Defending Against Deception

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

Jim Allred of NetVision Inc contributed the following essay to the column and I offer it with minor edits below. [I have no financial interest whatever in NetVision.]

* * *

Social engineering is the art of lying, cheating, tricking, seducing, extorting, intimidating and even threatening employees into revealing confidential information that can be used to break into a company's systems. Tricks such as phony e-mails or phone calls to “confirm” password information, or deliberately locking out an account using bad passwords and then phoning the helpdesk in a panic to open the system before an important meeting supposedly begins are just a few examples of this well-tried penetration technique.

So what is a responsible company to do in fighting social engineering?

In one controversial method of penetration testing, consultants purposely break in to an organization’s IT systems using social engineering to demonstrate where the vulnerabilities are. Whether or not you agree with the concept of using social engineering in penetration testing, it is critical that your company implement the right kind of policies, procedures and education regarding the methods social engineers may employ.

Whereas some organizations actually conduct social-engineering penetration tests, others feel more comfortable using education without such trials.

But regardless of your stand on the issue, it's increasingly critical that everyone in an organization, from top executives down, fully understands the issues of social engineering. How do these hackers work? What are the simple do's and don'ts that employees should use to protect themselves? What kinds of suspicious calls and e-mails should an employee report?

For example, employees can be taught to report and not respond to any phone or e-mail request for any password. They should be taught to report any unknown person walking the premises without a identity badge. Helpdesk personnel can be taught to recognize the tactics incoming callers may have used to disguise their identity.

How can companies accomplish this goal? In addition to possible penetration testing or consulting, organizations are building comprehensive security policy resource centers. One of the recent examples of this concept is the NV Policy Resource Center, from my company, NetVision (managed by META Security Group). In this example, the NV Policy Resource Center is a subscriber-based Web service that provides automated training to test, track and document employees’ understanding and compliance with security policies.

For example, a company may issue a memo, a policy and even an educational program on social engineering. But in a typical scenario, the written policy document is never read and the program is damaged two weeks later when several new employees join the firm without training.
With one of the new automated resource programs, each new employee is taken through the security training as a Web-based program. At the end of the program, each employee is tested to measure their comprehension. Then they sign a formal compliance agreement. The training is administered in language the users understand, and the employer has now verified that the training was received, understood and accepted.

The organization can require compliance testing at set intervals, such as a year, or they can invoke compliance testing each time a critical new element is added to the company policy. The system can track compliance and can send out education and update materials from a database of best practices drawn from a variety of security organizations as well as from current events.

The main point of a resource center is that it's ongoing and it's automated. It can address user training and awareness at every level in an organization. It can address compliance issues such as HIPAA (Health Insurance Portability and Accountability Act of 1996) and GLBA (Gramm-Leach-Bliley Act of 1999), and it can also address human issues such as the newest tricks that might be tried by the unfortunately ever-creative society of social engineers.

* * *

About the author


* * *


MSIA: 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2003 Jim Allred. 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.