Senior Technology Consultant Mike Drabicky has been working in the computer industry for over three decades in programming, system and network management and design, data center management and database security and compliance. He’s a regular and welcome correspondent and I was so taken with his most recent comments that I asked him for permission to publish them. Here, with slight edits, are his discussion of a new wrinkle in authentication (“I” refers to Mike).

* * *

I have a Bank of America (BoA) credit card and use their Website all the time to check charges, pay bills and all those normal online activities. As one who deals with security as part of his job, I am always concerned about phishing, phony Websites masquerading as the real thing, all dedicated to taking that which is not theirs to take: my personal information.

A year or so ago, BoA offered the SiteKey, a second level of authentication. With this, you would pick an icon representing something of interest as a way of authenticating the Website and only then provide a password to access your account. Mich published a couple of articles in April 2007 about SiteKey. <http://www.networkworld.com/newsletters/sec/2007/0402sec1.html>, <http://www.networkworld.com/newsletters/sec/2007/0402sec2.html>

More recently, BoA offered another frontend security option: SafePass, a text message code sent to your cell phone. <http://www.bankofamerica.com/privacy/index.cfm?template=learn_about_safepass> Upon request, BoA will send a 6-digit code to your cell phone via text message. When you enter the code, BoA validates the code and allows you to proceed to the icon/password verification page just described. The token expires in 10 minutes. They also offer an alternative mechanism of authentication should you be in a place unable to receive the message on your cell phone.

There are a number of really positive things to say about this scheme:

1) It is low cost. No tokens to tote, no tokens to lose, no software to load, nothing extra needed other than what you very likely already have: a cell phone.

2) It is easy to understand and use. There’s nothing complicated about this: anyone accessing their Website should be more than knowledgeable enough to appreciate the simplicity and elegance of this system.

3) It speaks volumes for BoA. This tells me that Bank of America understands the security risks of doing credit card business on the Web and has taken steps to make sure the person on the other end of the browser is indeed who they say they are.

Could this system be compromised? Well, since you’re reading this column, you know that any
system can be gamed. However, a criminal hacker will need to spend considerably more effort to do so than for other sites that use only a simple username/password authentication scheme. Why would a criminal bother attacking a difficult account when there are millions of easier marks (at least, for now)?

Perhaps it is time that other financial institutions stand up and take note. We, your customers, love the convenience of doing business online. But we do not control the security methods that you use (or fail to use). Unless you want to be in the next headline showing that your lack of adequate security resulted in allowing sensitive customer information to be leaked to hackers, it’s time you took a fresh look at the methods you employ to keep a lock on your door.

***

[MK adds: I enrolled in less than two minutes. Seems to work fine.]

***

Mike Drabicky welcomes your comments by e-mail.<mailto:mikesec1@wildblue.net>

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies 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. Drabicky & 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.