Ethical Debate over Computer Trespass (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

This is part two of a three-part dialogue with someone who challenged me to explain why using a found user-ID and password is wrong.

***

>If, at a public Web site, the company accidentally left their customer names and addresses in a file that I can access. Clearly, it was not their intention to give me access to these files; or was it? Have I broken the law by taking and using this customer base?<

Yes, you have appropriated information to which you have no legal or moral right. That the information is stored electronically is no more relevant than if it had been written on paper or graven in stone.

>What did I "break" into in these examples?<

Their security perimeter; you also broke ethical principles and the law.

>The door was left open and it was inviting. By not having proper security, did the company not authorize me to have access?<

No, it didn't. Making a mistake does not constitute permission.

>I think that we can use physical examples only so far in the cyberspace.<

"Cyberspace" is a metaphor too. There is no special privilege accorded behavior solely on the basis of medium of communication. That you are using electronic methods for accessing the information is no more relevant to the ethical and legal issues than if you claimed that you could legally eavesdrop on a conversation solely because it was in, say, German. Do you believe that we could convince anyone that "Germanspace" and "Frenchspace" have different rules from "Englishspace" bearing on the inappropriateness of listening in on conversation between human beings? Why should we view responsibility, courtesy, consideration and kindness as irrelevant solely because of the use of, say, the Internet? Do you feel that slander is wrong when it's spoken face-to-face but OK when it's communicated through a telephone? What other technological tools absolve the user from normal rules of civility? Is a driver who makes rude gestures at you any less rude because he's doing it from inside an automobile than if he did it on the sidewalk as you were walking past each other?

>In my opinion, if I as a company am sloppy, then I am responsible.<

You mean, surely, irresponsible. And yes, you are certainly responsible for the consequences of your failures. Why does that responsibility then remove responsibility from the criminal who attacks your system using the vulnerabilities you have left in place? What is he, then, a robot? A mere automaton, devoid of personal responsibility for his actions? Sounds very much like the
rationalizations of those defective people who abuse their spouses and then blame the victim for "provoking" their abuse. "Look what you made me do," cries the abuser after smashing his wife's face. "It's your fault for making me mad." Such refusal to accept responsibility is pathological; why should we not apply the same standard to abuse of other people's bad computer and network security?

> If via my sloppiness, my information security is violated, how can I blame the person who found themselves with access? I gave them this access via my sloppiness.<

No you didn't. You made it easier for dishonest people to abuse the information that you inadvertently made accessible. You are to blame for incompetence and they are to blame for taking advantage of it. Responsibility is not a zero-sum game where it's impossible for people to have different kinds of responsibility for a bad event. If a driver is not wearing a seat belt when another car smashes them off the road because that driver is drunk, do you think that the unbelted person's stupidity -- he's definitely partly responsibly for the severity of his head trauma -- absolves the drunk from responsibility for the consequences of _his_ actions?

***

To be continued.

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 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.