REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understand Security Software
Topic: Understand e-mail protection
(One 50-minute class period)
File name: SecurityFund_RL_4.2

Lesson Objective

4.2: Understand e-mail protection. *This objective may include, but is not limited to:* anti-spam, anti-virus, spoofing, phishing, pharming, client vs. server protection, SPF records, PTR records.

Preparation Details

Instructor preparation activities

- Make copies of Student Activity SecurtyFund_SA_4.2

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_4.2
- SecurityFund_SA_4.2
- SecurityFund_SA_4.2_Key

Teaching Guide

Essential Vocabulary

spam—unsolicited, unwanted e-mail sent by someone with whom the recipient has no personal or business relationship.

anti-virus—a computer program that scans a computer's memory and mass storage to identify, isolate, and eliminate viruses, and that examines incoming files for viruses as the computer receives them.

phishing and pharming—a technique used to trick computer users into revealing personal or financial information. A common online phishing scam starts with an e-mail message that appears to come from a trusted source but actually directs recipients to a fraudulent website configured to steal personal information.

PTR records—a reverse lookup record for the server, also known as a PTR resource record, is registered in a reverse lookup zone in the DNS database.

SPF records—an extension of the SMTP protocol that prevents spammers from forging the From: fields in e-mail messages by verifying that the IP address in the SMTP Received: header is authorized to send e-mail for the sender's domain.

spoofing—the impersonation of an e-mail sender, IP connection, or a domain that causes an e-mail message to appear as though it originates from a sender other than the actual sender of the message.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 5 minutes)

1. Student prompt (see PowerPoint® slide 4): On a sheet of paper, record your experiences with spam e-mail.
2. Give students a few minutes to research and 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 (35 minutes)

1. Teacher Instruction (20 minutes)
    - Use the included PowerPoint slides to review “phishing and pharming”.
    - At the end of the slide 7, Show the video: *What you should know about phishing identity-theft scams (http://www.microsoft.com/athome/security/email/phishing/video1.mspx).*
        - Learn more about **phishing** e-mail scams and how they are used for identity theft. Learn how fraudulent e-mail messages and spoofed Web sites—two common forms of phishing—can trick users into sending personal information, such as a credit card number, to an identity thief. You'll also learn three things you can do to protect yourself from being hooked by a phishing scam.
    - At the end of the video, students can take the quiz linked at the bottom of the webpage: "Can you spot a phishing scam?".
    - Have each student share his/her answers with the whole group.

2. Guided Practice (20 minutes; slide 13)
    - Demonstrate or have students complete the "Analyzer", identifying the different types of Windows® remote connectivity.
    - Give students a few minutes to research and respond, allowing them to work until they have finished.
    - As time permits, call on a few students to report to the group with their responses

Assessment/lesson reflection (10 minutes)

1. Show the video associated with slide 14: *How Do I: Enable the Anti-spam Agent in a Single Server Exchange Server Environment?* (*http://technet.microsoft.com/en-us/exchange/dd251269.aspx*).
    - On the same paper they used for the Anticipatory Set, students summarize what they learn from the video.
    - 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, tell students to write 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.

Microsoft® resources and Web links

- **Microsoft Exchange Remote Connectivity Analyzer**
  https://www.testexchangeconnectivity.com/#&&/wEXAQUBcwUBME93h2+JjI0+MV2gTqcRL0g43z9m
- **Microsoft Exchange Server TechCenter 2003: How Do I: Enable the Anti-spam Agent in a Single Server Exchange Server Environment?**
  http://technet.microsoft.com/en-us/exchange/dd251269.aspx
- **MS Security at Home: What you should know about phishing identity-theft scams**
  http://www.microsoft.com/athome/security/email/phishing/video1.mspx
- **Q&A: Microsoft Adds New Spam Filtering Technology Across E-Mail Platforms**
  http://www.microsoft.com/presspass/features/2003/nov03/11-17spamfilter.mspx