User Guide

Table of Contents

Chapter 1 - Getting Started

Welcome to McAfee.com VirusScan Online.

McAfee.com VirusScan Online is an online subscription service offering you comprehensive, reliable, and up-to-date virus protection. Powered by our state-of-the-art Olympus scanning engine, VirusScan Online protects against viruses, worms, Trojan horses, malicious scripts, and hybrid attacks.

With it, you get the following features:

ActiveShield - Scan files in real-time when they are accessed by either you or your computer.

Scan - Search for viruses in hard drives, floppy disks, and individual files and folders.

Quarantine - Encrypt and temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken.

Rescue Disk - Create a bootable floppy disk to start your computer and scan it for viruses if a virus keeps you from starting it normally.

New Features

This version of VirusScan Online provides the following new features:

- **Automatic file infection cleaning**
  VirusScan Online automatically attempts to clean infected files when an infection is detected.
- **Scheduled scanning**
  You can now schedule automatic scanning at specified intervals to thoroughly check your computer for viruses.
- **McAfee.com SecurityCenter integration**
  Seamless integration with the McAfee.com SecurityCenter provides a consolidated view of your computer's security status, plus the latest security and virus alerts. You can run SecurityCenter from the McAfee.com icon in your Windows system tray or from your Windows desktop.
- **File quarantine**
  You can use the Quarantine feature to encrypt and temporarily isolate infected and suspicious files in the quarantine folder until an appropriate action can be taken. Once cleaned, a quarantined file can then be restored to its original location.
- **Incremental virus signature (.dat) file updates**
  Smaller virus signature (.dat) files now drastically reduce the amount of time it takes to download VirusScan Online weekly updates.
- **Security alerts**
  Part of an emergency broadcast system, security alerts inform you about virus outbreaks and other security-related events. Once alerted, you can choose to remove the threat or to learn more about it.
- **Microsoft® Windows XP compatibility**
  VirusScan Online is now compatible with Windows XP.
- **Heuristic scanning**
  VirusScan Online now uses heuristic scanning techniques to detect new viruses by checking for telltale signs.
- **Offline scanning**
  You can now use VirusScan Online without needing to be connected to the Internet. (Previous versions required you to be connected to our Web site). VirusScan Online is now installed on your computer and kept up-to-date via weekly updates.
- **Virus Map reporting**
  You can now anonymously send virus tracking information for inclusion in our World Virus Map. You can automatically register for this free, secure feature and view the latest worldwide infection rates via the McAfee.com SecurityCenter.
- **More frequent checking for updates**
  ActiveShield now automatically checks for updates every four hours (rather than once a day) when you are connected to the Internet. This ensures that you get the latest updates during a virus outbreak.
- **Auto-detection and removal of conflicting software**
  The Installation Wizard now automatically detects and removes other anti-virus software installed on your computer to help prevent potential conflicts with your VirusScan Online installation.

System Requirements

- Microsoft® Windows 95, 98, Me, 2000, or XP
- Personal computer with 486 or higher processor (Pentium recommended)
- 16 MB RAM minimum; 32 MB RAM recommended
- 35 MB of free hard disk space (for installation)
- Microsoft® Internet Explorer 5.0 or higher

  Note: To upgrade to the latest version of Internet Explorer, visit the Microsoft Web site at http://www.microsoft.com/.

Downloading and Installing VirusScan Online

Before you can download and install VirusScan Online, you must purchase a subscription. To do so, go to the McAfee.com Web site, and create an account with a password and billing information to sign up for the service.

Before installing VirusScan Online, save all of your work and close any open applications before you continue with the following installation steps. After installing VirusScan Online, you must restart your computer.

Note: If you are upgrading from a previous version of VirusScan Online, VirusScan Online will automatically uninstall the previous version before it installs the current version. You must restart your computer when the Installation Wizard prompts you. After your computer restarts, the current version of VirusScan Online will install.

