Protecting Your Reputation in Cyberspace: Selling Products and Services

by M. E. Kabay, PhD, CISSP
Security Leader
INFOSEC Group
AtomicTangerine, Inc.

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 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.

***

In the next article in this series, I’ll look at unsolicited and unwanted e-mail.

***
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.