Revealing Too Much

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

In a preceding column, I discussed controls over the information posted in the WHOIS database for Domain Name System (DNS) registration, pointing out that it is unnecessary to give specific employees’ names and phone numbers in that database. Today I’d like to continue on that theme with some warning about other ways that we tend to reveal too much about ourselves and our activities in today’s electronically interconnected world.

Let’s start with e-mail. Why give away information that is unnecessary for most correspondence yet valuable for social engineering? In your signature block, is it necessary to post your complete physical address, including precisely which building and office you work in? If someone needs to visit you, you can give them your precise location details once you have established some basis for trust. Do you have to give your secretary’s name and phone number? What about your fax number – why invite junk fax? If someone needs to send you a fax, they can ask for the number.

When you are going away on a business trip or a vacation, is it really to your advantage to broadcast exact details of when you will be away, why and where? Doesn’t this information provide easy ways to impersonate you or to take advantage of your absence for robbery, data theft, sabotage or other types of harm? And remember that auto-replies are always dangerous: all you need is a message to be sent by someone who happens to turn on their own out-of-office autoreply and you have a mailstorm brewing. Your autoreply sparks their autoreply which sparks another autoreply from your mailbox and so on until a server crashes or someone notices the flurry of useless e-mail. But think now: when you leave your home for a vacation, you do not put a big sign on your front lawn that reads, “We’re going away for two weeks now, so there’s no one home and you can rob us blind or burn the house down more easily.” No, on the contrary, you arrange to stop newspaper and milk delivery so that there are no tell-tale signs of your absence; you may set automatic lights to go on and off; you arrange with your neighbor to water the plants and pick up regular mail – all to avoid announcing to Bad People that you aren’t at home. So why do the opposite at work? Are you really so important that every single person sending you e-mail absolutely has to know that you’re away? Why not let the ones who really care simply call your work number, fall back to the backup person who answers in your place, and learn a limited amount about your absence as required? While we’re on the subject, apply the same reasoning to your voice-mail messages. “I’ll be away until next week” may make you sound important, but it may also invite theft or spoofs.

As for the Web, just because it’s easy to post information doesn’t mean that all of it should be posted. For example, on a person Web site, some people post – I’m not kidding – their date of birth and their social security number. Resumés (CVs) can be so detailed as to provide the basis for successful impersonation; necessary? On corporate Web sites, some organizations post detailed internal phone lists with employee names, titles, departments, office numbers, phone numbers, fax numbers, secretaries’ names – the whole shebang. Hmm – maybe a bit too much, no? Some companies post excessively helpful competitive information such as detailed lists of important clients; what better help to competitors could one ask for? And some organizations
cheerfully post internal documents such as minutes of meetings, strategic plans, and competitive analyses on their public Web sites, perhaps under the mistaken impression that these are the same as their private intranets.

I hope that this litany of open-hearted, trusting publication of information has sent some premonitory chills up the spines of some readers. Perhaps there will be a flurry of activity as readers rethink just how much information really ought to be made public in their e-mails and Web sites.

Isn’t it awful being so suspicious?

Isn’t it worse not being able to be suspicious on demand?

* * *

See also


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.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 <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 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.