To install VirusScan Online:

1. Go to http://www.mcafee.com/, and click **My Account**.
2. If prompted, enter your subscribing email address and password, and then click **Log In** to open your **Account Info** page.
3. Locate **VirusScan Online** in **Your Web Services** list, and click the **Update/Download** icon.
4. If any dialog boxes appear, click **Yes** to continue. If the Installation Wizard does not appear automatically, click **Start**.
   If the Installation Wizard detects other anti-virus software installed on your computer, a list of detected products appears.
5. Click **Yes** (strongly recommended) to remove the detected products, and then restart your computer to continue the installation.
   When your computer restarts, the Installation Wizard dialog box appears again, prompting you to continue the installation.
6. Click **Next** to continue installing VirusScan Online.
   The Virus Map Reporting dialog box appears.
   a. Accept the default **Yes, I want to participate** option to anonymously send your virus information to McAfee.com for inclusion in its World Virus Map of worldwide infection rates. Otherwise, select **No, I don't want to participate** to avoid sending your information.
      Note: You can also configure this option at any time in the **Virus Map Reporting** tab of the VirusScan Online Options dialog box.
   b. If you are in the United States, select the state and enter the zip code where your computer is located. Otherwise, select the country where your computer is located. When you are finished, click **Next** to continue.
7. If the Installation Wizard prompts you, click **Restart** to restart your computer.
   A welcome dialog box appears when Windows restarts after the installation.
8. Click **What's New** to read about new product features, and then click **Scan for Viruses** to perform an initial scan of your computer for viruses.
   The Scan for Viruses dialog box appears and begins to perform an initial scan on your computer using the default scanning options. See "Manually Scanning for Viruses" for details.
9. When the scan is finished, click **Close** to exit Scan.

Testing VirusScan Online

Before initial use of VirusScan Online, it's a good idea to test your installation. Use the following steps to separately test the ActiveShield and Scan features.

Testing ActiveShield

To test ActiveShield:

1. Go to http://www.eicar.com/.
2. Click the **The AntiVirus testfile eicar.com** link.
3. Scroll to the bottom of the page. Under Download, you will see four links.
4. Click **eicar.com**.

If ActiveShield is working properly, it detects the eicar.com file immediately after you click the link. You can try to delete or quarantine infected files to see how ActiveShield handles viruses. See "If ActiveShield Finds a Virus" for details.

If ActiveShield did not detect the eicar.com file, please see "ActiveShield Fails to Detect the EICAR Test File" in the troubleshooting section.

Testing Scan

Before you can test Scan, you must download the test files and then move them to another folder.

To download the test files:

1. Disable ActiveShield: Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Disable**.
2. Download the EICAR test files from the EICAR Web site:
   a. Go to http://www.eicar.com/.
   b. Click the **The AntiVirus testfile eicar.com** link.
   c. Scroll to the bottom of the page.
   Under **Download**, you will see these links:
      - **eicar.com** contains a line of text that VirusScan Online will detect as a virus. #*
      - **eicar.com.txt** (optional) is the same file, but with a different file name, for those users who have difficulty downloading the first link. Simply rename the file "eicar.com" after you download it. #*
      - **eicar_com.zip** is a copy of the test virus inside a .zip compressed file (a WinZip™ file archive). *
      - **eicarcom2.zip** is a copy of the test virus inside a .zip compressed file, which itself is inside a .zip compressed file. *

      # The ActiveShield feature detects these file types.
      * The Scan feature detects these file types.

   d. Click each link to download its file. For each one, a File Download dialog box appears. Locate a temporary directory, click **Save**, and then click **Save** again in each Save As dialog box.
3. When you are finished downloading the files, close Internet Explorer.

To move the test files into another folder:

1. In Windows Explorer, double-click the My Computer icon.
   The My Computer window opens.
2. Double-click the icon for your computer's hard drive (usually drive C).
   A window opens showing the contents of the hard drive.
3. Right-click an area (not a folder) on the window, point to **New**, and then click **Folder**.
   A folder named "New Folder" appears.
4. Rename the folder "VSO Scan Folder."
5. Drag each file from your desktop into the VSO Scan Folder.
6. Enable ActiveShield: Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Enable**.

To test Scan:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Scan for Viruses**.
2. Using the directory tree in the left pane of the dialog box, go to the VSO Scan Folder where you saved the files:
    a. Click the **+** sign next to the Primary (C:) icon.
    b. Click the VSO Scan Folder to highlight it (do not click the **+** sign next to it).
    This tells Scan to check only that folder for viruses. You can also put the files in random locations on your hard drive for a more convincing demonstration of Scan's abilities.
3. In the **Scan Options** area of the Scan for Viruses dialog box, make sure that all options are selected.
4. Click **Scan** on the lower right of the dialog box.
    VirusScan Online scans the VSO Scan Folder. The files that you saved to that folder will appear in the List of Infected Files. If so, Scan is working properly.

