A reader recently wrote to me with a practical question:

> I'm at a cyber cafe and see an IBM rep log into the IBM site using GoToMyPC. I see the login and password. It was there for public display.

Is it legal for me to login to that site, and download a customer list, and use this information?

Has IBM, and this employee, left the door open for me and, in doing, made this information public?<

[Mandatory disclaimer: I am not a lawyer and this is not legal advice. For legal advice, consult an attorney.]

As I understand the laws and jurisprudence in the United States, using a system login without authorization is a violation of law(s). The Computer Fraud and Abuse Act (CFAA) of 1986 applies to federal-interest computers (essentially any computer used by or for federal, states, county, or municipal government departments and agencies OR any vendors supplying services to those entities).

Additionally, the Electronic Communications Privacy Act (ECPA) of 1986 has no limitations on its applicability. It applies not only to unauthorized interception of private communications such as e-mail messages during transmission but also to stored versions of such documents.

Neither the CFAA nor the ECPA makes an exception for unauthorized access using a stolen (or borrowed, or inadvertently seen) user-ID & password. It’s irrelevant how easy it is to break into a system: contrary to the widely-posted beliefs of criminal hackers and their supporters, exploiting obvious vulnerabilities to make unauthorized use of a restricted system does not exculpate the intruder.

The parallel in the real world is that if someone drops the metal key for entering a secured area of a business office or to enter the front door of a home, the finder of the key has no legal right to use it to enter the premises and then to eat pastries, steal radios, or snuffle through private information or any other property in the poorly-secured area. Similarly, just because a computer network is poorly secured, no one has a legal right to penetrate it – regardless of how they do so – and to access confidential information or to tamper with corporate systems.

There have been occasional discussions in the courts about whether a system visible on the Internet that does NOT have any kind of warning about being restricted can be penetrated inadvertently without criminal penalty; to avoid such ambiguity, security policies should include an explicit warning equivalent to the NO TRESPASSING sign on a field in the countryside. Such a sign makes it illegal to walk on the land, regardless of whether the perimeter is protected by barbed wire, automatic machine guns or land-mines. But although all restricted systems
should be so noted for maximum legal protection, my understanding is that failing to post a
warning does not excuse electronic trespass under law.

I hope you will forgive me for adding a personal note about ethical standards here. When I
returned from a plane trip to Washington last week, I was walking out to the parking area when I
noticed a parking stub lying on the floor. Upon picking it up to throw it in the waste basket (I
just don’t like litter), I noticed that it was time-stamped for a few minutes before I landed.
Before I go further, I hope you won’t interpret my example as insufferable self-righteousness –
I’m just trying to make a point. So as I was saying, I threw the ticket away. Now, why didn’t I
use the ticket to get out of paying for a whole day of parking in the garage? After all, the
security system of the garage is clearly inadequate: it does not authenticate the authorized user of
a particular ticket (for instance, by printing an image of the license plate of the car used when
getting the ticket at the dispenser). I just plain don’t like the idea of cheating the parking garage
out of their fee. The fact that I could do so is irrelevant: being able to cheat someone doesn’t
make it right.

***

I hope you found this summary helpful. For more details on cyberlaw, see

have useful summaries.


0-387-94832-5. xiv + 362. Index.

You may also find this Web site helpful: Cyberspace Law Institute
http://www.eli.org/default.html

***

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

bookstore or from Amazon at: <http://www.amazon.com/exec/obidos/ASIN/0471412589/tag=fusion0e>

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.