
e-Mail Spam

Consumer Reports: August, 2003 (Copyright © 1999-2003 Consumers Union of U.S., Inc.)

How to stop it from stalking you

- **How They Find You**
 - **Behind the Spam**
 - **Internet Providers as Blockers**
 - **Spam-Blocking Software**
 - **Winning the War**
 - **AOL Graph: Spam on the Rise**
-

The battle between those who send unsolicited e-mail advertisements, commonly known as spam, and those blocking them has become an arms race. On one side are hordes of spammers who find ways, through technology and guile, to penetrate consumers' inboxes, for example by misspelling telltale words like "V1agra" (for Viagra) or "D E B T" (for debt).

On the other side are Internet providers with industrial-strength spam-blocking software, vigilante organizations that blacklist spammers, and consumers armed with retail spam-blocking programs. This side is losing. Big time.

Between February and April 2003 alone, according to America Online (AOL), the maximum number of messages that spammers had lobbed toward the service's 35 million customers in a single day tripled, to 2.4 billion. (See "Spam on the Rise," below.) A typical day's volume averages about 1.5 billion. And those are just the ones AOL blocks and deletes. The service averages 7 million complaints daily about spam that reaches customers.

Indeed, spam volume throughout the Internet has grown so much that it is about to overtake that of legitimate e-mail. It's even expanding beyond computers, invading cell-phone text messages (see "Spam's New Frontier," below). In Japan, cell-phone spam is widespread, according to the country's largest carrier, NTT DoCoMo. Roughly one-sixth of the customers the company surveyed said they receive one to five cell-phone spams daily.

At the heart of the spam slam is money: Spamming is far cheaper than conventional mail. Spammers can broadcast a million messages for as little as \$500. If even a few recipients buy what's advertised, the campaign most likely pays.

But spam imposes heavy costs on most consumers, who must spend time sifting through all that junk and can feel violated when pornographic spam invades their home. They can miss out on legitimate e-mail that's mistakenly blocked from delivery by their Internet provider or that they themselves delete in the course of eradicating spam.

Most spam is also deceptive, the better to sneak past your provider, trick you into opening it, and separate you from your money. When the Federal Trade Commission recently examined

spam forwarded by consumers, it found that nearly two-thirds contained false information. Last year, the FTC found that only about one-third of requests to be taken off spammers' lists were honored.

Can anything stop spam and those who send it? Who is behind this pollution of the information superhighway? *Consumer Reports* investigated to find out.

We ferreted out many of the ways in which spammers find you, then figured out how to elude them. We examined hundreds of spam e-mails received by our staff, tracked down some spammers online, set up decoy addresses to attract spam, and examined the spam-blocking practices of major Internet providers.

We attended government hearings, interviewed consumers who had experienced spam-related intrusions into their lives, and collected hundreds of spams in our labs to test blocking software for the home. We also tested the e-mail program that comes with every new Macintosh.

The best news our research unearthed is that spam-blocking software works, but to varying degrees: All 11 products we tested recognized at least 40 percent of the junk; the best identified 90 percent or more. (For details, see the [Ratings](#) and [CR Quick Recommendations](#).) We found, too, that a little ingenuity can go a long way; see [What you can do](#).

But we also concluded that it may take years to control spam's overall growth. Not all companies have policies curbing their marketers from using spam. Companies with policies often can't enforce them because they can't monitor the mailing lists. As we went to press, 33 states had laws regulating spam. Many, however, simply require messages to be labeled as ads. An exception: Virginia's law, enacted in April, provides up to five years' jail time for those who send more than 10,000 deceptive messages in a day.

There is no federal law against spamming. Three have been proposed, but even if passed those may not be effective. That's because taking legal action against perpetrators can be extremely difficult.

The bottom line: Spammers need your money to stay in business. Our advice to anyone who doesn't want spam is don't buy anything sold through spam. Don't respond to spam. Don't even open it.

