

## **Real-World Scenario 2-2: Filtering and Screening E-mail**

**Scenario:** You are the security administrator for a midsized organization. One of your many tasks is to train users to filter and/or screen their e-mails.

E-mail vetting (screening) has become increasingly necessary over the past decade due to the amount of spam that dominates the Internet. Imagine how you might reduce the amount of spam (which everyone gets at some point) in Outlook e-mail accounts and free web-based e-mail accounts such as Gmail. Write down your answers and compare them with the following solution.

## Real-World Scenario 2-2 Solution

Spam and other junk mail is prevalent in today's e-mail communications. There are so many sources of junk mail that it is impossible to stop altogether; however, through filtering and user education (e-mail screening) it can be reduced to a manageable level.

One way to do this is to increase the level of security for junk e-mail. E-mail applications such as Outlook offer this feature. Another way is to set up filters either through third-party software locally, at the e-mail server (be it in-house or on the Internet), or by using a filtering appliance, such as the Barracuda devices mentioned in Chapter 2. The use of blacklisting (and/or whitelisting) can help with re-occurring spam. However, the best method is to train users to scan their e-mails carefully, deleting any that appear suspicious, and by all means to not open any attachments from an unknown source. While deleting the e-mail, the domain it came from can be marked as blacklisted as well, so that any e-mails originating from that domain (any e-mail address on that domain) will be automatically blocked.

**Simulation:** Complete the simulation "2-2: Filtering E-mails."