The training video “Stolen Access” from Commonwealth Films <http://www.commonwealthfilms.com> is subtitled, “Keeping Information Secure.” This 2003 production starts with a credible scenario demonstrating social-engineering techniques as industrial spies penetrate an organization by posing innocent-sounding questions to employees by phone. The criminals find the name and position of their target, his secretary’s name and their phone extensions. They pose as job applicants, new employees, and customers. They determine that their target is on holiday, that he has forgotten his new password, and who has the emergency password list. They impersonate the target’s sister-in-law, provide convincing sound effects to convince the keeper of the password list that the target is too ill to come to the phone, and achieve their objective: the target’s password. The criminals then steal copies of the target’s confidential files and read his e-mail for weeks. They sell the competitive information to competitors and cost the target’s company several contracts in competitive bids.

The film summarizes some warning signs that can indicate a social-engineering attack:

* The caller tries to frame his or her request as an emergency;

* Social engineers often invoke authority as a tool of intimidation;

* They may claim that there’s a technical emergency and offer or ask for technical help.

I’d add that a real bell-ringer is that they ask for passwords over the phone. Down boy! Bad social engineer. BAAAADDD social engineer! [Sorry, we have a new puppy and I’m getting into strange verbal habits.]

Advice from the technical consultants at Commonwealth Films on handling an unusual call:

* “If it seems wrong, assume it is wrong.”

* “If you’re uncomfortable, end the call.”

* “Don’t violate policy to ‘help’ a friend or associate.”

* Disclose only appropriate information.

* Report unusual calls.

The film continues with an interesting scenario demonstrating how eavesdropping on indiscreet conversations can allow an industrial spy to deduce passwords when employees use personal preferences and interests to secure their system access. Casual public conversations and overly-
explanatory, unencrypted directories and files make spies’ work too easy by half. The film provides excellent suggestions for choosing effective passwords.

Other scenarios in the film:

* Phishing scams using bogus “virus warning” e-mails and fake Web pages that ask for system logon information.

* Being too trusting at work by leaving confidential files accessible on a workstation session, discarding unshredded bad photocopies of confidential documents, leaving confidential documents in photocopies and on fax machines, and (yikes) putting password on Post-It™ notes.

* Using public wireless access points for communication of confidential data without virtual private network software.

* Bogus cellular phone calls asking users to input their PINs “to keep your service active.”

As always, this Commonwealth Film training video is a valuable contribution to corporate security awareness programs. Congratulations to writer and director Bruce McCabe, producer Jennifer Wry and veteran executive producer Thomas P. McCann.

[Note: The author has no financial interest whatsoever in Commonwealth Films. However, these nice people allow me to show their previews to my students in class and I am grateful to their Director of Customer Relations, David J. Burke, for his consistent kindness over many years.]

* * *

For further reading:

Other security-awareness film reviews by Mich Kabay:

* * *

A Master’s degree in the management of information assurance in 18 months of online study from Norwich University – see <http://www3.norwich.edu/msia> for details.

M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management 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 © 2004 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.