How They Find You

Here are four common ways in which spammers get your e-mail address:

- **Public Web pages.**
 - If your address appears on a public Web page, spammers can automatically "harvest" it using widely available software. Ads for one product say that it collects thousands of addresses hourly and is "so simple a 12-year-old could

- learn how to run it in 15 minutes."
- The Center for Democracy & Technology, a Washington, D.C., advocacy group, recently posted 250 new e-mail addresses publicly. Within six months, it received more than 10,000 e-mails, mostly spam. We tried a smaller-scale test, putting four new addresses on public Web pages. One received its first spam within six days.
 - Chat rooms.
 - Use your e-mail address in these groups and you're a target. When we used a newly minted e-mail address in several AOL chat rooms, we received our first spam within 25 minutes.
 - "Dictionary" attack.
 - Some spammers send e-mail to many addresses using combinations of names and numbers, such as John101, John102, etc. If you reply, or in some cases even read the e-mail, the spammer knows the address is valid. To determine how your e-mail address affects how readily such spamming can reach it, we created short addresses and longer, harder-to-guess ones with five large Internet providers. Within 6 to 12 weeks, spammers had found some of our short addresses but none of the long ones.
 - Online registration.
 - Disclosing your address when shopping online can unwittingly bring spam. The riskiest sites are those with no privacy policy, a statement that tells you what information the site collects on you and with whom it may share it. But even a site that posts a policy can be risky if the policy allows for sharing your address with unnamed "partners."

Behind the Spam

Much of the spam that consumers receive is sent by bulk e-mail services on behalf of clients selling everything from credit cards to Viagra. To prevent their outgoing transmissions from being blocked, bulk e-mailing services sometimes use computers based abroad.

In April 2003 we visited the Web site of, and reviewed promotional literature distributed by, one such service, BulkingPro.com. A third party had used the New Jersey-based company to spam a staff member.

One BulkingPro.com sales pitch tells prospective customers: "Don't expect to make large profits if you aren't mailing 1-3 million emails/daily (at least!)." The company says it will send bulk e-mail for customers from its own computers based outside the U.S. Clients receive technical support via a toll-free number; online chat-based support via systems like AOL and MSN Messenger; and monthly improvements to the e-mailing system, such as the ability to "penetrate tough domain filters and spam blocking techniques."

BulkingPro.com's head, Peter DeCaro, told us that his company's services are not intended to be used to hide identities or abuse Internet resources. But BulkingPro.com's Web site and literature offered precisely what spammers want: updated lists of Internet-based relay and proxy servers, the kind of computers spammers commandeer to transmit e-mail

anonymously; e-mail address "harvesting" software; the ability to insert random characters into e-mails to foil spam-blocking software; and, the literature says, "other new tricks to get past aggressive domain filters."

Bulkingpro.com's site offered a \$299 "Bulkers Bundle" featuring 50 million addresses ("We harvested these and verified them ourselves!"), including those of 12 million AOL users ("verified twice in past 4 months") and 8 million MSN users.

Not all spam is sent by anonymous marketing companies using offshore computers for clients whose products you've never heard of. Some marketers, we found, send spam on behalf of household name brands, a number of which have policies prohibiting spam marketing. But the chain of contractors and subcontractors linking the promotional e-mails to the brand-name company can be so long and tenuous that the company can't enforce its own policies.

For example, a member of our staff received an unsolicited e-mail promoting a MasterCard from Morgan Beaumont, a Sarasota, Fla., marketing company.

MasterCard International, whose brand name appeared in the e-mail, ought to have a tough, effective anti-spam policy. After all, the company is a member of the Council for Responsible E-mail, within a subsidiary of the Direct Marketing Association.

In fact, Veronika Clough, a MasterCard spokeswoman, said the company has no spam guidelines. She said that it relies on those that market MasterCard to "follow local laws. If someone thinks there's a violation, they should go to law enforcement."

Cliff Wildes, Morgan Beaumont's president, said its contracts with Internet marketers prohibit spamming and that it will terminate its relationship with any it finds spamming. But Wildes also noted: "We can't trace who gets the ads. I get an ad for a Sony Walkman, I can't call Sony and ask how they got my name."

Wildes couldn't identify who had sent the unsolicited e-mail we received. He noted that Morgan Beaumont works with "three big marketing companies" and as many as "10,000 agents and affiliates."

