You CAN can the spam

By Malinda Lingwall

Spam is the junk mail of the information age. The term “spam” is Internet slang for unsolicited commercial E-mail or unsolicited bulk E-mail. Some call this “junk E-mail” to equate it with the paper junk mail that comes through the U.S. mail. Unsolicited E-mail is E-mail that you did not request; it most often contains advertisements for services or products. Very few reputable marketers use unsolicited E-mail to advertise goods and services—instead, they send E-mail only to those who request it or those with whom they have a prior relationship.

The most common spam includes the following, many of which are illegal under U.S. federal law: chain letters; pyramid schemes, including multi-level marketing; other “Get Rich Quick” or “Make Money Fast” schemes; foreign bank scams or advance fee fraud schemes; ads for phone sex lines and pornographic Web sites; offers of software for collecting E-mail addresses and sending unsolicited commercial E-mail; offers of bulk E-mailing services for sending unsolicited commercial E-mail; quack health products and remedies; and pirated software (“Warez”).

You won’t get in trouble for receiving spam at your university accounts. Even if you’re getting blatantly illegal or prurient messages, you aren’t likely to get in trouble unless you forward them on to someone else or if you spend excessive time viewing them. (Granted, it’s embarrassing to have a colleague or supervisor come up behind you just as you’re trying to delete a message with a subject line of “FREE HOT SEXXXY PICTURES,” but he or she likely has received similar messages!)

Why am I getting spam?

Spamming is a cheap, sneaky and lazy way to try to attract customers. Spammers send millions of E-mail messages because E-mail is free to them. They guess at addresses (e.g., mary@indiana.edu, john.doe@iupui.edu) and even send thousands of messages that bounce—they don’t care, because there’s no cost to them. They usually don’t put much effort into harvesting E-mail addresses—they use
automatic programs called “bots” to scour the Web and USENET
newsgroups for addresses. Is your E-mail address on any Web pages? Do you post to newsgroups using your IU computing account? A simple
way to find out why you’re getting so much spam is to plug your E-mail
address into a search engine, such as search.iu.edu or google.com. The
number of times your address is found by the search may surprise you.
Although your IU personal home page isn’t indexed by search engines,
departmental pages and other official university Web sites are. If your
address is on one of those, it’s definitely available for harvesting.

You might also receive spam if you fill out online forms, correspond
with disreputable companies or just visit their Web sites. Although most
reputable sites have good privacy policies and won’t share your
information, some sites do share it. Some even sell your information.

IU does not and will not sell your information. Moreover, IU will not
share your information except in cases when that sharing is consistent
with the university’s mission or is required by law. For instance, IU has a
legal requirement to provide directory information, including E-mail
addresses, to the U.S. military for all eligible recruits. This information
is required under the terms of the Solomon Amendment, which requires
male students to register with the Selective Service to be eligible for
Title IV Federal Student Financial Aid.

**What can you do about it?**

The number one technique for reducing the amount of spam you receive
is to protect your E-mail address. Here are several ways you can do this.

- Do not reply to spam. When you receive spam, never reply to the
  message. Even if it says, “to unsubscribe, send E-mail to this address,”
don’t do it. Chances are you won’t be unsubscribed—in fact, spammers
often use this technique to verify that they are sending spam to active
E-mail addresses! Replying to spam may actually lead to an increase in
the amount of spam you receive. Delete the message and forget about it.
This is the least time-consuming, lowest-stress option when it comes to
dealing with spam—once it’s out of your inbox, it’s out of your life.

- Obtain a “throwaway” E-mail address. Do you fill out forms online or
  post messages to newsgroups? Whenever you buy something, register
for an account on a Web site, or post a message on USENET
newsgroups, you’re giving out information that may be used for
nefarious purposes. As mentioned above, most reputable companies
won’t share or sell your information, but the same doesn’t hold true for
newsgroups. You might choose to obtain a “throwaway” E-mail address
for these purposes. Many sites such as mail.com and yahoo.com offer free, Web-based E-mail accounts that you can access from any Web browser. If you have one of these accounts, you can use that E-mail address in online forms or messages you post in a newsgroup. You’ll still be able to get confirmation notices and other legitimate correspondence, but you won’t have to spend as much time dealing with spam in your university E-mail account.

