STUDENT ACTIVITY 1.3 KEY: INTERNET SECURITY

MTA Course: 98-367 Security Fundamentals
Topic: Internet Security
File name: SecurityFund_SA_1.3_Key

Lesson Objective

1. 3: Understand Internet security. *This objective may include but is not limited to:* browser settings; zones; secure websites.

Resources, software, and additional files needed for this lesson

- None

Directions to the student

Answer the following questions.

Content:

1. Define the three major types of secure point-to-point communication. Do a "compare and contrast" of the three types:

   a. SSH Secure Shell
   Sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for getting secure access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely.

   b. IPSec
   A security mechanism under development by the IETF (Internet Engineering Task Force) designed to ensure secure packet exchanges at the IP (Internet Protocol) layer. IPSec is based on two levels of security: AH (Authentication Header), which authenticates the sender and assures the recipient that the information has not been altered during transmission, and ESP (Encapsulating Security Protocol), which provides data encryption in addition to authentication and integrity assurance.

c. SSL (Secure Sockets Layer) and TLS (Transport Layer Security)
A protocol developed by Netscape Communications Corporation for ensuring security and privacy in Internet communications. SSL supports authentication of client, server, or both, as well as encryption during a communications session. While primary purpose of SSL is to enable secure electronic financial transactions on the World Wide Web, it is designed to work with other Internet services as well. This technology, which uses public key encryption, is incorporated into the Netscape Navigator Web browser and Netscape's commerce servers.