You can try to delete or quarantine infected files to see how Scan handles viruses. See "If Scan Finds a Virus" for details.

If Scan did not detect the eicar.com file, please see "Scan Fails to Detect One or More of the EICAR Test Files" in the troubleshooting section.

Using McAfee.com SecurityCenter

The McAfee.com SecurityCenter is your one-stop security shop, accessible from its icon in your Windows system tray or from your Windows desktop. With it, you can perform these useful tasks:

- Get free security analysis for your PC.
- Launch, manage, and configure all your McAfee.com subscriptions from one icon.
- See continuously updated virus alerts and the latest product information.
- Receive free trial subscriptions to download and install trial versions directly from McAfee.com using our patented software delivery process.
- Get quick links to frequently asked questions and account details at the McAfee.com Web site.

Note: For more information about its features, please click **Help** in the SecurityCenter dialog box.

While the SecurityCenter is running and all of the McAfee.com features installed on your computer are enabled, a red M icon appears in the Windows system tray. This area is usually in the lower-right corner of the Windows desktop and contains the clock.

If one or more of the McAfee.com applications installed on your computer are disabled, the McAfee.com icon changes to black .

To open the McAfee.com SecurityCenter:

1. Right-click the McAfee.com icon .
2. Click **Open SecurityCenter**.

To access a VirusScan Online feature:

1. Right-click the McAfee.com icon .
2. Point to **VirusScan Online**, and then click the feature you want to use (see Figure 1).

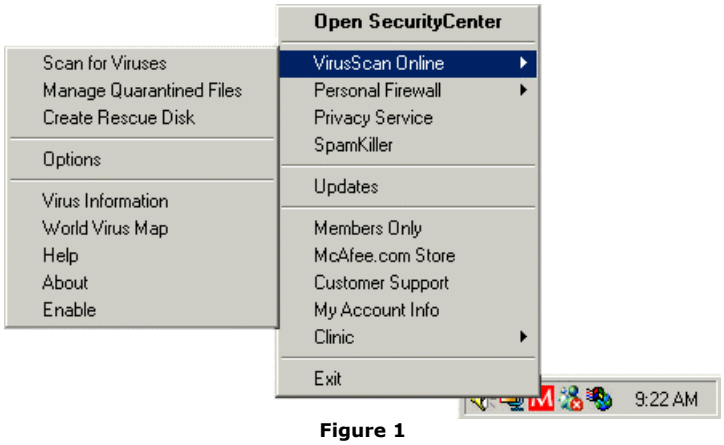

Figure 1

To accomplish additional tasks at the McAfee.com Web site via the McAfee.com icon, click the following menu items:

Virus Information - View information about viruses (including alerts, library definitions, glossary terms, and cleaning methods).

World Virus Map – View worldwide infection statistics.

Members Only – Get special offers and discounts for valued members.

McAfee.com Store – Get news, product information, and promotional offers for our other security products.

Customer Support – Get help, send feedback, and report bugs or problems.

My Account Info – View your subscription status.

Clinic – Access additional McAfee.com services to enhance your computer's performance.

Chapter 2 – Using McAfee.com VirusScan Online

Note: Windows 2000 and Windows XP users must have Administrator rights to configure the ActiveShield and Virus Map reporting options.

Using ActiveShield

When ActiveShield is started (loaded into computer memory) and enabled, it is constantly protecting your computer. ActiveShield scans files when they are accessed by either you or your computer. When ActiveShield detects an infected file, it automatically tries to clean the virus, or to delete the entire infected file.

Warning:

- VirusScan Online and ActiveShield are not upgrades from McAfee VirusScan v4.x, 5.x, or 6.x. If you have McAfee VirusScan on your computer, you must remove it so ActiveShield runs correctly.
- Software packages such as Guard Dog, Nuts & Bolts, First Aid, McAfee Office, and Microsoft Plus! might have versions of McAfee VirusScan bundled with them. You must remove the anti-virus components from these applications before ActiveShield will function properly.

Enabling or Disabling ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by red M) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (not loaded) or is disabled (denoted by black M), you can manually run it, as well as configure it to start automatically when Windows starts.

