STUDENT ACTIVITY 4.2_KEY: EMAIL PROTECTION

MTA Course: 98-367 Security Fundamentals
Topic: E-mail Protection
File name: SecurityFund_SA_4.2_Key

Lesson Objective

4.2: Understand email 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.

Resources, software, and additional files needed for this lesson

- Internet access

Directions to the student

Answer the following questions.

Content

1. How can a pharming attacker redirect my Web browser to another site?

   Answer: Attackers access the giant databases that Internet providers use to route Web traffic. Once inside, they can make modifications on the spot so that you are diverted to the criminal site before you access the site you intended. This is called "DNS poisoning". (*http://www.microsoft.com/australia/protect/yourself/phishing/pharming.mspx*)

2. Some companies claim that their firewall software also works against pharming. Is this true?

   Answer: Some Web privacy providers claim that customers who route all their Internet activity through their own secure servers are protected against pharming attacks.

   The nature of pharming seems to suggest otherwise, but regardless of a company's claims, it's always a good idea to research security products carefully.

   Before you invest in and rely on any software solutions, read product reviews from reputable sources, such as CNET Reviews.

3. Can't I tell that a website is false simply by moving the cursor over the links and seeing if the code goes to an apparently random number off the site?

   Answer: Not necessarily. The false websites used in pharming scams usually "spoof" (*http://www.microsoft.com/security/incident/spoof.mspx*) their links so that they look exactly like the ones you expect to see, even in the code that appears when you place your cursor over them.

   Also, websites may change the code in their own links from time to time for various internal reasons, such as when they upgrading their software, server platform, and customer traffic analysis methods.

4. Why is pharming spelled with a "ph" instead of an "f"?

   Answer: It's part of an underground slang system that began with "phone phreaking": using electronics to hack into telephones and get free calls. Read about it in our Parent's primer to computer slang (*http://www.microsoft.com/protect/family/activities/leetspeak.mspx*).