

July 2004
 No. 15

The CAN-SPAM Act of 2003: A Six-Month Progress Report

Contact Mark Schirmer at 502-564-2851 or mark.schirmer@lrc.state.ky.us

The quantity of spam—and the cost to combat it—continue to rise.

The CAN-SPAM Act overrode all state spam laws.

E-mail harvesting continues unabated in spite of CAN-SPAM.

Opting-out actually increases illegal spam.

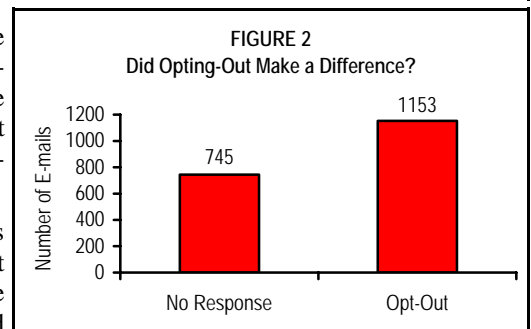
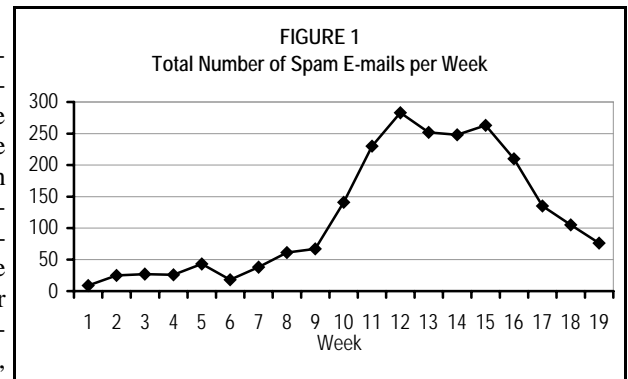
“Spam” has emerged as the electronic albatross of the digital world, stuffing inboxes with e-mails hawking mortgages, pharmaceuticals, pornography, and all manner of too-good-to-be-true “miracle” products. Given that 87 percent of Kentuckians have Internet access—and therefore access to e-mail—the problem is as local as it is global.¹

Beyond mere advertising, spam has also become the preferred method for virus distribution, swindles, and identity theft. In short, spam is no longer simply a nuisance; it’s a serious, expensive problem. Spam could cost the U.S. economy an estimated \$10 billion this year in lost productivity and expenditures for spam-filtering software,² though Microsoft’s Ryan Hamlin suggested a year ago that businesses might spend upwards of \$18 billion on filtering software and storage hardware *alone* in 2004.³ To combat the threat of viruses and compromised security, public agencies and private businesses now routinely purchase costly server and software upgrades. And the predicament continues to worsen. As of April 2004, spam accounted for 67 percent of all global e-mail activity and 83 percent of all e-mail sent to U.S. destinations.⁴

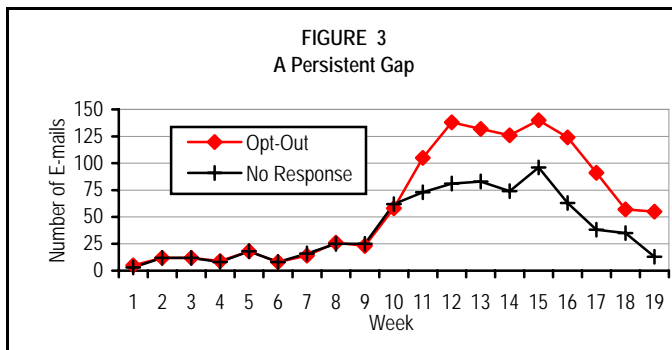
By the end of last year, 36 states had anti-spam laws either in place or about to go into effect. In Kentucky, an anti-spam bill was prefiled for the 2004 session of the General Assembly, but tabled because the federal Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act superseded all state spam laws when it went into effect January 1, 2004. One question looms large: *Can CAN-SPAM can spam?* Here, we offer a six-month progress report on the federal law based on findings from a Center study and provide some suggestions about what Internet users can do to reduce the spam they receive.

The CAN-SPAM Act specifically prohibits its electronic harvesting or gathering of e-mail addresses from the Web. To gauge whether “spammers” were heeding the law, we placed 11 e-mail addresses on selected government Web pages in mid-February 2004.⁵ We formatted these addresses so they would be invisible to the human eye but conspicuous to computer programs designed to harvest e-mail addresses illegally. By the end of June, these dummy addresses had received a total of 2,258 spam e-mails (see Figure 1). Figure 1 suggests that the illegal harvesting of e-mail addresses has continued at a strong pace, though the volume of e-mail traffic has dropped off in recent weeks. Perhaps even spammers take summer vacations.⁶

The efficacy of CAN-SPAM rests largely on its opt-out provisions. All commercial e-mails must offer recipients the opportunity to opt out of future e-mailings, either via e-mail or an Internet-based mechanism; e-mailers are required by law to honor these requests. Four of our hidden addresses sent opt-out replies to all the e-mails they received; four control addresses

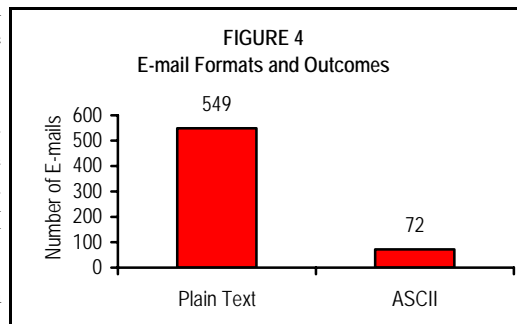


ignored everything. Did opting-out make a difference? Yes, it did. It attracted more spam. As Figure 2 illustrates, the opt-out addresses received 1,153 messages, while the comparison addresses received only 745 e-mails. The two groups showed little difference until week 11. When the amount of spam began to increase, so too did the gap between the Opt-Outs and the No Responses (see Figure 3). The persistent gap in Figure 3 demonstrates that CAN-SPAM's opt-out provision has had the opposite of its intended effect.



