Don’t Just Talk About Security:  
DO Something!  

by M. E. Kabay, PhD, CISSP-ISSMP  
CTO, School of Graduate Studies  
Norwich University, Northfield VT

In the previous article in this two-part series, I reviewed disheartening research commissioned by CISCO Systems showing that in general, our security-awareness efforts don’t work. Most people seem to blame poor communications or the obtuseness of users.

In contrast with this standard view of the failure of compliance with sensible advice, scientists at Carnegie Mellon University (CMU) have been studying why people fail to follow perfectly good advice on how to avoid phishing scams. Several of their research reports are available on the PhishGuru site<http://phishguru.org/>. Lorrie Faith Cranor, DSc< http://lorrie.cranor.org/>, Associate Professor of Computer Science< http://www.scs.cmu.edu/> and also of Engineering and Public Policy< http://www.epp.cmu.edu/> at CMU has also written a popular article on phishing for the December 2008 issue of Scientific American< http://www.sciam.com/article.cfm?id=how-to-foil-phishing-scams> which discusses how ineffective acquisition of information has been in changing people’s resistance to phishing attacks. As a result, she writes,

“With some of these insights in mind, members of my team, Ponnurangam Kumaraguru, Alessandro Acquisti and others, developed a training system called PhishGuru, which delivers antiphishing information after users have fallen for simulated phishing messages. The program incorporates a set of succinct and actionable messages about phishing into short cartoons, wherein a character named PhishGuru teaches would-be victims how to protect themselves. In a series of studies, we demonstrated that when people read the cartoons after falling for the simulated phishing e-mails that we sent to them, they were much less likely to fall for subsequent attacks. Even a week later our test subjects retained what they had learned. In contrast, those who read the PhishGuru cartoons sent to them by e-mail, without experiencing a simulated attack, were very likely to fall for subsequent attacks.”

In addition to the cartoons, the scientists created an interactive game< http://wombatsecurity.com/phil.php> involving worms (annelids, not computer programs) representing Web sites that a cute little fish can either eat or not. A wise older fish explains the failures and successes in a friendly way. Playing this simple cartoon-based game for a few minutes “makes a significant difference in users’ ability to identify phishing sites. Comparing their performance before and after the training, we saw a drop in the number of false negatives, phishing sites mistakenly deemed to be legitimate, and false positives, legitimate sites judged to be phishing sites. The game players also outperformed participants who trained with a tutorial or with materials from other sources.”

I’m not surprised.

In 1994, I published the first edition of “Totem and Taboo in Cyberspace: Integrating Cyberspace into our Moral Universe.”<http://www.mekabay.com/ethics/totem_taboo_cyber.pdf> Based on well-established principles of learning and the psychology of behavior change, I wrote,
“To learn new habits, it is useful to address the conflict directly: acknowledging that the policy will be uncomfortable at first is a good step to making it less uncomfortable. For example, employees should participate in role-playing exercises. First, they can practice refusing access to colleagues who accept the policies graciously, then move on to arguments with less friendly colleagues. Finally they can learn to deal with confrontations with colleagues who pretend to be higher rank and hostile.”

You can find additional recommendations on role-playing in my PowerPoint slide deck on “Social Psychology and INFOSEC.”<http://www.mekabay.com/courses/academic/norwich/is342/lectures/35_Social_Psychology.ppt>

I think it will be worthwhile for readers to try the demonstration game on the Web<http://wombatsecurity.com/antiphishing_phil/index.html> and to ask family – and especially young members of your families – to try the game too. If your organization is interested in customizing the game to suit your needs, you can do that too.

All in all, the evidence is simple to summarize: if you want to make your employees more security-savvy, stop just yacking at your employees and get them to DO SOMETHING!

***

M. E. Kabay, PhD, CISSP-ISSMP <mailto:mekabay@gmail.com> specializes in security and operations management consulting services. CV online.<http://www.mekabay.com/cv/>

Copyright © 2008 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.