Filters getting better at blocking spam

The Boston Globe

Security firms say junk e-mail abounds, but less of it reaches your inbox

By Hiawatha Bray, Globe Staff | April 11, 2009

You might not believe it after glancing at your e-mail inbox, but professional spam fighters say they're making progress in the war on digital junk mail.

Billions of unwanted spam messages continue to flood the Internet; indeed, spam now accounts for about 90 percent of all e-mail traffic, according to e-mail security officials who attended a conference on spam held late last month at the Massachusetts Institute of Technology. But improved filtering technology means that the great majority of these messages never arrive at their destinations. And last year saw the shutdown of several major spam senders.

"This is not an impossible problem to solve," said Garth Bruen, chief executive of Knujon, an e-mail security company in Wilmington, Vt., whose name is "no junk" spelled backward.

The federal CAN-SPAM Act of 2003 hasn't been much help. The law was intended to put a crimp in spamming activity, but it lacks teeth, according to Nilesh Bandhari, a product manager at Cisco Systems Inc.'s Ironport e-mail security service. "The penalties have not been se vere enough to prevent others from sending spam out," Bandhari said. Besides, a US law can't do anything to halt spammers based in other countries.

But private citizens are finding ways to slam the spammers. Bruen pointed to last year's shutdown of McColo, a California company that was one of the world's leading senders of spam. Goaded by evidence compiled by Knujon and other antispam researchers, two major Internet providers stopped doing business with McColo, knocking the company offline. Overnight, worldwide spam output dropped about 75 percent, according to Ironport's spam-tracking survey.

But it was a relatively short-lived victory. Bandhari said spam volumes have returned to the levels of last summer, before McColo was shuttered. He added that spammer shutdowns were "something that can be successful in the short term," but "in the longer term, it's not a silver bullet."

Bruen and his father, Robert, cofounder of Knujon, are trying to remove the profit from spam. Most spam messages contain Web addresses, so the recipient can go to a website to make a purchase. Web addresses are purchased from a company called a registrar. Spammers provide the registrars with false names and street addresses to make it harder for law enforcement agencies to track them down.

Knujon is pressuring the Internet Corporation for Assigned Names and Numbers (ICANN), an Internet governance group, to force registrars to demand accurate information from purchasers of Web addresses. This would make it far easier to put spammers out of business. Already, said Bruen, pressure from ICANN has caused two domain registries, one in Germany and the other in China, to largely eliminate their sales of domains to spammers. "It's been slow, but we are getting progress," said Bruen.

Meanwhile, individuals and businesses are finding it easier to avoid the torrent of unwanted e-mails. Improvements in filtering technology mean most spam never arrives in the target's inbox. "A lot of the big ISPs (Internet service providers) are actually handling it pretty efficiently," said Michael O'Reirdan, an engineer at a major ISP and chairman of the Messaging Anti-Abuse Working Group, an association of antispam experts from a variety of major Internet companies.

Companies like Cisco's Ironport kill much of the spam simply by tracking its source. When the company intercepts spam, Ironport notes the Internet address of its origin. If the same address keeps turning up, Ironport assigns it a "bad reputation," and stops incoming mail from that source. Cisco claims that this method can eliminate up to 80 percent of all spam.

Meanwhile, researchers continue to improve filtering programs that analyze the words and images in e-mails to decide whether to let them through. Bill Yerazunis, senior research scientist at Mitsubishi Electric Research Laboratories in Cambridge, helped create the CRM114 Discriminator. This spam filter, named after a communication device in the Stanley Kubrick film "Dr. Strangelove," is designed to be self-improving. The more e-mail fed into the filter, the better it gets at spotting spam. "I haven't had an error this year," Yerazunis said.

Other companies, like Sendio Inc. in Irvine, Calif., and Spam Arrest LLC of Seattle, use a "challenge-response" technique. Send an e-mail to a challenge-response user and you'll get an automated reply, asking you to type in some words or numbers. This will prove your e-mail came from a human being and not a spam-spewing computer. If you send the correct reply, all your future messages are delivered immediately, but spam messages can't get through.

Armed with these tools, e-mail users can now avoid the great majority of incoming junk e-mails. But that doesn't mean the battle against spam is won. "Is it going to go away? I can't say that," said Adam Swidler, product marketing manager of Postini, an antispam service owned by Internet search giant Google Inc.

Filters or no filters, spam remains an effective sales tool. The British research firm Marshal Ltd. claimed last year that 29 percent of Internet users had purchased products from spammers.

Hiawatha Bray can be reached at bray@globe.com. ■
