In the two preceding columns, Dr. John Orlando discuss the ethical dimensions of social engineering in penetration testing. Today I want to look at how to use social engineering effectively for penetration testing.

I have long believed and taught that social engineering can be useful for security testing, but only with careful preparation. The first and most obvious warning is bad penetration testing in general is pointless unless the organization has implemented the best available security measures it can manage. Why bother testing security if even a simple vulnerability analysis or common sense assessment shows gaping holes? A penetration test of obviously flawed security is a waste of time and money.

In a _Network World_ column published in 2000 (<http://www.networkworld.com/newsletters/sec/2000/00292157.html>), I pointed out that deception techniques should be used only with a great deal of preparation of the staff. The key points were as follows:

When preparing for a penetration test that involves social engineering, everyone in the organization should be thoroughly trained to understand the techniques of social engineering before beginning the tests. The key points were as follows (quoting from my article):

- The entire organization can prepare for social engineering simulations as a team; no one is subjected to attempted deception without knowing that the experience was part of a training and awareness exercise.
- Even if someone falls for a trick, the emotional effect is far less than if the same error occurred without preparation.

I think that preparing staff for the onslaught of skilled social engineers has many benefits. We can frame the exercises as a form of game or contest: who will be the best at spotting the confidence tricksters? Who will be quickest to foil their nefarious plans? Role-playing games are an excellent way of changing beliefs, attitudes and behavior: having staff members take up the roles of social engineer and defender – and then reversing roles – is not only amusing, it has a long-term effect on people’s perceptions. It’s much easier to remember a social interaction we’ve experienced personally than to pay attention to abstract words. We can even turn the event into an opportunity for a good deal of fun and laughter, making security and secure behavior a positive experience instead of the usual drudgery.

Moreover, in addition to risk avoidance (reducing the likelihood of hurt feelings, frustration and anger), solid preparation can result in increased vigilance at all times. Once staff members are sensitized to the social engineering tricks they’ve experienced in role-playing games, they are more likely to recognize them in strangers. Having practiced alerting the security team to apprehended breaches, they will find it easier to take the initiative later when they spot real breaches.
In my next column, I’ll finish with this topic (for now) by discussing approaches to handling cases of successful social engineering.

* * *

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. 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.