret Blackman, Team Lead

Dan Kenny, Application Development

Matt Galardi, Workstations & End User Education

Aaron Murray, Network & System Security

Stephen McIntyre, Daily Operations & Business Continuity

Miun Criffield, Data Storage & Transmission

George Blessing, Server Security

SpamJam activation link:

<https://unomail2.unomaha.edu/databases/ITS/RequestForm/Insjreqform.nsf/Form?OpenForm>

Free: McAfee Anti-virus

ITS provides free to all members of the campus community McAfee anti-virus, enterprise edition. This is available for Windows and Macintosh environments and licensed for home use. To obtain this product, go to <http://install.unomaha.edu>. A login page will request your UNONet ID and password. Installation instructions are located on the right side of the web page. If installation assistance is required, please call the UNO HelpDesk at 554-4357 during normal business hours.