Social Engineering in Penetration Testing (6): Overloads, Fascination & Awareness and Training

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

Distinguished correspondent Paul Schumacher continues with contributions of his perspectives on additional social engineering techniques. We finish with comments on training employees to resist social-engineering techniques. What follows is Mr Schumacher’s comments with minor edits.

* * *

I have thought of two other methods of social engineering you may want to consider. One is overload: present the individual with so many decisions to make that they start to default to simple responses on those that seem innocuous. This is very excellently presented by the movie "Sneakers" when Robert Redford had to get into a building, and his team overloads the guard, who in desperation just buzzes Redford into the building.

The second is fascination. A staged 'play' that is interesting to the target will at worst totally engross the target individual, and at best, distract them from their job. In fact, the methods and techniques are as varied as there are individuals on the planet. What they have in common is the desire to have someone behave in a manner that is counter to security. Those who have the responsibility to protect security should be taught that it is far safer to maintain the safety of the security than to please or give in to someone who wants us to compromise it.

It could be an excellent teaching tool to have a class think up new methods of social engineering, particularly those that exploit the unexpected. The idea is to get them to think not just outside the box, but beyond the walls of the building the box is in. This is what those attacking security are doing more and more these days.

* * *

[MK adds:] In many of my articles, I have emphasized the power of play-acting or role-playing exercises in security awareness and training. In my experience, students and employees who act out a situation are far more likely to remember the lesson than if they simply hear about it or see a simulation. Rebecca Teed of the Science Education Resource Center at Carleton College has put together an introductory overview of role-playing in teaching (including a pointer to readings) and also a detailed tutorial on “How to Teach Using Role-Playing” that can help readers who want to apply this powerful tool to information assurance.

* * *

Paul Schumacher (mailto:psch@optonline.net) welcomes correspondence. He is particularly happy to work on interesting research projects with anyone who can benefit from his expertise.
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 Paul Schumacher & 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.