CallingID Fights Web Fraud

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

Many online frauds depend on deceiving victims into trusting a Web site and revealing confidential information such as credit card numbers. Phishing frauds, for example, use deceptive e-mail messages to trick people into visiting Web sites whose URLs are misrepresented as trustworthy ones (e.g., the classic use of "paypal.com" labels for URLs that are actually in some under-regulated and under-policed country where governments don't even pretend to follow the rule of law). Other frauds simply use nice-sounding domain names (e.g., the spate of Katrina-related Web sites that arose after the hurricane disaster) but are actually run by crooks who steal the money outright.

One of the ways to help spot fraud is to find out who has registered a particular Web site; this knowledge does not prevent all fraud, but it is a useful step forward. If you are looking at a site that claims to be in Ohio but the owner lives in the Moldovan Republic (no offense to Moldovans intended), maybe everything is not as it appears.

In previous columns, I've mentioned the free utility SamSpade v1.14 (available from < http://www.samspade.org/ >) which, among other things, makes "whois" lookups of Domain Name Server (DNS) information quick and easy.

Readers may also know that the free, open-source Firefox Web browser from Mozilla < http://www.mozilla.org/products/firefox/ > has an "extension" (add-in) called "whois 0.4" that can supply a DNS lookup for each Web address being visited.

I've been trying out an add-in for Internet Explorer (IE) over the last two months called CallingID < http://www.callingid.com/Default.aspx > that does all that and much more.

I had the pleasure of speaking and corresponding with Yoram Nissenboim, CEO of CallingID, the company that makes the CallingID secure Web-browsing add-in product. Among other things, CallingID provides automatic DNS lookups for all URLs. A quick installation of this (currently) free product adds a new bar to the IE window showing ownership information including geographical location for the Web site being visited.

However, as Mr Nissenboim pointed out, "Whois information is very unreliable. Everyone can write whatever he wants into DNS records. CallingID has external sources beyond Whois to detect the site owner and to verify that it is a real organization located where it claims to be, in most cases automatically." If any of more than 50 warning signs shows reason for suspicion, the product alerts the user with an understandable pop-up; for example, one test checks for anonymized owner information in the DNS and any such concealment flags the site as suspect.

The company has expanded its checking to incorporate known-good sites from many sources such as the Better Business Bureaus, certification authorities and Dunn & Bradstreet; their database now includes more than a million legitimate sites worldwide and this information is provided almost instantly to users without having to rely on DNS servers, thus maximizing performance. It is noteworthy that some users have complained about slow DNS lookups in various forums (see < http://www.linuxquestions.org/questions/history/335170 > for a sample thread).

Mr Nissenboim also pointed out that their tests verify such technical security features as the validity of site certificates or the use of encryption and explain the significance of these factors in plain, non-technical language that allows the user to judge the safety of interacting with the site. A particularly valuable feature is that the product detects attempts to send data to a destination on a different server than the one for the Web site the user is visiting – an immediate reason for concern about the legitimacy of the data transfer. As usual, CallingID reports on the identity and trustworthiness of the ultimate destination.

In summary, and quoting the company CEO once again, "CallingID is a tool that provide full risk assessment for users that send personal or confidential information (such as password, credit card details etc.) over the Web. The tool shows them the identity of the site receiving their information and alerts them about any risk associated with the site they send data to and the form they use."

This tool may be helpful in increasing resistance to phishing scams, especially for novices. Mr Nissenboim told me that his company's recent survey of 110 users indicated that "55% stopped sending data to a site following information provided by CallingID." In my two month trial, I saw no negative side effects of the product.

Worth a try, I think, especially for naïve users.

[Disclaimer: I have no financial interest in this company or product despite this glowing review and had never met Mr Nissenboim before our correspondence and phone interview.]

* * *

New information assurance journal – Norwich University Journal of Information Assurance (NUJIA). See < http://nujia.norwich.edu >.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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 >.