Enabling ActiveShield

To enable ActiveShield for this Windows session only:

Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Enable**. The McAfee.com icon changes to red M.

If ActiveShield is still configured to start when Windows starts, a message tells you that you are now protected from viruses. Otherwise, a dialog box appears that lets you configure ActiveShield to start when Windows starts (see Figure 2).

Figure 2

Disabling ActiveShield

To disable ActiveShield for this Windows session only:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Disable**.
2. Click **Yes** to confirm.

   The McAfee.com icon changes to black  .

If ActiveShield is still configured to start when Windows starts, your computer will be protected from viruses again when you restart your computer.

Configuring ActiveShield Options

You can modify ActiveShield starting and scanning options in the **ActiveShield** tab of the VirusScan Online Options dialog box, which is accessible via the McAfee.com icon  in your Windows system tray.

Starting ActiveShield

ActiveShield is started (loaded into computer memory) and enabled (denoted by red ) by default as soon as you restart your computer after the installation process.

If ActiveShield is stopped (denoted by black ), you can configure it to start automatically when Windows starts (recommended).

Note: During updates to VirusScan Online, the Update Wizard might exit ActiveShield temporarily to install new files. When the Update Wizard prompts you to click Finish, ActiveShield starts again.

To start ActiveShield automatically when Windows starts:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**.
   The VirusScan Online Options dialog box opens.
2. Select the **Start ActiveShield when Windows starts (recommended)** check box, and then click **Apply** to save your changes.
3. Click **OK** to confirm, and then click **OK**.

Stopping ActiveShield

Warning: If you stop ActiveShield, your computer will not be protected from viruses. If you must stop ActiveShield, other than for updating VirusScan Online, please make sure that you are not connected to the Internet.

To stop ActiveShield from starting when Windows starts:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**.
   The VirusScan Online Options dialog box opens.
2. Clear the **Start ActiveShield when Windows starts (recommended)** check box, and then click **Apply** to save your changes.
3. Click **OK** to confirm, and then click **OK**.

Scanning All Files

If you set ActiveShield to use the **All files** option, it scans every file type that your computer uses, as your computer attempts to use it.

Note: Scanning all files can slow down your computer and is not recommended for everyday use.

To set ActiveShield to scan all file types:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**.
   The VirusScan Online Options dialog box opens.
2. Click **All files**, and then click **OK**.

Scanning Program Files and Documents Only
If you set ActiveShield to use the default **Program files and documents only (recommended)** option, it scans program files and documents, but not any other files used by your computer. The latest virus signature file (.dat file) determines which file types that ActiveShield will scan.

To set ActiveShield to scan program files and documents only:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**. The VirusScan Online Options dialog box opens.
2. Click **Program files and documents only (recommended)**, and then click **OK**.

Scanning Email Attachments
ActiveShield automatically scans email attachments when you try to open them or save them to your hard drive. For your protection, this feature cannot be disabled.

For maximum protection, do not open email attachments directly from an email message. Save them to your hard drive first, and then open them. If an attachment contains a virus, ActiveShield detects it when you try to save it to your hard drive.

If ActiveShield Finds a Virus

If ActiveShield finds a virus, a Virus Has Been Detected dialog box similar to Figure 3 appears. For most viruses, Trojans, and worms, ActiveShield automatically tries to clean the file.

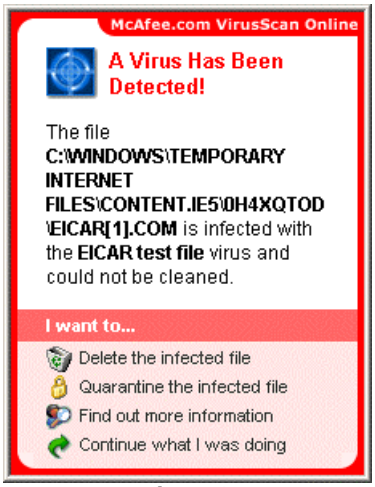

Figure 3

If ActiveShield can clean the virus, you can learn more or ignore the alert:

- Click **Find out more information** to view the name, location, and virus name associated with the infected file.
- Click **Continue what I was doing** to ignore the alert and close the dialog box.

