Protecting Your Reputation in Cyberspace:  
Don’t Talk to Strangers

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’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 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?

* * *

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.