Security Training Videos:

"Look Out for Your Laptop"

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 "Look Out for Your Laptop" from Commonwealth Films < http://www.commonwealthfilms.com > is subtitled, "Information Security and Laptop Theft Prevention." The film starts wth a genial former thief who demonstrates exactly how thieves can take advantage of people attending conferences in hotels. "Frank" puts his laptop computer near the podium where he will be speaking, then goes out to grab some coffee and pastries. A woman with a similar computer bag exchanges hers for his – and five minutes later, Frank discovers that "his" bag contains a phone book. The commentator notes that Frank would never leave his wallet (with maybe fifty dollars in cash) out in the open, unattended, in a public place – but thinks nothing of abandoning his valuable laptop and all the corporate data it holds.

Next, Frank calls his IT manager, who tells him he will probably never see his laptop again. She asks if he has backups of his data; nope. She then explains to the viewer that reconstructing Frank's data would cost hundreds of times more than the price of the stolen hardware. In addition, the computer bag contained Frank's palmtop personal digital assistant (PDA) and his cell phone. The scene shifts to a motel room where three criminals are gloating over their booty. The PDA has passwords for the corporate systems and the cell phone is unsecured, allowing free long distance calls for a while. The corporate data on the laptop itself included user ID/password combinations for corporate systems, access codes of various kinds, autologon scripts for sensitive systems, and confidential corporate phone lists. The IT manager continues with vivid examples of the kinds of information that could be used for competitive intelligence, foreign spies, and terrorists.

In the case being discussed, Frank was attending a symposium on satellite telecommunications engineering; the scenario shows how the thieves, who had been paid to steal any laptop from that conference, are able to penetrate the secure communications channels and even interfere with satellite tracking.

We return to the genial former thief, who discusses risks at work. Leaving a computer on your desk, unprotected, overnight. Several scenarios are simulated: theft by a messenger, impersonation of cleaning staff for systematic laptop removal, and even insider theft by an office-mate who wants a spare computer at home. The IT manager recommends physical locking devices to make theft harder. She then turns to travel, and recommends that during

travel, camouflage the computer in a nondescript case. Conceal details of affiliation on luggage tags by using holders with flaps. Label the computer and carry locking devices with you.

The former thief illustrates the perils of careless travel: leaving the laptop unprotected while you nap; asking total strangers to watch your luggage while you get a snack; leaving your luggage unattended. When checking in, place the laptop on the counter. Don't check your computer, carry it on. If you have to put the computer down, say when you are phoning, grip the computer between your legs. [Sometimes I loop the carrying-case strap around my foot in such circumstances.]

We then see a clear demonstration of the notorious security-check scam. A "grabber" goes through before the victim; a decoy then waits for the laptop to be put on the X-ray machine belt and then slips into line in front of the victim. The decoy delays the victim by setting off alarms with metal; puts a coat through the scanner – anything to let the grabber seize the computer as it comes out of the X-ray machine. Good advice from the IT manager: wait until you are definitely next through the portal before placing the computer on the belt; and if you are intercepted, call out to the guards to watch your bag as you wait to go through.

On board the plane, avoid putting your laptop in the overhead bins, where it might fall; put it on the floor under the seat in front of you. The video shows why you should never leave laptops in your car – it's too easy to open those locked doors without a key. And in hotels, don't leave your laptop on your luggage even for a moment: thieves know that checking in is a time full of distractions and they often wait for the opportunity to walk off unnoticed with your computer. In the hotel room, don't leave your computer unattended at any time; lock it into the room safe or the hotel safe. Don't leave any confidential information lying around in hotel rooms, either.

The video shows kids using their dad's computer – and infecting it with malicious software. In addition, unauthorized users of a business laptop may end up sending e-mail in the user's name.

Users should also be prepared for disaster by keeping good backups; keep backup media in a different part of your luggage when you travel. Eliminate autologons, and saved passwords. Encrypt sensitive data according to policy. Keep information separately about what to do if you lose your computer so you can warn IT immediately of the theft and the network managers can initiate emergency measures on the networks.

The video was written by Webster Lithgow and Bruce McCabe; it was directed by McCabe and produced by Jennifer Wry. The technical advisors were from the Henry Consalves Co. and Kryptonite Corporation. The Executive Producer was Thomas P. McCann.

"Star Wars" it's not, but this short video packs a lot of practical information into a palatable medium for getting the message across to employees.

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 >.