- Read Web site privacy policies before submitting your information. Always read a site’s privacy policies before handing over your information. They’re generally long, boring, and full of legalese, but reading them thoroughly is one way to evaluate whether a company is legitimate and will handle your information appropriately.

- Don’t put your personal E-mail address on any Web pages you maintain. If you absolutely must include E-mail addresses on a Web page, modify them to make them invisible to address-harvesting robots. Learn various ways to do this in the Knowledge Base (KB) document “How can I protect my Web pages from E-mail address harvesting?”

http://kb.indiana.edu/data/alcm.html

- If you maintain a department’s or student organization’s Web site and prefer not to remove or modify the E-mail address given on the site, you may wish to request a departmental or group account to list on that Web site instead. Including a departmental or group address won’t reduce spam to that account, but it will make it seem less personal since it won’t be coming to your own account. For more information, see the KB’s “How can my IU group or department request an account?”

http://kb.indiana.edu/data/acyi.html

- Change the security settings in your Web browser. Make security as tight as possible by adjusting the settings in your Web browser. These will usually be found in the browser preferences. For a higher level of security, avoid: accepting “cookies,” listing your name and other personal information in your browser profile, and allowing your browser to fill in fields for you. This will help reduce the amount of personal information transmitted to sites. The tradeoff is that you won’t be able to surf the Web as easily—many sites require you to accept cookies before they’ll allow you to see any content. For more information about cookies, see the KB document “What are cookies?”

http://kb.indiana.edu/data/agwm.html

- Apply filters to your E-mail. IU doesn’t filter mail at a university-wide
level—we want to be sure you receive the mail you need to see.

It’s up to you to determine what you do with the E-mail that you receive. Your E-mail software or a commercial E-mail filter program can filter messages based on their subject line, the sender’s address or even the domain from which they came. You can configure your filters to automatically delete the next message from the same address, which is useful if you are receiving multiple messages from the same spammer.

However, most spammers use free accounts as throwaway accounts, because they can abandon them and move on to another when the Internet Service Provider (ISP) cancels the account due to spam complaints. You can filter out an entire ISP, but we recommend this only if you are sure no one you need to correspond with uses that ISP. If you choose to filter your mail, be aware that spammers change subject lines and addresses frequently, making it hard for filters to get the desired results. Filters are not foolproof—there is a good chance that they will accidentally filter out some messages you don’t consider spam. For this reason, filtered messages should be personally reviewed before permanently deleting them. For more information about filtering your E-mail, see the KB document “In my E-mail account, how do I filter out spam?”

http://kb.indiana.edu/data/alfb.html

- Report spam to the correct authorities. This may or may not make a difference—spammers jump from account to account, and the authorities may be able to close only one particular account while the spammer moves on to another. Before you report spam, you’ll need to know how to enable full headers. See the KB document “In E-mail, what are full headers, and how do I display and send them?”

http://kb.indiana.edu/data/akij.html

*Editor’s note: Today we give you Part I of the UITS spambuster survival kit. Part II will be printed in our next issue, Nov. 15.*

**Spambusters, Part II**
Spambusters, Part II

Got spam? Here’s how to report it, here’s what IU is doing to protect your E-mail account.

By Malinda Lingwall

(Editor’s note: This is Part II of our UITS spambusters survival kit. Access Part I in our Oct. 25 issue at this Web site or we’ll send you a copy by Campus Mail. E-mail your request to homepgs@indiana.edu).

Where to report spam

Spam that appears to come from a valid IU account: Report this to IU’s Information Technology Policy Office (ITPO). ITPO will investigate the message; if it is from someone at IU, they will identify the person and work with appropriate disciplinary authorities to stop the activity.

