REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understanding Physical Security 1.2
Topic: Understand physical security principles
(One 50-minute class period)
File name: SecurityFund_RL_1.2

Lesson Objective

1.2: Understand physical security. *This objective may include but is not limited to:* site security; computer security; removable devices and drives; access control; mobile device security; disable LogOn Locally; keyloggers.

Preparation Details

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_1.2
- Pictures, magazine articles, web pages and examples that your students can recognize and associate with the different threat types.
- See the *Additional notes to the instructor* at the bottom of this lesson.

Teaching Guide

Essential Vocabulary

access controls—the mechanisms for limiting access to certain items of information or to certain controls based on users' identities and their membership in various predefined groups. Access control is typically used by system administrators for controlling user access to network resources, such as servers, directories, and files.

keyloggers—keystroke logging (often called **keylogging**) is the process of recording the keys typed on a keyboard, typically without the users' knowledge.

site security—physical security is concerned with the protection of personal and business assets and premises through the use of security controls that restrict and manage the movement of people and equipment.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Student prompt (see PowerPoint® slide 3): On a sheet of paper, write down as many "site access controls" as you can.
2. Give students a few minutes to respond, allowing them to work until they have finished.
3. As time permits, call on a few students to report to the group with their responses.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
    a. Use the included PowerPoint slideshow to review the different types of site access controls, removable devices, mobile devices, and keyloggers.
    b. At the end of the slideshow, conduct a short group discussion about each example.
    c. Show the examples and give the students 1 minute to process the question and come up with answers.
    d. Finally, have each group of students share their findings with the whole group.
2. Guided Practice (20 minutes; see the "additional notes" section regarding this assignment)
    a. Have the students perform a "Building Site Threat Analysis" by observing your school, business, etc. Look for alarms, special door locks, cameras, etc.
    b. If time allows, have students note any hazards that could pose a threat to the premises.

Assessment/lesson reflection (10 minutes)

Use a "ticket out the door" to encourage the students to process the review and to give an opportunity for additional questions. The last slide in the PowerPoint facilitates this exercise:

1. On the same paper they used for the Site Threat Analysis, ask students to summarize the differences between "natural" and "man-made" threats, as directed on the final PowerPoint slide.
   - Be sure to give ample time for students to write their summaries.
   - If time allows, pick a few students to read their summaries.
2. At the bottom of the page, ask students to write down any questions they have or topics about which they would like more assistance
3. After class, look through the student responses and follow up with any student requiring additional help.

Microsoft resources and Web links

- **Microsoft® TechNet**
  http://technet.microsoft.com/en-us/library/bb457125.aspx
- **Microsoft Small Business Security Guidance Center**
  http://www.microsoft.com/smallbusiness/security.aspx

Additional notes to the instructor

- Before students perform the Guided Practice threat analysis survey activity (Lesson Activity #2 survey), ask permission from an administrator or manager. Do not enter any restricted areas without explicit permission.
- As part of the instructor preparation, get this permission and conduct your own threat assessment so you can anticipate what students will find.