

Are You Receiving More Spam? Well, Stop It!

If you think you are receiving more junk e-mail (spam) at work or at home than last year, you are probably correct. The article "U.S. Sending More Than Half of All Spam," July 1, 2004, Internetnews.com, provides these numbers:

- According to a report from Commtouch Software Ltd, an anti-spam company based in Mountain View, California, spam has increased from almost 350,000 unique outbreaks in January 2004 to 500,000 in June 2004.
- A report released last month by MessageLabs, Inc., an e-mail management and security company based in New York, showed that nine out of 10 e-mails in the U.S. are now spam. Globally, 76 percent of all e-mails are spam.
- Michael Osterman, founder and president of Osterman Research, Inc. (Black Diamond, WA) predicts, "In the next year to a year and a half, spam will account for 98 percent of all e-mail. That's being pessimistic some would say. The optimistic forecast is that it will only get to 95 percent."

How can you reduce the amount of spam you receive?

Use a spam filter. If you have a Lotus Notes account, you should be using **spamJam** to stop the spam. SpamJam has default settings that catch most spam, and, if needed, you can add configuration settings to stop additional mail items from reaching your inbox.

With spamJam activated, you will receive a "Summary Message" from the spamJam log of what was caught during the previous day. If you see a message that you want to read you can View it or Restore it to your inbox. Messages are kept in the log for 14 days and then are deleted from the server.

To request that spamJam be added to your account, go to the spamJam Web page <<http://notes.unl.edu/newnotes/spamJam.htm>>. You will need to use the Lotus Notes full-client software to make changes to your configuration settings and to view or restore messages from the spamJam log. More information is available on the spamJam page.

For spam filtering on a home e-mail account, please check with your Internet Service Provider (ISP) or e-mail service to set up spam filtering.

Don't display your e-mail address on public Internet sites. Typically, an e-mail spammer buys a list of e-mail addresses from a list broker, who compiles it by "harvesting" addresses from the Internet. If your e-mail address appears in a

newsgroup posting, on a website, in a chat room, or in an online service's membership directory, it may find its way onto these lists.

If you do participate in chat rooms or newsgroups, you should use a different e-mail address for this activity or use an alias or disposable e-mail address service.

Don't provide your address without knowing how it will be used. If you need to provide your e-mail address to a website before you can access the full array of information or before you can complete a purchase, be sure to read the privacy policy. Also, make sure that you have correctly "opted out" of receiving e-mail from their "partners," and even from the site owner's list. You may also want to use an alias or disposable address for these sites.

What should you do with the spam that is in your inbox?

Delete it! If the sender's address is unknown and the subject is suspect (or missing), don't even open it.

A lot of spam e-mails now contain images that when viewed (the e-mail note is opened) runs a small program that alerts the sender that their mail has arrived and that the receiving e-mail address is valid. You may find yourself receiving even more spam!

Never respond! If you open the e-mail, DO NOT use the reply option to take yourself off the list. Any response or acknowledgment tells the spammer your e-mail account is active, and you may then find yourself receiving more spam.

DO NOT buy anything — most offers are scams. Spam is growing because it works. Netscape news reported that according to a Yahoo! Mail survey of over 35,000 Internet users, 20% of Americans buy something advertised in spam.

DO NOT answer e-mail asking you to help someone recover their personal fortune.

Report it to the Federal Trade Commission, (FTC), your ISP, and the sender's ISP. Please see the FTC article "You've Got Spam: How to 'Can' Unwanted E-mail" <www.ftc.gov/bcp/online/pubs/online/inbox.htm> for more information on reporting spam.

~ Pam Peters

Have You Changed Your Network Logon Password?

The IANR Password Policy went into effect on May 1. This means that you need to **change your IANRDOM network logon password to 10 characters in length (minimum) with a mix of alpha (lower and upper case) and numeric characters**. We are currently working with IANR faculty and staff during the phase-in of this policy and will soon make changes to the server that will check for proper passwords.

You need to create a password that is easy to remember, but not easy to guess (i.e., easily figured out by hackers).