If ActiveShield cannot clean the virus, you can delete or quarantine the file:

1. Click **Delete the infected file** to try to remove the file.
2. If ActiveShield cannot clean or delete the file, you can do one of these actions:
    - Click **Quarantine the infected file** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken. A confirmation message appears and prompts you to check your computer for viruses. Click **Scan** to complete the quarantine process.
    - Click **Find out more information** to view the name, location, and virus name associated with the infected file.
    - Click **Continue what I was doing** to ignore the alert and close the dialog box.

If ActiveShield cannot clean or delete the file, please consult the Virus Information Library at http://vil.mcafee.com/ for instructions on manually deleting the virus.

If the virus prevents you from using your Internet connection or from using your computer at all, try using a Rescue Disk to start your computer. The Rescue Disk, in many cases, can start a computer if a virus disables it. Please see "Creating a Rescue Disk" for details.

If all of the above fails, please call McAfee.com Customer Support at (408) 992-8599 for your fee-based telephone options.

Scanning Your Computer for Viruses

The Scan feature lets you selectively search for viruses on hard drives, floppy disks, and individual files and folders. When Scan finds an infected file, it automatically tries to clean the file. If Scan cannot clean the virus, you can delete or quarantine the file.

Manually Scanning for Viruses

To scan your computer:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Scan for Viruses**.
   The Scan for Viruses dialog box opens (see Figure 4).

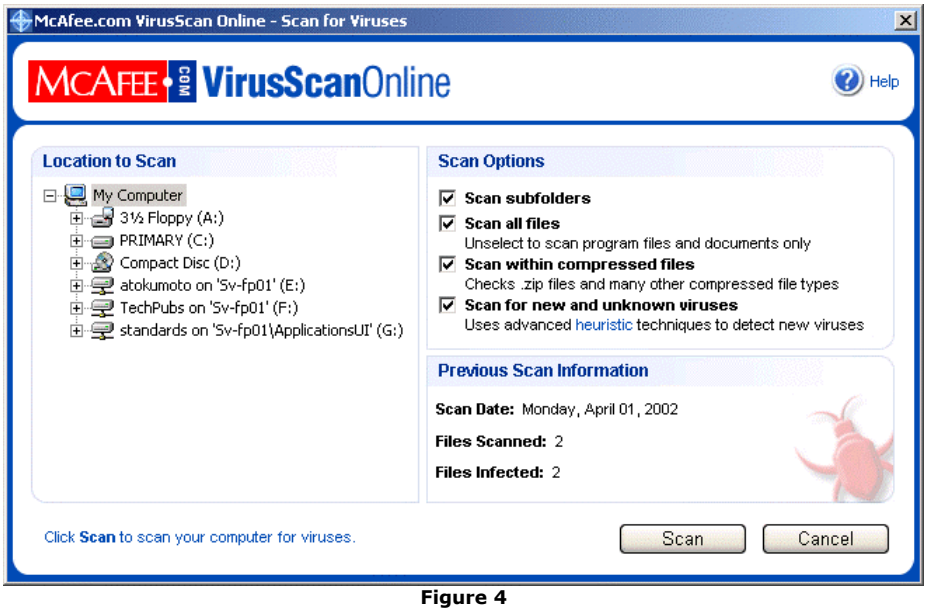

Figure 4

2. Click the drive, folder, or file that you want to scan.
3. Select your Scan Options. By default, all of the Scan Options are pre-selected to provide the most thorough scan possible (see Figure 4):

   Scan subfolders - Use this option to scan files contained in your subfolders. Clear this check box to allow checking of only the files visible when you open a folder or drive.

   Example: The files in Figure 5 are the only files scanned if you clear the **Scan subfolders** check box. The folders and their contents are not scanned. To scan those folders and their contents, you must leave the check box selected.

