The column about finding a user ID and password in a cyber-café provoked some interesting e-mail responses from readers who were interested in the problem. Some correspondents were appalled by what they interpreted as the original reader's lack of moral sense. I learned through further correspondence with this person, who wisely chooses to remain unnamed in this column, that he is definitely not a moral imbecile: he was genuinely interested in how to respond to such questions, not taking a stance in favor of trespass.

Most readers of this column are already highly qualified to discuss the ethical issues of criminal hacking, especially with young people. I hope that some of these readers will be interested in the following correspondence that followed his initial questions and stimulated to engage in dialogue with criminal hackers and would-be hackers and exploiters of vulnerabilities to challenge their assumptions.

The following is a slightly edited version of my response to a series of questions and arguments he put up for discussion. Because of the length of the debate, I've broken the correspondence into three parts.

* * *

You wrote:
> If I see an ID and password and use this am I breaking in? <

Yes.

> What did I break? <

Ethical principles and the law. And "breaking in" is a metaphor, not a literal description of physical damage, so your question about what you broke is surely disingenuous -- that is to say, sophistry.

Who is to say that this was not meant to be a public login ID.<

You are, by applying your own good sense and experience of how people make mistakes by failing to protect their systems. You don't seriously expect anyone to believe that you truly think that a user ID and password left visible on a screen in a cyber-café constitute a public access ID?

> It was given to me in public.<

No it wasn't, any more than a person who leaves her purse on a table in that cyber-café is giving it to you when you steal it.

* * *
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.