Other high-profile companies we contacted about unsolicited mailings that our staff had received have policies against spamming. But they were unable to trace those mailings with enough precision to identify any business relationship with the recipients. A spokeswoman for AT&T Business, in whose name a marketing firm had sent e-mail to an address that, we believe, could have been obtained only through spammer-style Web-site harvesting, attributed the mailing to a processing error.

Will Jerro, the CEO of ReliaQuote, an insurance service that had e-mailed a CR editor, traced the message in question to a partner that had contracted with another company, which actually sent the e-mail. "We have relationships with hundreds of different

companies," he said.

But control is an issue even when relationships are more limited. For example, Consumers Union, the publisher of *Consumer Reports*, deals with only a handful of vendors. CU opposes the use of spam and does not knowingly spam consumers. CU makes its e-mail marketing policies known to vendors who communicate with consumers by e-mail on our behalf. Still, we are currently undertaking a thorough review of our contracts with outside companies to strengthen our controls and to ensure that spam isn't sent in our name.

Internet Providers as Blockers

Your Internet provider is your first defense against spam. Here's how:

- AOL. It automatically blocks billions of spams daily. You can sort your mail into those from senders you know and those from strangers. There's also an onscreen button that removes offending e-mail.
- EarthLink. Optional blocking lets you inspect blocked mail; with an optional system, someone sending you an e-mail must respond to a system message before the e-mail goes through. This helps stop computer-generated spam, but it requires more effort from you and those sending valid e-mail.
- MSN. You can tell the service to block spam automatically. There's an onscreen button that removes spam.

Spam-Blocking Software

Some e-mail programs can weed out spam that your provider doesn't catch. Two widely-used ones that we tested, Microsoft Outlook and Apple's Mac OS X Mail--which comes with new Macs and Apple's OS X operating system--were good overall. But Outlook was only fair at recognizing spam, and Mac OS X Mail was only fair at recognizing legitimate e-mail.

Ideally, spam-blocking software should do both tasks well. Several add-on programs we tested, which work in tandem with most popular e-mail programs, fared far better than Outlook or Mac OS X Mail.

Winning the War

Blocking the daily spam consumers now receive is only a temporary fix. A long-term solution requires a combination of technological, legal, and consumer action.

Without strong federal laws, authorities face formidable obstacles. Few state laws have been used to take action against spammers. Delaware, whose law has been on the books since 1999, has yet to press charges against anyone.

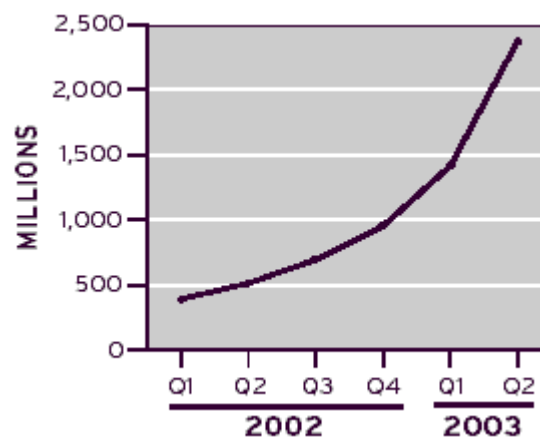
"It's extremely difficult to investigate and prosecute spammers," says M. Jane Brady, Delaware's attorney general. "You get multiple servers; anonymizers; mail coming from Korea, Russia, the Islands--and no one at the end of the trail when we got there." Her office,

she said, plans to "follow the money" instead, pursuing those receiving fees for referring people to the Web sites promoted in spam.

One Senate bill, the CAN-SPAM Act of 2003, requires unsolicited commercial e-mail to be labeled as such and carry truthful information. But in April 2003, 44 state attorneys general wrote Congress opposing the bill because it might pre-empt even tougher state laws.

In April 2003, Consumers Union joined a coalition of anti-spam advocates in opposition to the bill because it lacks two provisions included in the Telephone Consumer Protection Act of 1991 (which banned junk faxes): an opt-in rather than opt-out policy and a provision allowing consumers to sue spammers for damages up to \$500.

Spam on the rise



Quarterly, from March 2002 to June 2003, the peak number of daily spam e-mails detected and blocked by America Online.

Source: America Online