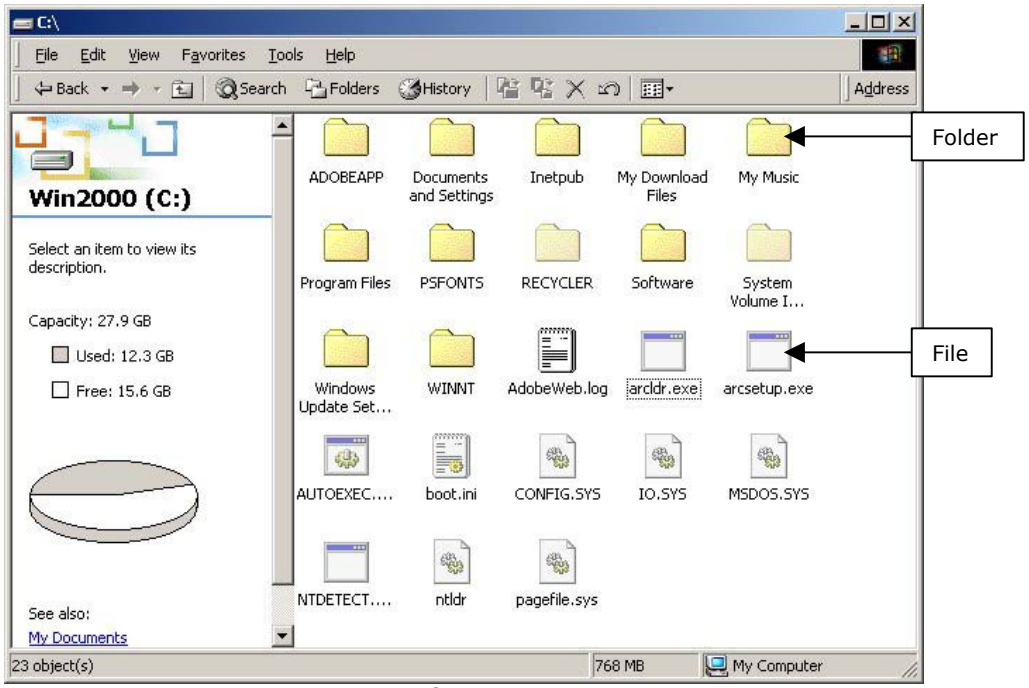

Figure 5

Scan all files – Use this option to allow the thorough scanning of all file types. Clear this check box to shorten the scanning time and allow checking of program files and documents only.

Scan within compressed files - Use this option to reveal hidden infected files within .zip and other compressed files. Clear this check box to prevent checking of any files or compressed files within the compressed file.

Sometimes virus authors plant viruses in a .zip file, and then insert that .zip file into another .zip file in an effort to bypass anti-virus scanners. Scan can detect these viruses as long as you leave this option selected.

Scan for new and unknown viruses - Use this option to find the newest viruses that might not have existing "cures." This option uses advanced heuristic techniques that try to match files to the signatures of known viruses, while also looking for telltale signs of unidentified viruses in the files.

This scanning method also looks for file traits that can generally rule out that the file contains a virus. This minimizes the chances that Scan will give a false indication. Nevertheless, if a heuristic scan detects a virus, you should treat it with the same caution that you would treat a file that you know contains a virus.

This option provides the most thorough scan, but is generally slower than a normal scan.

Note: Leave all options selected for the most thorough scan possible. This effectively scans every file in the drive or folder that you select, so allow plenty of time for the scan to complete. The larger the hard drive and the more files you have, the longer the scan will take.

4. Click **Scan** to start scanning files. When the scan is finished, a list of any infected files appears in the Scan for Viruses dialog box (see Figure 6).

