



'Print this' sponsored by

Soaking In Spam

The Net is buckling under the weight of billions of unsolicited bulk e-mail ads. Current weapons aren't working—but there's hope. A report from the front lines

By Brad Stone

Newsweek International

Dec. 8 issue - Scott Richter doesn't mind telling you how successful he is. His 28-employee company, OptInRealBig, clears \$2 million in sales each month. He drives a Lexus convertible and a Lexus SUV, owns a half-million-dollar home outside Denver, Colorado, and just returned from vacation on the Caribbean island of Anguilla. But the 32-year-old former restaurateur has made his small fortune in an unpopular way: sending out 80 million e-mail advertisements a day. He hawks diet pills, porn sites, sexual aids and miracle products. He's also impulsive and resourceful. During the Iraq war he churned out ads for copies of the Pentagon's Most Wanted playing cards.

ALTHOUGH RICHTER practices a reviled occupation on the Net, he says he never makes false claims in his ads and that there's nothing wrong with unsolicited bulk commercial e-mail messages, or spam. He's also confident that bulk e-mailers are immune from new laws and lawsuits. "We can set up in another country within an hour," he says. "There are people in other countries who would love to sell us bandwidth."

Richter's insouciance and general visibility—his phone number is posted on his Web site—suggests an unpleasant fact about the eternal cat-and-mouse game that the Internet's spam war has become: the nefarious mouse is winning, and it's not even a close race. In the past two years spam has congested the Internet, threatened to overwhelm Internet service providers and sent Web surfers of sensitive disposition scampering away from their computers in embarrassment. Spam is now approaching 60 percent of all e-mail, according to the research firm Gartner Group. Ferris Research says spam puts a \$9 billion annual drag on productivity.

The forces who say they hate spam—politicians, tech companies, beleaguered e-mail users and anti-spam vigilantes who spend their own time and money trying to clean up the Net—haven't managed to make a dent in the problem. Current approaches aren't working; even though home users and many companies started filtering their e-mail two years ago, the overall amount of junk mail has ballooned exponentially. Filtering and antivirus companies always seem one step behind the rapidly evolving methods of clever spammers. And most individual lawsuits against spammers have been defeated, settled or concluded with penalties unpaid and bulk e-mailing operations open for business.

Can anything be done? Reports from the front lines of the spam war show how traditional anti-spam tools are outmatched and suggest some promising solutions.

Filtering: Even when spam never finds its way to individual e-mail accounts, it creates havoc for Internet companies. Servers at AOL and Microsoft sag under the weight of a billion blocked spam messages each day; smaller ISPs that get fewer messages suffer even more. Barry Shein is the founder of The World, a small Internet service in New England. One day last week Shein arrived early at work to spend three hours personally sifting through his jammed e-mail servers and deleting thousands of messages his filters caught. With so many flagrantly illegal spam techniques, Shein wonders why no one is slapping handcuffs on spammers. "Imagine being dragged out in front of your house and beaten every day in front of your neighbors, and the police won't respond to it," he says. "That's what this feels like."



Using e-mail filtering tools helps companies and individual users block spam, but it's not perfect. CipherTrust, an Atlanta, Georgia-based anti-spam firm, makes software that hunts for specific words, blocks the addresses of repeat offenders and analyzes message headers for telltale spam signs. CipherTrust engineer Steve Davis reviews the dozens of unwanted messages sent to his own protected e-mail account that morning. Messages promoting work-from-home schemes ("Attention Moms!") and junior-college programs ("Degree Programs That Fit Your Life!") get successfully blocked.

But another message, masquerading as an important upgrade from Microsoft and carrying a virus, gets through the CipherTrust filter. The message is similar to a legitimate customer-service message, and was not sent by any known spammer, and doesn't fit any known pattern. In other words, an ingenious spammer somewhere in the world knows exactly what filters look for and has found a new way to evade them. "We are trying to hit a target that is coming at us from all directions and moving at the speed of the Internet," Davis says.

The virus that made it through represents a new and deleterious kind of spam: it seeks to turn a PC into an unwitting bulk e-mail generator that remotely does the spammer's bidding. In the past few weeks more and more of these so-called spam zombies have been turning up.

Prosecution and legislation: The European Union has banned e-mail marketing without prior consent, and an anti-spam bill is making its way through the U.S. Congress. But many experts doubt these measures will have much of an impact. Even zombie attackers are avoiding capture because it's so difficult to trace the origin of spam back through hijacked computers and abandoned Internet locations. And at overworked law-enforcement computer-crime divisions, e-mail fraud takes a back seat to kiddie porn and identity-theft cases.

New approaches: The best way to solve the problem may be changing the very architecture of e-mail itself. Internet-standard-setting bodies are looking at ways of revising the code for delivering mail so ISPs can check whether incoming e-mail is faking its origin. But those changes would take years to trickle down into every network around the world. In the shorter term, "challenge/response" systems let users send direct messages only to people who have the sender in their address books. When you e-mail a stranger, the system sends back a puzzle that only a human, not an automated spam program, can solve; give the correct response, and the e-mail goes through. Another system, dubbed micropayments, would charge a tiny amount for each e-mail sent, and would add up to large sums only for bulk e-mailers. These solutions may conflict with the original spirit of the Internet, but they're among the few reliable ways to foil spammers and fraudsters. The bathwater might be gone, but in an age of ever increasing junk-mail volumes, the greater challenge is to save the baby.

With Dan Weil in Boca Raton, Florida

© 2006 Newsweek, Inc.

URL: <http://msnbc.msn.com/id/3606138/>

© 2006 Newsweek, Inc.