

Protecting Your Reputation in Cyberspace*

M. E. Kabay, PhD, CISSP-ISSMP

Associate Professor of Information Assurance

School of Business & Management, Norwich University

This paper 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.

Contents

1	Introduction	2
2	Selling Products and Services	3
3	Unwanted Messages	4
4	The Prime Directive.....	5
5	Responsible Posting.....	6
6	No Covert Ads or Shills	7
7	Don't Talk to Strangers	8

* This paper consists of several short articles I originally published in *Network World Security Strategies* in 2000.

1 Introduction

I first started using e-mail in 1982 at work, when I was a “systems engineer” for Hewlett-Packard Canada. In the early 1980s, E-mail was restricted mostly to businesses and academic users; a few thousand individuals exchanged messages through bulletin board systems (BBSs), and there were various schemes for mail relay among BBSs and value-added networks (VANs) such as Prodigy and CompuServe. Basically, amateurs did not have much exposure to electronic communications.

In contrast, today millions of people have grown up using e-mail, chat rooms and news groups from their childhood or youth, quite apart from businesses and formal organizations. Because of the rapid rise of these high-tech communications media, there has been a rupture in civility. There is a disjunction between the customs of civility and courtesy that were defined for earlier generations in terms of speech, telephone and written communications and the habits of a couple of generations who have developed their own style almost free of guidance from older people.

There is nothing unusual about different modes of communication for different contexts; conversational spoken language, for example, sounds quite different from the formal speech of conferences or the structured writing of an article. Speech between two long-married people, for example, is highly idiosyncratic. Jean-Paul Sartre once said that a good marriage is like a conversation that never ends, but the conversation becomes quite peculiar after a while. I remember my wife’s and my amusement when we heard a tape we accidentally made during a car trip when we must have somehow gotten a recorder going: it sounded completely off the wall (“Is that surprising?” I imagine some of you thinking) with sentence fragments, long companionable pauses, code words (e.g., “Do I have baboons?” “No, you have no baboons.”), resumption of topics many minutes later as if there had been no intervening content, and a general lack of any obvious structure.

From a business point of view, however, some of the people most comfortable with electronic communications have developed some bad habits. This series will serve a guide to standards of appropriate behavior when employees are communicating online. Topic areas will include

- Selling Products and Services
- Netiquette for Beginners
- Public Relations Nightmares
- Appropriate Use Policies
- Protecting Your Web Site

2 Selling Products and Services

There is nothing inherently unethical about using the Net for selling products and services, but there are some fundamental problems peculiar to the Net: messages can be

- immortal;
- modified and become inaccurate;
- forged;
- unwanted.

Messages circulate on the Net without central control. Old copies of documents reside on individual servers and workstations and can be resuscitated years later. Imagine an advertisement for a special price on a company's product; having a client ask for that price two years later might cause problems if conditions have changed. However, from the client's point of view, the message may have arrived from a friend yesterday; even if the supplier explains that the sale is over, the client may be disappointed and perhaps even angry. From a commercial perspective, all communications offering goods and services ought to have a date of origin and an expiration date.

What good is an expiration date if someone alters it before rebroadcasting the message? For that matter, anyone can alter any aspect of a message before sending it back into the Net. The ultimate alteration is forgery: inventing a false message ostensibly from a specific person or organization. To avoid embarrassment and possibly litigation based on misleading or libelous documents, one should be able to repudiate such messages. There is no absolute repudiation, but one can build a strong case for repudiating a message if one uses digital signatures on all communications (see "Why Everyone Should Sign their Digital Documents" from 2000-02-14 at <http://www.nwfusion.com/newsletters/sec/0214sec1.html>). If thousands of messages have all been signed digitally, then an unsigned message or a message with an invalid digital signatures can reasonably be repudiated.

3 Unwanted Messages

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.

4 The Prime Directive

The most important principle you can teach your network users is that every communication made using the organization's e-mail system should be considered as equivalent to something written on official letterhead. Lack of professionalism in such communications can seriously damage the entire organization's reputation and credibility.

We have already looked at spamming – sending unsolicited commercial e-mail. Other forms of unwanted messages include hoaxes and chain letters. Many hoaxes refer to non-existent malicious software; a general policy that makes sense is to explain to all users that they must not broadcast any warnings. Users alarmed by such messages should simply contact their technical support team and let experts investigate (and often debunk) stories of exploding monitors, damaged disk drives and the like. As for chain letters (messages asking people to forward a warning, health information, or a petition to everyone in the recipient's address book), adults ought to know better than to forward such drivel, but at least within the organization, such forwarding can be interdicted by policy.

A simple lack of professionalism is to send or publish correspondence (or worse, articles) with spelling, grammatical or factual errors. Yes, of course no one is perfect, and the occasional blunder is forgivable (I sure hope so, given the errors I have made in print). What I am referring to is slovenly writing: poorly thought-through ideas, poorly expressed. Anyone can use a spell-checker at the very least; even a grammar-checker is better than nothing. But if an employee is involved in public discourse, especially on an important and highly-visible topic, it might be a good idea to have the Public Relations (Marketing, Corporate Communications. . .) experts check the content and style before launching it into the public sphere.

Another form of unprofessional behavior is “flaming.” Many users of e-mail and of the USENET think that making rude remarks about the people with whom they are corresponding is just a normal way of expressing disagreement. But rudeness is unprofessional. It is inappropriate for a professional to use profanity, obscenity, sarcasm, and other demeaning modes of expression. Even more embarrassing is to see correspondents who make *ad hominem* remarks – comments about the personality or personal characteristics of others. “If you had bothered to read what I wrote. . . .” or “You are obviously incapable of understanding my point. . . .” and similar slurs and innuendos demean not only the recipient but also the sender. They can certainly embarrass the sender's employer.

