

Security Training Videos: “Targets of Opportunity”

**by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Dept. of Computer Information Systems
Norwich University, Northfield, VT 05663-1035 USA**

This series of short reviews is intended to help security-awareness officers evaluate training videos for their training programs. The author and his employer have no financial interest in or involvement with the companies whose products are reviewed.

* * *

The training video “Targets of Opportunity” from Commonwealth Films < <http://www.commonwealthfilms.com> > is subtitled, “The Human Factor.” As usual with this company’s consistently good productions, the video plunges into a realistic, exciting case study of a major lapse in security. A top-secret document gets sent by accident to three different locations around the world by fax because someone carelessly included it along with some low-security pages intended for the CEO.

The incident sparks an investigation ordered by a furious CEO and the company brings in a specialist on human factors in security. This expert simulates an industrial spy; he begins with a review of public documents about the company and then monitors the USENET for confidential information. He hits the jackpot when one of the research engineers reveals in a discussion group that both he and his assistant are planning to be away. The security expert visits their empty cubicles and opens up a \$15 set of tools to impersonate a phone technician. He rummages through their desks and finds access codes written down which then allow him to log on to the system using an R&D account. He orders delivery of confidential documents to the absent assistant’s desk by e-mail.

Later, he checks the recycling bins near photocopiers for documents that he can examine later, offsite. Unattended incoming and outgoing faxes, documents on unsecured network printers, and unlocked filing cabinets are all generous sources of valuable information to the spy.

The next day, a logged-on workstation gives the security expert access to the entire list of customers; in addition, because the absent user has write-access, the customer files would have allowed him to cause havoc by, for example, diverting shipments to the wrong addresses.

On day 3, the expert shows how indiscreet phone calls in public places can reveal critically important, sensitive data. The spy goes to a local restaurant where employees are carelessly talking openly about specific contracts, complete with names and details. He uses an overheard voice-mail access code to listen to a series of phone calls to one of the employees involved in a crucial bid and learns the bottom-line position for their offer – information of enormous value to a competitor.

The rest of the video continues with interesting, believable examples of the social-engineering skills of criminal hackers. The film then reviews the cases and asks viewers to answer some good

questions about their own awareness and working environment.

I think that this video will be a real eye-opener for employees who believe that only technical vulnerabilities matter. Thomas P. McCann, Executive Producer, and his colleagues Bruce McCabe, Peter McCann and Jennifer Wry have contributed a valuable tool for security awareness.

For further reading on industrial espionage, see

Winkler, I. (1997). *Corporate Espionage: What it is, why it is happening in your company, what you must do about it*. Prima Publishing (Rocklin, CA). ISBN 0-7615-0840-6.

Commonwealth Films are in Boston; phone 617-262-5634.

* * *

Information about M. E. Kabay, PhD, CISSP < <mailto:mkabay@norwich.edu> > is available at < <http://www2.norwich.edu/mkabay> >.

Copyright © 2003 M. E. Kabay. All rights reserved.