This series of articles looks at how we can use e-mail and other electronic communications responsibly and professionally. It is intended to provide useful information for corporate INFOSEC awareness programs.

* * *

There are plenty of ways of marketing products and services electronically without offending anyone, violating standards of civility, or breaking the law. Using the World-Wide Web is one; generating and using legitimate, opt-in e-mail lists is another.

However, there are at least three types of unwanted messages: unsolicited commercial e-mail (UCE), usually called “junk e-mail” and sometimes known as “spam” (much to the horror of the trademark owners for “Spam” luncheon meat); chain-letters; and hoaxes.

Employees who are new to the Net may think naively that sending advertisements to millions of recipients at little or no cost sounds like a great deal. Certainly thousands of gullible nitwits have fallen prey to charlatans selling systems for sending out junk e-mail; many of these novices unthinkingly accept the notion of forging e-mail headers to avoid the consequences of their actions. However, no reputable organization will permit such abusive behavior; junk e-mail puts the organization into bad company, uses the recipients’ resources (bandwidth, disk space, time) without permission, and generates outrage from many of the victims. That outrage can take both legal and extra-legal methods.

A notorious case of header forgery came to light in May 1997, when Craig Nowak, a college student, chose a return address at random for his first attempt at junk e-mail. Unfortunately for his victim, “flowers.com” was a legitimate business whose owner received 5,000 bounced messages and plenty of abuse for supposedly spamming the world. Fortunately for the anti-spam cause, the enraged florist, Tracy LaQuey Parker, launched a lawsuit for damages and was supported by the Electronic Frontier Foundation and the Texas Internet Service Providers Association. In late September 1997, the plaintiffs won a temporary injunction against the defendant and his ISP preventing him from further use of the appropriated domain name (not that he'd have wanted to, at that point). In November 1997, the defendant was fined $18,910 plus court costs.

A different sort of response occurred in 1994. In the December issue of Network World an anonymous writer told the following story. Without knowing that he was violating standards, he posted a message about his company’s products on about a dozen USENET groups. Within hours, he was swamped with abusive e-mail, abusive USENET group messages, and – worst of all – his company’s 800 number was widely posted in alt.sex groups as if it were a free phone-sex line. The volume of calls (all of which were paid for by the company) by sex-seeking callers...
not only saturated the company’s phone lines, but also annoyed the receptionists to such an extent that one of them resigned and the other forwarded all the 800-line calls to the phone of the employee who started the whole mess. The 800 number had one of those fancy letter combinations and it was all over the company’s advertising and letterhead, so changing the number was not an option; the company simply had to wait for the fuss to die down.

These cases are good enough reason to convince most sensible employees that sending junk e-mail is (shall we put it mildly?) not a good idea for their employers or for their careers.

* * *

Mich Kabay can be reached by e-mail at <mkabay@atomictangerine.com>. He invites inquiries about a wide range of information security courses and INFOSEC consulting services that he and his colleagues at AtomicTangerine would be delighted to deliver to your employees at your site and at your convenience. For information about AtomicTangerine, visit <http://www.atomictangerine.com>.

Copyright © 2000 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.