In my last column, I described a novel approach to Website authentication involving a user-selected picture and label; one technique using this approach is the SiteKey currently being used by the Bank of America. <http://www.bankofamerica.com/onlinebanking/index.cfm?template=site_key>


“We asked 67 bank customers to conduct common online banking tasks. Each time they logged in, we presented increasingly alarming clues that their connection was insecure. First, we removed HTTPS indicators. Next, we removed the participant’s site-authentication image—the customer-selected image that many websites now expect their users to verify before entering their passwords. Finally, we replaced the bank’s password-entry page with a warning page. After each clue, we determined whether participants entered their passwords or withheld them. . . . We confirm prior findings that users ignore HTTPS indicators: no participants withheld their passwords when these indicators were removed. We present the first empirical investigation of site-authentication images, and we find them to be ineffective: even when we removed them, 23 of the 25 (92%) participants who used their own accounts entered their passwords. We also contribute the first empirical evidence that role playing affects participants’ security behavior: role-playing participants behaved significantly less securely than those using their own passwords.”

The 23 out of 25 test results for the SiteKey (or equivalent) results in a rate of 92% of the subjects ignoring the absence of the SiteKey; I calculate the 95% confidence limits to be 74% to 99% if the sample was random. These results are not encouraging. If the study results are replicated in independent trials, we may be faced with the unhappy conclusion that trying to make amateurs responsible for identifying phishing attacks is a waste of time. The only question remaining then is whether the actual costs of implementing the technique are warranted by measured savings in reduced fraud.

One unfortunate aspect of the fight against such fraud is that financial institutions seem to have little interest (no pun intended) in reducing fraud if the measures would in any way reduce utilization of their financial services; after all, the costs of fraud are borne not by the institutions’ shareholders but by the unfortunates who fail to pay their monthly balances every month and are subjected to usurious interest rates currently approaching 25% per annum.

Nonetheless, I think that perhaps the SiteKey might still be useful with specific populations of
highly-trained or professional users; for example, a corporate extranet might authenticate itself to users using such a system before asking users to authenticate themselves to the server. Ideally, such a system would be used with token-based authentication involving strong encryption. Under such circumstances, the site-authentication could be helpful despite the possibility of the relatively difficult and non-scalable process of executing man-in-the-middle attacks on the system.

* * *


M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.msia.norwich.edu> at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2007 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.