Spam: 
Unsolicited commercial electronic mail

In a Harris Poll released in January 2003, 75% of all internet users thought the federal government needed to pass a law banning spam. Referred to officially as unsolicited commercial e-mail, spam has grown from simply being an annoyance, to imposing serious costs and inconvenience to individual users, businesses, and service providers. Estimated costs have reached $8.9 billion to U.S. corporations, $1.5 billion for European, and an additional $500 million for both continent’s service providers. Korea has launched a serious enforcement effort against spammers where penalties can reach $8,500 in fines or two years in prison. In the United States, 29 states have passed anti-spam legislation, but with little effect.

The costs involved are often difficult to measure. By clogging the e-mail system with unwanted traffic (in the case of AOL spam constitutes as much as 50% of their traffic), businesses and service providers are forced to add more bandwidth and storage. Staff time is diverted to deal with the problem, and even though there are technical solutions available, they are expensive and require a great deal of maintenance. Liability issues arise as users feel harassed by obscene messages. Employees increasingly consider it a security issue, feeling the sanctity of the workplace is being invaded. In Korea, one third of domestic hacking attacks on mail servers were blamed on spam artists.

A variety of solutions have been attempted, but increasingly there is realization that any effective action needs to be combined with federal legislation that can set the stage for international agreements. Technological innovation has greatly reduced the volume of unwanted e-mail for corporations who can afford it. The problem with technology alone is that spam producers follow quickly on the heels of innovation with adjustments of their own, leading to a continual escalation of efforts. Efforts many feel would be better placed solving other problems. Technology faces the equally difficult risk of filtering out important messages by mistake. “False positives” could lead to individuals doubting the reliability of e-mail and diminish the medium’s ultimate value.

Significance for EDUCAUSE members:
In reaching their goal of providing secure, reliable and affordable computing systems for their campuses, spam is an increasing problem for EDUCAUSE members. In-house solutions tap resources that are already being stretched, and state laws are ineffective for a crime that is interstate and international. Well-written and strongly enforced federal law could help take the pressure off campus ISP’s and allow them to use their resources elsewhere. As users of legitimate mass-e-mailing marketing techniques, campus administrators must be assured that this medium is still available to them.
Current EDUCAUSE position:
In their role of protecting consumers, the Federal Trade Commission and the Attorney General’s of New York, California, and Washington have launched successful prosecutions of know spammers. While many feel this is a futile effort, it has raised the awareness of the problem and garnered support for more uniform and easily enforceable laws. The Direct Marketing Association (DMA), once strongly opposed to anti-spam law, now supports federal legislation that would enforce the e-mail marketing industry best practices:

- An honest subject line.
- No forging of headers or technological deceptions.
- Identity of the sender, which includes a “physical” address.
- An opt-out that works, is easy to find, easy to use and has a standardized format that records the date and URL opted-out of.
- No harvesting of email addresses via automated mechanisms without consent.

In addition, the DMA wants any federal spam law to preempt state law, and provide both civil and criminal penalties.

The DMA approach has received initial support in Congress and protects the ability to market using e-mail in a responsible way. EDUCAUSE feels it is a reasonable place to start and that it could build a foundation for eventual international agreement.

Lead Government agencies/departments/contacts:
Any new legislation would have to be introduced and passed in Congress. Currently the bills that seem most likely to progress are the “CAN-SPAM Act of 2003,” Senate Bill 877, and the “Reduction in Distribution of Spam Act of 2003,” House Resolution 2214. Both bills have very broad support in Congress as well as among ISP’s and the direct marketing industry. The FTC would be the regulatory agency responsible for enforcement. It currently can prosecute fraudulent spam and Internet scams under its deceptive and unfair trade practices mandate.

Resources:
Telecommunications Research and Action Committee “Ban the Spam” campaign: [http://trac.policy.net/banspam/](http://trac.policy.net/banspam/)
EDUCAUSE Resources:
Wendy Wigen, EDUCAUSE Policy Analyst, wwigen@educause.edu
Legislative Tracking Chart: http://www.educause.edu/ir/library/excel/net0015a.xls
Information Resources Library: http://www.educause.edu/ir/ir-library.html

Last updated 6/3/2003