ASCII addresses were less susceptible to harvesting.

We created nine of our experiment's e-mail addresses in plain text, but encoded the remaining two in ASCII, a computer code that transforms ordinary text into numerical representations: "this," for example, appears as "this".⁷ As seen in Figure 4, the two ASCII addresses received 72 spam e-mails compared with the 549 received by the two comparison addresses. Spammers are nothing if not adaptable, leapfrogging new anti-spam measures, so using ASCII might not make a bit of difference six months from now.⁸



Spam filters can help, but choose and use them carefully.

A completely foolproof spam filter—one that blocks all spam and lets in all legitimate, desired e-mails—has yet to be invented. There are extremely accurate spam filters, but some CAN-SPAM-compliant firms sending legitimate, legal (though perhaps unwanted) marketing e-mails often find themselves on the wrong side of the filters. Legal action on the part of these law-abiding businesses seems almost predestined.

Use ASCII for e-mail addresses.

Being on the Internet makes any e-mail address a spam magnet. If an address must be published online, create it in ASCII, which can be done with an e-mail encoder.⁹

Do not "opt out."

Though it seems counterintuitive, spam intake can be reduced by *not* opting-out. Unscrupulous spammers use opt-out requests to confirm the functionality of e-mail addresses.

Attached files might contain computer viruses.

Resist the urge to open attached files, even if they're included in e-mails from people you know, but especially if they're sent by strangers. Seek some confirmation that an attached file is legitimate before you open it or you're liable to infect your computer with a virus and possibly convert it into a spam transmitter or relay.¹⁰

Make yourself a moving target.

An increasing number of Web sites offer disposable e-mail addresses, which enable a single user to have multiple addresses, with all incoming messages forwarded to a single address. As one disposable address begins to receive spam, shut it down and create another disposable address. Because disposable e-mail addresses probably aren't feasible for businesses and government agencies, it's important that people reserve their professional e-mail accounts for professional purposes only. Separating business and pleasure reduces the demands placed on an organization's computer resources, freeing them for their intended usage.

CAN-SPAM has yet to prove itself.

CAN-SPAM offers a legal remedy rather than a technological one. As such, its effectiveness will not become fully apparent until a number of spammers have been successfully prosecuted, which could take years.¹¹ By being opt-out-oriented rather than opt-in-oriented, CAN-SPAM essentially legalizes some types of unsolicited commercial e-mails and offers windows of opportunity during which spammers can continue to clog inboxes. Indeed, the results of this six-month progress report suggest that the legal remedy is less than perfect, at least for now. For the immediate future, our best hope in combating spam lies in technological savvy—ever-improving spam filters and wise use of the Internet.

¹ This estimate is from the University of Kentucky Survey Research Center Spring 2004 Kentucky Survey. Households were selected using a modified list-assisted Waksberg-Mitofsky random-digit dialing procedure, which ensures every residential telephone line in Kentucky has an equal probability of being called. Calls were made from April 14 until May 17, 2004. The sample includes 831 noninstitutionalized Kentuckians 18 years of age or older. The margin of error is approximately ± 3.4 percentage points at the 95 percent confidence level. ² Anita Ramasastry, "Why the new federal 'CAN Spam' law probably won't work," 5 December 2003, online <<http://www.cnn.com/2003/LAW/12/05/findlaw.analysis.ramasastry.spam/>>.

³ Joris Evers, "Microsoft: Spam can be contained within two years," 30 May 2003, online <<http://www.computerworld.com/softwaretopics/software/groupware/story/0,10801,81677,00.html>>. ⁴ Bob Sullivan, "Now, two-thirds of all e-mail is spam," 22 May 2004, online <<http://msnbc.msn.com/id/5032714/>>. ⁵ For a more detailed description of our experiment, please see the Technical Appendix at <www.kltprc.net/policynotes/pn15techinfo.htm>. ⁶ The first week in July—Week 20—saw the volume of spam begin to increase once again, matching the amount received during Week 17. ⁷ Special thanks go to Jim Swain, CIO of the Legislative Research Commission, for suggesting the use of ASCII and for creating the actual code. ⁸ Case in point, in an extensive six-month study published last year, the Center for Democracy and Technology seeded the Internet with hundreds of spam-baiting e-mail addresses, including some created with ASCII. Out of all their ASCII-encoded addresses, none received a single piece of spam. ⁹ Run a Google search for "email encoder" and you'll find plenty. Avoid online converters that require registration or send the code via e-mail. ¹⁰ By using compromised computers to send or bounce e-mails, spammers can move from machine to machine, covering their tracks as they go and making it look like someone else is sending their spam. ¹¹ To report the illegal spam you receive, visit <<http://www.ftc.gov/spam>>.