To report a message to ITPO, follow the Knowledge Base (KB) instructions on displaying and sending headers and forward the message to it-incident@iu.edu

Nigerian bank scams or advance fee fraud schemes: These messages usually state that a reputable foreign company or individual is needed for the deposit of an overpayment on a procurement contract. In variations of this scheme, the son or daughter of a murdered official may plead for your assistance in depositing an inheritance in a U.S. bank. Report these directly to the U.S. Secret Service. To do so, follow the KB instructions on displaying and sending headers and forward the message to: 419.fcd@usss.treas.gov.

For more information on advance fee fraud, see:

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

Pyramid, Ponzi or multi-level marketing schemes: These are the messages that often tell you that you can make $30,000 in 30 days. All three schemes are similar in that they are based on the idea that you can receive money by investing money or getting other people to join.
Report these types of messages directly to the Federal Trade Commission (FTC). To report a message to the FTC, follow the KB instructions on displaying and sending headers and forward the message to uce@ftc.gov. For more information on the FTC’s recent law enforcement actions against spammers, see:

http://www.ftc.gov/bcp/conline/edcams/spam/

**Mail that makes you feel personally threatened:** Sometimes it's difficult to tell if a message is spam or if it's targeted directly at you. If you receive E-mail that makes you feel personally threatened, contact your local police department immediately. You can find phone numbers for all campus police departments in the KB document "For each Indiana University campus, how can I contact the university police?" at:

http://kb.indiana.edu/data/akoj.html

**All other types of spam:** Report spam to the original ISP. Be sure you're sending it to the proper ISP—often, the message headers will be forged so the message appears to come from somewhere other than its true origin. For more information about determining where a message came from, see the Knowledge Base document "What should I do when I get spam E-mail?" at:

http://kb.indiana.edu/data/aknx.html

For further information on reducing the amount of spam you receive, see the KB document "What can I do to avoid receiving spam E-mail?" at:

http://kb.indiana.edu/data/adbh.html

**What is IU doing about the amount of spam I receive?**

UITS is investigating systems that block spam and E-mail harvesting without disrupting legitimate use of IU systems. ITPO has already taken steps to protect the online IU Address Book from spammers by limiting the allowed number of search results. UITS and ITPO continue to investigate global safeguards, including developing a pilot anti-spam service to which users will be able to subscribe. (If all goes well, this service is expected to debut in 2003.) As mentioned in Part I of this story in the Oct. 25 edition of Home Pages, IU doesn't filter mail at a university-wide level because UITS wants to be sure you receive the mail you need to see.

**Other ways IU helps reduce the spam**
On the central Exchange E-mail system, the number of individual recipients for each E-mail message is limited to 1,000 addresses.

IU's Online Address Book is configured to allow only 50 results at one time. This means that users must enter enough information to get fewer than 50 addresses. It is fairly difficult to write a program to harvest addresses from Web-based address books, since the program has to be smart enough to interact with the search engines on each address book. For example, you cannot search the IU Address Book unless you enter at least two letters of the last name.

For more information, see the KB document "What does Indiana University do to protect users from spam and virus-infected E-mail?" at:

http://kb.indiana.edu/data/aele.html

More information

Read what IU's KB has to say about spam at:

http://kb.indiana.edu/menu/email.html#section10

Fight Spam on the Internet! has a lot of information about spam, news articles and links to other spam-fighting organizations:

http://spam.abuse.net/

Junkbusters is one of the best sites on the Web for information on spam and other privacy invasion issues:

http://www.junkbusters.com/

The SpamCon Foundation protects E-mail as a viable communication and commerce medium by supporting measures to reduce the amount of unsolicited E-mail that crosses private networks, while ensuring that valid E-mail reaches its destination:

http://www.spamcon.org/

Stop-spam.org is another site dedicated to stopping spam. It includes ways to stop spam, what ISPs to avoid (or use) and why, and an excellent primer for learning about spam:

http://www.stop-spam.org/