Reforming the WHOIS Database

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

In fighting spam and other forms of Internet and e-mail abuse, many defenders of the ‘Net have noticed that the worst offenders often include obviously false information in their WHOIS database entry. The WHOIS database records the contact information for each registered domain in the Domain Name System (DNS). In my attacks on originators of spam, I’ve often seen the phone number (nnn) 555-1212 (where nnn is an area code) supplied as the contact point; addresses such as “12345 Street Road” with bogus ZIP codes; real-looking phone numbers that turn out to be nonexistent or disconnected; and countless e-mail addresses that bounce like the walls in a squash court.

The Internet Corporation for Assigned Names and Numbers (ICANN < http://www.icann.org is “the non-profit corporation that was formed to assume responsibility for the IP address space allocation, protocol parameter assignment, domain name system management, and root server system management functions. . . .” In other words, ICANN regulates the administrative infrastructure of the Internet. In March of this year, the board of directors voted to accept four important recommendations from the Generic Names Supporting Organization (GNSO) Council to maintain the integrity of information in the WHOIS database. These recommendations are as follows:

>1. Accuracy of WHOIS Data.

A. At least annually, a registrar must present to the Registrant the current WHOIS information, and remind the registrant that provision of false WHOIS information can be grounds for cancellation of their domain name registration. Registrants must review their WHOIS data, and make any corrections.

B. When registrations are deleted on the basis of submission of false contact data or non-response to registrar inquiries, the redemption grace period -- once implemented -- should be applied. However, the redeemed domain name should be placed in registrar hold status until the registrant has provided updated WHOIS information to the registrar-of-record.

2. Bulk Access to WHOIS Data.

A. Use of bulk access WHOIS data for marketing should not be permitted. The Task Force therefore recommends that the obligations contained in the relevant provisions of the RAA be modified to eliminate the use of bulk access WHOIS data for marketing purposes. . . .

B. Section 3.3.6.5 of the Registrar Accreditation Agreement currently describes an optional clause of registrars’ bulk access agreements, which disallows further resale or redistribution of bulk WHOIS data by data users. The use of this clause shall be made mandatory.<

In addition, the recommendations strongly supported development of “a reliable contact point to receive and act upon reports of false WHOIS data.” The recommendation continued, “ICANN
should encourage registrars to (i) provide training for these contact points in the handling of such reports, and (ii) require re-sellers of registration services to identify and train similar contacts.”

These measure will help to fight the scourge of spam by shutting down entire domains that are run by dishonest people. They will also inadvertently shut down perfectly legitimate domains whose owners are too disorganized to keep their information up to date. If you run a business that depends on the existence of your own domain (e.g., for your own Web site or to send and receive important e-mail), you had better put proper measures into place to ensure that a named individual (and a backup person) are explicitly responsible for keeping the WHOIS database correctly updated (and your DNS registration fees paid on time) or you might suffer a self-imposed denial of service.

Lastly, as you consider how to comply with these regulations and update your own registration information, keep one other factor in mind: no one has asked you to provide information that would permit easy social engineering. For example, you don’t have to provide the exact name of the human being(s) who will be the administrative contact and the technical contact; instead, you can give a title (e.g., Hostmaster) and an accurate and working, but generic e-mail address such as hostmaster@domain.tld. The additional benefit of such a system is that you control where e-mail directed to this address ends up; this flexibility means you don’t have to update the WHOIS database every time you reassign responsibility for the domain to another employee. For the same reasons, the phone number can be the switchboard rather than a specific extension, thus allowing you to direct calls to the right person without giving away valuable internal information that might support a criminal hacker’s attempts to spoof someone’s identity.

* * *

In my next column, I’ll look at other kinds of problems that can occur with posting of internal information where it isn’t necessary.

* * *

For further reading:

Minutes of the Regular Meeting of the Board of Directors of ICANN 27 March 2003 <http://www.icann.org/minutes/minutes-27mar03.htm>

* * *

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.