- # Don't use any of the popular passwords: the word "password" or "admin," immediate family name, sports team or popular cultural name, or pet name.
- # Don't use passwords that are based on personal information that can be easily accessed or guessed.
- # Don't use a password based on the computer name or your logon account or user name (e.g., don't use ppeters2004).
- # Don't use a password based on a word found in any dictionary of any language or a common misspelling of a word or a word spelled backwards (e.g., don't use secret8, terces).
- # Don't use word or number patterns (e.g., qwerty, 123321).

You want to create a unique password but not one that you have to write down as others could find the paper and access your computer and the network. How do you do that when you have to use a mixture of lower and upper case characters, numbers, and, possibly, punctuation characters? Here are three guidelines for creating secure, easy-to-remember passwords.

- # Create a password based on a favorite song lyric or phrase. For example, if the phrase is "Four score and seven years ago," the password could be *FS+7YrsA04*.
- # Create a password based on easy-to-remember names or words that are not directly related to each other but that you can remember. When you have the words you want to use, combine the words and change several letters in the words to upper-case letters, numbers, or symbols (e.g., cat's, bell becomes *Ca7's\$b3lL*).
- # Create a password based on typing a word using alternate keys, for example use the keys to the above-left of normal typing position and add numbers for the month and year you started using it. Let's say your grandmother's middle name is Pamela and you are going to use the alternate-keys method, here is a possible password: *0qj3oq-704*.

A recent study by Cambridge University Computer Laboratory found that passwords based on mnemonic phrases (using the first letter of a phrase and mixing in numbers and symbols) are just as easy to remember as simple passwords for most users and are nearly as effective against attack as random passwords. (Report from study: <http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/tr500.pdf>)

Two good resources for more information on creating secure passwords are: "Choosing Good Passwords" <<http://security.uchicago.edu/docs/userpassword.shtml>> and "Lock IT Down: Creating passwords that are secure and easy to remember" <<http://techrepublic.com.com/5102-6264-1047939.html>>.

Another important item to remember is to NOT use personal password(s) used for home and personal accounts (e.g., bank PINs) for work related resources.

For instructions on changing your network logon password, please see the March/April issue.

~ Pam Peters

Keep It Legal!

Lots of new computers have arrived on campus and at offices across the state so it is time to remind everyone that the University has a strict policy against violating software licenses or copyrights. You should review the [Executive Memorandum #16: Policy for Responsible Use of University Computers and Information Systems](#) (revised and dated August 28, 2001).

Section six of the policy "Misuse of computers and network systems" states, in part, that misuse of University information systems is prohibited. Misuse includes the following: *Violating any software license or copyright, including copying or redistributing copyrighted software, without the written authorization of the software owner.* (Subsection h)

Be sure to maintain all records of software purchases and licensing information to verify that all installations are legal.

It is also the responsibility of each office to have UNL server access or purchased CDs for all installed software. The media is needed for installing new licenses on new computers, for fixing problems, or for uninstalling programs.

UNL has site licenses for several software suites and individual applications. All licenses are basically the same. The site licenses are for departmental purchases, not purchases by individuals for home use. **Each computer must have a separate license.** To upgrade the license to a newer version of the software, you must have purchased a "maintenance license" or purchase a new license.

For the details on each UNL site license, including at-home or portable computer use, please see the UNL Licenses homepage (sales.unl.edu/licenses/default.asp).

Generate More Web Traffic

When people use Yahoo!, Google, or another search engine, they tend to only look at the search results on the first page. If they don't see a relevant match, most people start a new search. Naturally, you want your website to be listed on the first page of search results. Use these tips from the Tip of the Month on the CIT Computing website (citcomputing.unl.edu) to generate more Web traffic.

- # Select your keyword phrase.
- # Place your keywords in the title and in the text.
- # Use text links and link internally between your pages.
- # Get links from the outside to your site.
- # Avoid search engine stumbling blocks.
- # Remember to use traditional promotion.

Please see the Tip page for more information.