REVIEW LESSON

MTA Course: 10753 Windows Operating System Fundamentals
Lesson name: Windows Operating System Fundamentals 3.3
Topic: Remove malicious software (One 50-minute class period)
File name: 10753_WindowsOS_RL_3.3

Lesson Objective

3.3: Remove malicious software. *This objective may include but is not limited to*: understanding Windows® Defender, Action Center, the Malicious Software Removal tool, Windows Registry, and Microsoft® Forefront® Endpoint Protection.

Preparation Details

Prerequisite student experiences and knowledge:

This MTA Certification Exam Review lesson is written for students who have learned about Microsoft Windows operating system fundamentals. Students who do not have the prerequisite knowledge and experiences cited in the objective will find additional learning opportunities using resources such as those listed in the "Resources" section at the end of this review lesson.

Instructor preparation activities:

- Make copies available of the Student Activity document 10753_WindowsOS_SA_3.3.
- The instructor should have access to an existing system running Windows 7 Professional or a virtual machine with Windows 7 Professional installed for the purpose of demonstrating how to remove malicious software.

Resources, software, and additional files needed for this lesson:

- The Malicious Software Removal Tool from Microsoft
  - Download from *http://www.microsoft.com/security/pc-security/malware-removal.aspx.*
  - The removal tool has both x86 and x64 versions.
- 10753_WindowsOS_RL_3.3
- 10753_WindowsOS_SA_3.3
- 10753_WindowsOS_SA_3.3_key
- 10753_WindowsOS_PPT_3.3

Teaching Guide

Essential Vocabulary

firewall—a program or device that monitors and regulates traffic between two points, such as a single computer and the network server or one server to another.

malicious software—software created and distributed for harmful purposes, such as invading computer systems in the form of viruses, worms, or innocent-seeming plug-ins and extensions that mask other destructive capabilities.

Registry—a central, hierarchical database in Windows used to store the information necessary to configure the system for one or more users, applications, and hardware devices. The Registry contains information that Windows continually references during operation, such as profiles for each user, the applications installed on the computer and the types of documents each can create, property sheet settings for folders and application icons, what hardware exists on the system, and which ports are being used.

spyware—a general term used to describe software that performs certain behaviors, generally without obtaining your consent. Spyware is often associated with software that displays advertisements (called *adware*) or software that tracks personal or sensitive information.

virus—a small software program designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on your computer, use your email program to spread itself to other computers, or even erase everything on your hard disk.

Lesson Sequence

Activating prior knowledge/lesson staging (5 minutes):

Direct students to answer each question in their notes.

1. What is a computer virus? (a small software program designed to spread from one computer to another and to interfere with computer operation)
2. What is Windows Defender? (software that helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software by detecting and removing known spyware from your computer)
3. What is a firewall? (a program or device that monitors and regulates traffic between two points, such as a single computer and the network server or one server to another)

Lesson activity (40 minutes):

1. Teacher instruction (20 minutes; see the "Suggested best practices" section below regarding this presentation).
2. Use the included Microsoft PowerPoint® presentation to review removing malicious software.
3. Guided practice (20 minutes):
   a. Direct students to complete the Student Activity document 10753_WindowsOS_SA_3.3.

Assessment/lesson reflection (5 minutes):

1. In the same notes that they created for the "Activating prior knowledge/lesson staging" at the beginning of the class, direct students to check their initial answers and make any changes if necessary.
2. Instruct students to write and submit any questions they have or any 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.

Resources:

- **Microsoft: Malware Protection Center**
  http://www.microsoft.com/security/portal/
- **Microsoft: Malicious Software Removal Tool**
  http://www.microsoft.com/security/pc-security/malware-removal.aspx
- **Microsoft: Resources: Microsoft Security Center**
  http://www.microsoft.com/security/resources/default.aspx#Security-terms
- **Microsoft: Spyware and Malware Protection: Security Essentials**
  http://www.microsoft.com/security_essentials/
- **Microsoft: Windows Defender: Home Page**
  http://www.microsoft.com/windows/products/winfamily/defender/default.mspx
- **Microsoft: Microsoft Forefront Endpoint Protection**
  http://www.microsoft.com/forefront/endpoint-protection/en/us/default.aspx
- **Microsoft: Action Center: Windows 7 Features**
  http://windows.microsoft.com/en-US/windows7/What-is-Action-Center

Additional activities (homework or enrichment):

- Encourage students to download and install Microsoft Security Essentials on their student workstations or their home PCs. This free download is a viable antivirus solution and is a great solution for personal use.

Suggested best practices:

- It is recommended to perform Quick Scans only with the tools mentioned in the activity. Full scans will be time-consuming.

Additional notes to the teacher:

- It is recommended to have the appropriate tools downloaded for the students prior to the activities. Be sure to download based on the hardware architecture (x86 or x64).
- It should be emphasized that regardless of what the tools may be able to do, you may have to explore the Registry to remove some viruses and malware completely. Students should be warned to back up their Registry before they attempt to make any changes to it.