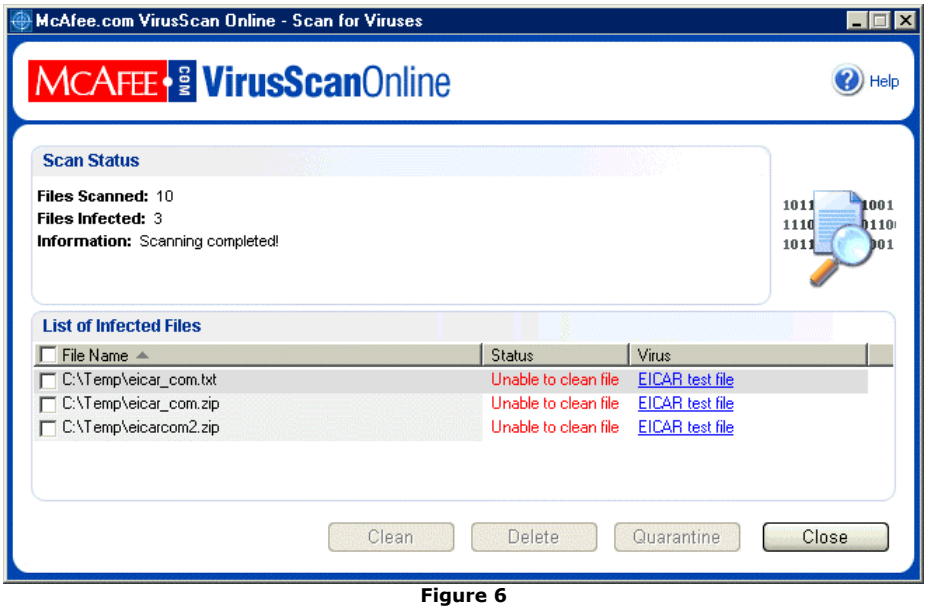

Figure 6

Note: Scan counts a compressed file (.zip, .cab, etc.) as one file within the **Files Scanned** number. Also, the number of files scanned can vary if you have deleted your temporary Internet files since your last scan.

5. If Scan finds no viruses, click **Back** to select another drive or folder to scan, or click **Close** to close the dialog box.

Automatically Scanning for Viruses

Although VirusScan Online scans files when they are accessed by either you or your computer, you can schedule automatic scanning in Windows Scheduler to thoroughly check your computer for viruses at specified intervals.

To schedule a scan:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**. The VirusScan Online Options dialog box opens.
2. Click the **Scheduled Scan** tab (see Figure 7).

Figure 7

3. Select the **Scan My Computer at a scheduled time** check box to enable automatic scanning.
4. Define a schedule for automatic scanning:
    - To accept the default schedule (8PM every Friday), click **OK**.
      - or –
    - To edit a schedule:
        a. Click **Edit**.
        b. Click the **Show multiple schedules** check box to display a list of available schedules at the top of the dialog box. Click **New** to add a new schedule to the list that you can edit, or click **Delete** to remove one.
        c. Select the schedule in the list.
        d. Select how often to scan your computer in the **Frequency** list, and then select additional options in the dynamic area below it:

           Daily - Specify the number of days between scans.

           Weekly (the default) - Specify the number of weeks between scans as well as the names of the day(s) of the week.

           Monthly – Specify which day of the month to scan. Click **Select Months** to specify which months to scan, and click **OK**.

           Once – Specify which date to scan.

           At system startup – Select to automatically scan your computer at every Windows startup.

           At user logon – Select to automatically scan your computer every time a user logs on to your computer.

           When idle - Specify the number of minutes that your computer must be idle for a scan to start.

        e. Select the time of day to scan your computer in the **Start time** box.
        f. To select advanced options, click **Advanced.**
           The Advanced Schedule Options dialog box opens.
            i. Specify a start date, end date, duration, end time, and whether to stop the task at the specified time if the scan is still running.
            ii. Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.
5. Click **OK** to save your changes and close the dialog box. Otherwise, click **Cancel**.
6. To revert to the default schedule, click **Set to Default**. Otherwise, click **OK**.

If Scan Finds a Virus

For most viruses, Trojans, and worms, Scan automatically tries to clean the file.

If Scan cannot clean the virus, you can delete or quarantine the file:

1. If a file appears in the list of infected files, click the check box in front of the file to select it. **Note:** If more than one file appears in the list, you can select the check box in front of the **File Name** list to perform the same action on all of the files. You can also click the virus name in the **Virus** list to view details from the Virus Information Library.
2. If Scan cannot clean the virus, click **Delete** to remove the file.
3. If Scan cannot clean or delete the file, you can do one of the following actions:
    - Click **Quarantine** to encrypt and temporarily isolate infected and suspicious files in the quarantine directory until an appropriate action can be taken. (See "Managing Quarantined Files" for details.)
    - Click **Cancel** to close the dialog box without taking any further action.

If Scan cannot clean or delete the virus, please consult the Virus Information Library at http://vil.mcafee.com/ for instructions on manually deleting the virus.

If the virus prevents you from using your Internet connection or from using your computer at all, try using a Rescue Disk to start your computer. The Rescue Disk, in many cases, can start a computer if a virus disables it. Please see "Creating a Rescue Disk" for details.

If all of the above fails, please call McAfee.com Customer Support at (408) 992-8599 for your fee-based telephone options.

Managing Quarantined Files

The Quarantine feature encrypts and temporarily isolates infected and suspicious files in the quarantine directory until an appropriate action can be taken. Once cleaned, a quarantined file can then be restored to its original location.

