worth of legal judgments against them, which they'll probably never pay, and they're still blasting away millions of spams a day. For some of them spamming is almost a sociopathic outlet. It's very hard to prove where a spam came from, and they'll get e-mail addresses any way they can. The list," he said ironically, "would be a prize."

• **Making E-mail Expensive.** One reason spam propagates is because it's so inexpensive to send it. "It costs about $200," said Cambridge, Mass., programmer Paul Graham in Technology Review, "to send one million messages." It's an effort, Graham said, that typically yields about 100 responses. If those responses equal an average of $2 each, the spammer breaks even.

One theory is that if all e-mails cost 10 cents apiece (e-mail without purchased e-stamps would be blocked), raising a spammer's cost to $1,000 per million messages, spamming would become economically unfeasible.

The Local Fight

While System Administrators for the UO and EFN (www.efn.org) don't know of much spam originating from Eugene or Springfield, they do know that a lot of spam comes into the area, and they do their best to stop it.

"In terms of e-mail system management," said VanDevender, "the greatest amount of our energy is spent blocking spam." Both EFN and the UO manage fairly aggressive spam filtering systems, using various black lists and filters. Together, these lists can stop a great deal of spam from entering your inbox.

MAPS RBL (Mail Abuse Prevention System Realtime Blackhole List), Spam Assassin, Spamhaus Black List (SBL) and the Blitz Open Proxy Monitor (BOPM) are all among EFN's defensive weaponry. Switch from AOL or Hotmail and get an account with EFN and their programs will be doing some filtering work for you. Not only that, but you'll be keeping your money local.

MAPS RBL, SBL and BOPM all keep track of known spam locations, and so EFN is able to shuttle all e-mail from those locations into a separate folder for users, marking each e-mail for a high probability of being spam. Spam Assassin takes another interesting approach to defining what is and what isn't spam before it gets to you.

The folks at Spam Assassin have decided that there's certain criteria that all spam will "often" have in common, and for each criteria an incoming e-mail meets, the e-mail is assigned points. If the point total exceeds a certain value, it's labeled spam and either returned or sent to a junk folder. For example, it seems that most spam is written in a language called HTML; if the message is 50 percent to 60 percent HTML, it's assigned .2 points. If the font size of the e-mail is large, the message is assigned .1 points. If the subject heading uses the words "ANAL GRANNIES," the e-mail is obliterated, and so on.

If spam makes it past one of EFN's filters, it still has to get through the others. Very rarely a legitimate e-mail will be filtered out, and at that point a user will ask EFN to adjust filtering on a particular account to avoid future errors. Users such as yourself can wield a heavy hand in the melee, by following simple suggestions and using simple tricks. Master them, and you'll be, like me, a step closer to mastering spam. Until then, do your best to put up with it, and choose your replies carefully. **EW**

Mainsleazers: For money they'll do an e-mail marketing campaign for your company. They'll send spam out for you, your company gets a black eye and the mainsleazer moves on to another unsuspecting client. Bad mojo.

E-MAIL WORMS: Spammer viruses that can install unauthorized proxie software onto a host system. Then millions of emails can be sent through the system. Your system.

SPIDERS: Web crawling programs that search the net for unguarded proxies. Didn't I see one of these in *The Matrix*?

DICTIONARY ATTACKS: Spammers use software opening a connection to a victim's mail server. They automatically submit millions of random addresses and record which addresses succeed. These are then added automatically to the spammer's list, and can be resold to spammers worldwide.

CHICKEN-BONERS: People spamming from some inexpensive location, such as a trailer park.

SPOOFING: Showing a fake route or return address in order to conceal where an e-mail originated.

PHISHING: Spamming and scamming to get account and credit card numbers. Don't give 'em out!

419 SCAMS: Spam e-mails named for the Nigerian legal code supposedly making them illegal (even though the government is suspected to be involved) "introducing" you to a wealthy foreigner who's having trouble getting money out of his or her country. The individual needs your account information and promises a huge cut if they can smuggle money into your account. Give 'em your data and it's *your* money that gets the chop.

RATWEAR: Software designed to exploit open proxies.