When was the last time you had to threaten to shoot an unauthorized executive who was demanding access to a secure area? Read on for a real-life story and an important lesson on effective security training (even without rifles).

Paul Schumacher had a long and distinguished career in the US Army in electronics. Now retired, he has been a faithful correspondent for many years and I always enjoy his comments. Today I am pleased to publish his analysis (and a terrific example) of intimidation as a social-engineering technique. What follows is Mr Schumacher’s comments with minor edits.

***

There is one form of social engineering that you missed – a form of bullying. An individual (or several) with the trappings of authority approaches the targeted individual and demands access to something that’s off-limits. The tester (or criminal) tries to intimidate the victim by using the implied authority of clothing (business, suit, lab coat, uniform) and force of personality (assurance, confidence, anger).

This technique was tried on me when I was a PFC (Private First Class) in the Army during a field exercise in Korea. I was guarding the van where we stored our cryptographic equipment when a Master Sergeant (E-8 – enlisted ranks go only to E-9) and Sergeant First Class (E-7) approached. I stopped and challenged them, but they demanded entry. I checked the access roster and told them that they could not enter, as they were not on it. They demanded to see the roster, but their attitude was annoying me, so I told them (correctly) that it was not for general distribution. They started into the passage through the wire demanding that I either give them entry or go contact my commanding officer. Now, this crypto equipment was the only gear for which defense using deadly force was authorized, so I chambered a round, which on an M-14 rifle is a very distinctive sound from simply cycling an empty rifle. They rushed the inner entry, threatening me with court marshal for having threatened them with lethal force and again demanded immediate entry. With the muzzle in the Master Sergeant's stomach, I clicked off the safety, letting the rifle do my talking. They finally backed down and left, uttering yet another threat of charges.

I stood there wondering if I were headed for trouble. An hour later, I was relieved for lunch, and during lunch, the First Sergeant stood me up before the company as an example of how to deal with these two sergeants who were evaluating the security readiness of the company. They had bullied their way into many of the company's various operations where they had no authority to do so even though the troops were authorized to use limited physical force to prevent unauthorized access by anyone. Most troops could have used simple non-cooperation to achieve the same denial of access. I was just glad that they had backed down, as I had been fully prepared to shoot them.

Many people do not have the strength of personality to stand up to bullying and to the threat of
official action. Having clear and precise directives as to what to do when confronted by a
challenge for access, with alternative actions if the first is not available (the person who could
authorize the access is unavailable, as in your example) is mandatory for people to resist this, and
many other, types of social engineering. It is the uncertainty that the social engineer exploits,
together with the desire of people to be helpful to others.

Simple, direct statements of policy work much better than overly-detailed, complex, cover-
everything, policies. People are more likely to read and follow understandable principles than to
wade through endless details of micromanagement. On the other hand, not having any policy at
all leaves people to make their own judgment, which may not be in the best interest of security.

In the next installment, Mr Schumacher looks at additional social-engineering techniques that
can be useful and which employees must be prepared to resist. He also suggests effective
approaches to employee training for such resistance.

* * *

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 <
mmailto: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.