A reader recently asked me why I consistently suggest that particular tidbits from my security columns and other sources be included in corporate newsletters about information security. Why should the enterprise be concerned about telling employees how to protect their families against, say, Nigerian advance-fee (“4-1-9”) fraud? What does that have to with corporate liability?

The benefit of including useful information about security that can help employees and their families comes from the psychological phenomenon called _internalization_. When we act in a particular way, we come to see ourselves in a new light: we integrate our behavior into a revised conception of ourselves.

This phenomenon is thought to explain the success of the notorious “foot-in-the-door” technique used by salespeople and social activists: get the customer / potential volunteer to agree to a small purchase / action and there’s a better chance that they’ll agree to a larger purchase / action later.

For example, when political activists are looking for places to put up a prominent sign in a new neighborhood, they don’t just baldly go up to any old house and ask, “May we put up this big sign on your lawn?” No, they start small. They’ll canvas the block and ask people, “Do you support < whatever the issue is >? You do? Great! Could you display this little postcard-sized sign in your window? You WILL? Oh, that’s wonderful! Thank you!!”

Naturally, a week later, the little sign marks those houses which should be visited again. This time, the request can be for permission to, say, put up a sign two feet square on a wooden stick at the edge of the lawn. The week after that, some of the people with lawn signs may agree to join a demonstration or put up a really big sign or whatever the next phase of the plan is.

Why does this technique work?

According to some psychologists, agreeing to the modest request sets up a change in self perception: “Oh, I guess I must be more interested in this than I thought.” Then when the next request arrives, the person seems to think something like, “Well, I suppose I really am interested in this after all – sure, go ahead.” Changing behavior a little makes it more likely that you can change behavior a lot.

Some employees who act to protect their families against information security threats may come to see themselves as security people; they internalize security as part of their own interests and value system. So when you ask them to cooperate at work on a security project, they may respond better than if they’ve never done anything security-related. You’ve converted some neutral bystanders into interested participants. Considering how inexpensive it is to include a paragraph about a useful security tip in a corporate newsletter that will be published anyway, the cost of the program is tiny compared to the potential benefits.
Besides, can you really argue against protecting children and families against bad cyberstuff? No, go ahead: put those little tidbits about save hex into your newsletters and let your employees bring security home.

Don’t worry – you’ll get it back.

* * *

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 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.