The converse is that as recipients, we need to be tolerant of what may appear to be rudeness. Not everyone has the practice required to write with sensitivity and subtlety, and sometimes people's sentences misrepresent their intentions. There is no cause for a professional to respond to other people's rudeness by descending into the written equivalent of a shouting match, regardless of provocation.

My own practice has been to avoid flaming back when I receive even private communications that cross the rudeness boundary. Over the years, I have occasionally written viciously vitriolic responses to rude people and laughed uproariously at how much fun it is to fight back. Then I have deleted the nastygrams and written back as politely as I can. The professional responses have not necessarily been friendly, but at least they were civil.

Corporate users should be made aware of these principles in policies and in training classes. It might even be fun having users practice responding to rude messages with civil responses as part of the classes.

5 Responsible Posting

We have seen in a previous section that posting advertisements in USENET news groups is a poor idea. Although not all news groups are moderated, there are nonetheless written or unwritten rules about whether advertising is welcome in any given group.

In general, there are some straightforward principles for being a responsible and welcome participant in a news group or other discussion forum:

- Lurk before you leap: learn about the specific style in use in the USENET group you intend to join. Do participants use formal or informal language? Do they seem to value pointers to documents produced by companies and other organizations? Is it appropriate to refer to your own products in this particular forum?
- Remember that on the USENET, everything you write may be archived and available indefinitely. Keep that in mind at all times before posting anything.
- Don't flame people (as discussed in a previous section).
- Avoid profanity, ethnic/religious slurs, and other offensive language.
- Stick to the forum/section subject area: don't post materials that are irrelevant to the subject, no matter how interesting you think it ought to be to participants. For example, most people in, say, a Windows 2000 technical discussion group would find it offensive to be told about human-rights violations in, say, Kosovo, no matter how important the topic may be in a wider sense.
- Make messages concise. In most groups, netiquette proscribes quoting an entire message; generally it's enough to quote just enough of a text to make it clear how your response is germane.
- Respect copyright laws: don't publish someone's comments elsewhere without asking for and receiving permission.

6 No Covert Ads or Shills

In addition to the general rules on civil collaboration in USENET groups and mailing lists, vendor staff should understand that only honesty is acceptable in selling products. It is unacceptable to post forum messages that are covert advertisements. Responses should be focused on the issue at hand and should be as helpful as possible. Forums, newsgroups may have strict standards and there may be negative responses to introduction of your company name and product without clear benefits to recipients. Repeated marketing hyperbole in technical forum repels potential customers. Indeed, even subtle propaganda will be punished: beware of posting superficially-objective responses that are slanted: misleading information will inevitably be punished by public exposure, humiliation of the guilty, and embarrassment of the employers.

Much worse than propaganda from an identified employee of a company is propaganda in the guise of disinterested comment. Company policy should make it clear that employees who are posting information that is relevant to company interests should clearly identify themselves as employees. Commenting on competitive products or services or praising one's own without clearly identifying oneself. Such shills are highly objectionable, and group members will often express their disapproval in the strongest terms. Shills may be locked out of controlled-access groups, both individuals and employers may receive torrents of abuse, and the effects may last for a long time.

Conversely, it is appropriate to post a disclaimer when appropriate to indicate genuine disinterest; e.g., "Neither the authors nor their employers have any financial interest in the companies, products and services mentioned in this communication."

7 Don't Talk to Strangers

There's a funny thing about becoming an active member of a discussion group – whether in real-space or in cyberspace. The longer you participate, the closer you feel to the regulars. There's a sense of camaraderie, of belonging to a group of interesting people; indeed, in some real and electronic groups, the regulars act like a regular clique. Like the snotty brats in high-school cliques, these folks treat newcomers with disdain and assume a position of superiority that can be truly offensive.

However, that same sense of camaraderie, even when it is expressed positively and not through putting down others, may fool employees into forgetting that they don't necessarily know with whom they are corresponding. Furthermore, they don't know who is lurking (reading the exchanges without contributing). The audience may very well include people from direct competitors, and there is nothing illegal about using information that is posted openly in a public forum.

Employees should not post intimate details of a particular project, a new product version, plans for expansion in a new geographical area, their employer's marketing strategy or inside information that could violate Securities and Exchange prohibitions on reveling insider information that could affect share prices. Appropriate use policies should make it clear to everyone that by definition, confidential information may not be disseminated outside the organization. Only the Public Relations or Corporate Communications / Marketing departments would normally be authorized to decide how and what to post publicly.

The principle of discretion applies equally well to criticisms of the employer, partners, suppliers, or individuals. It is foolish to think that broadcasting internal grumblings about an employer will be ignored by management. Such public criticisms can severely damage the organization. Now, if the organization is breaking the law, employees can report the crimes to law enforcement or regulatory authorities; however, posting details in public may make it difficult or impossible for investigators to gather information that will be usable for prosecution. Employees who have resigned or who are fired might also want to check the terms of their contracts; some employment contracts impose a gag on criticism even after an employee has left the employ of an organization. When in doubt, consult an attorney with experience in employment law and litigation.

One last note: employees should remember that most of what is posted on the USENET and today's World Wide Web is archived and can be available to prospective employers years later. If employees fail to protect the interests of one employer, what would convince a new employer that their discretion would be any greater in the future?

