Dr John Orlando continues his two-part series on the ethics of social engineering for penetration testing. What follows in this column and the next is entirely Dr Orlando’s work with minor edits.

* * *

Analysis

The cases described in the previous column have been deliberately ordered from least to most ethically troubling. I would argue that there are morally relevant differences between the shoulder surfing and piggybacking cases on one hand, and the computer technicians and bribery cases on the other. For one, the latter two cases expose the employee being tested to significant psychological stress. The employee in the computer technician example is worried about losing his job, while the one in the bribery example is faced with an offer to do something illegal.

Moreover, the deception in the latter two cases is established by verbal manipulation. Why is this relevant? After all, all cases involve some level of misrepresentation, and we can just as easily misrepresent ourselves with our appearance and actions as we can with our words. The difference is that when the deception is established verbally, the deceiver is plugging into deep-seated psychological triggers humans use to establish trust with others. Con men are good at playing on these triggers, and while people can be expected to follow procedures, they cannot be expected to resist the kind of psychological manipulation employed by skilled manipulator. We would say the same thing of an attractive consultant soliciting an executive to see if he would exchange sex for secrets. The enticement is unfair. Moreover, the episode will undermine the employee’s trust in the company.

There is also the question of the professionalism on the part of the consultant when he moves from providing security advice to acting. Once the deceiver starts the charade, he will not know how much acting will be needed to get the employee’s cooperation. At some point the question becomes whether the consultant is measuring the strength of the company’s security policies, or his own acting skills. The consultant has put himself or herself into a compromising situation that could undermine faith in the profession as a whole.

Finally, what is the employer going to do with the employee in the bribery case if he agrees? The employer cannot trust the employee anymore, yet if he fires the employee, he can be accused of entrapment.

These observations allow us to draw up some guidelines for the use of social engineering in penetration tests. Social Engineering can be used in situations to gain knowledge of a security program that cannot be derived in other ways, but must be bound by ethical principles, including:

1. Just as human research guidelines demand that subjects are protected from harm, social engineering tests should not cause psychological distress to the subject.
2. Employees that fail the test should not be subject to public humiliation. The consultant should not identify an employee who fails a test to other employees or even the employer, as it might undermine the employer’s view of the employee. The information can be presented as part of an education program without identifying the employee.

3. Independent oversight is an important component of human research protocols. Just as universities have human research oversight committees, consultants should get approval from at least two individuals at the organization before using social engineering in a penetration test.

4. Testers should avoid any verbal misrepresentation or acting to establish the deception.

* * *

In the next column, I [Mich] will follow up on John’s articles by adding a few observations about when and how to use social engineering effectively in penetration testing.

* * *

John Orlando, MSIA, PhD, <http://www.linkedin.com/profile?viewProfile=&key=1521965> is Instructional Resource Manager in the School of Graduate Studies at Norwich University. He earned his doctorate in philosophy from University of Wisconsin at Madison in 1993 and has more than a decade of experience in online university education. He teaches undergraduate ethics and philosophy courses at Norwich and can be reached by e-mail at <mailto:jorlando@norwich.edu>.

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 John Orlando & 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.