To manage a quarantined file:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Manage Quarantined Files**.
   A list of quarantined files appears (see Figure 8).

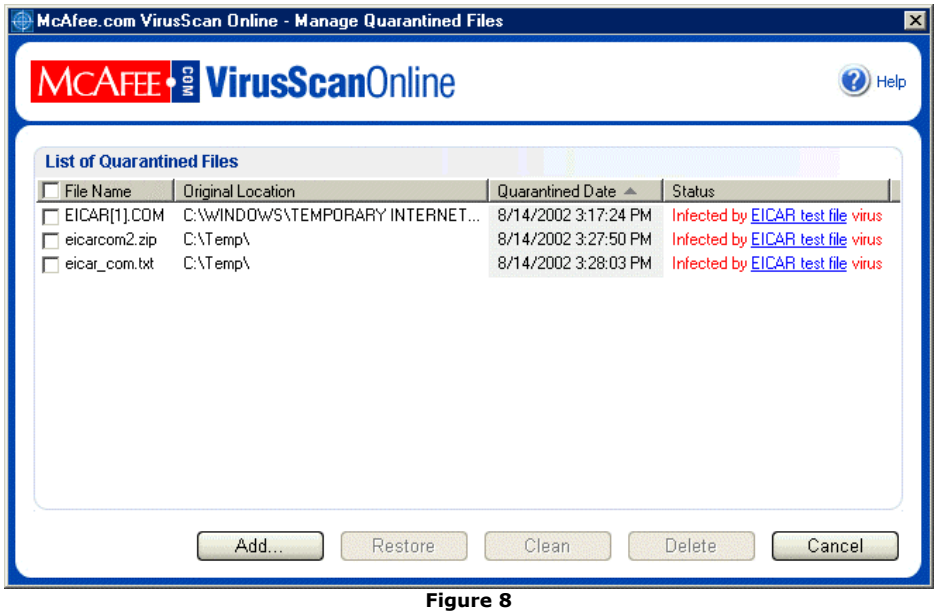

Figure 8

2. Select the check box next to the file(s) you want to clean.
   Note: If more than one file appears in the list, you can select the check box in front of the **File Name** list to perform the same action on all of the files. You can also click the virus name in the **Status** list to view details from the Virus Information Library at McAfee.com.
   - or -
   Click **Add**, select a suspicious file to add to the quarantine list, click **Open**, and then select it in the quarantine list.
3. Click **Clean**.
4. If the file is cleaned, click **Restore** to move it back to its original location.
5. If VirusScan Online cannot clean the virus, click **Delete** to remove the file.
6. If VirusScan Online cannot clean or delete the file, click **Cancel** to close the dialog box without taking any further action.

Creating a Rescue Disk

Rescue Disk is a utility that creates a bootable floppy disk that you can use to start your computer and scan it for viruses if a virus keeps you from starting it normally.

Note: You must be connected to the Internet to download the Rescue Disk image. Also, Rescue Disk is available for computers with FAT (FAT 16 and FAT 32) hard drive partitions only. It is unnecessary for NTFS partitions.

To create a Rescue Disk:

1. On a non-infected computer, insert a non-infected floppy disk in drive A. You might want to use Scan to make sure that both the computer and the floppy disk are virus-free. (See "Manually Scanning for Viruses" for details.)
2. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Create Rescue Disk** (see Figure 9).

Figure 9

3. Click **Create** to create the Rescue Disk.
   If this is your first time creating a Rescue Disk, a message tells you that Rescue Disk needs to download the image file for the Rescue Disk. Click **OK** to download the component now, or click **Cancel** to download it later.

   A warning message tells you that the contents of the floppy disk will be lost.
4. Click **Yes** to continue creating the Rescue Disk.
   The creation status appears in the Create Rescue Disk dialog box.
5. When the message "Rescue disk created" appears, click **OK**, and then close the Create Rescue Disk dialog box.
6. Remove the Rescue Disk from the drive, write-protect it, and store it in a safe location.

Write-Protecting a Rescue Disk

To write-protect a Rescue Disk:

1. Turn the floppy disk label-side down (the metal circle should be visible).
2. Locate the write-protect tab. Slide the tab so the hole is visible.

Using a Rescue Disk

To use a Rescue Disk:

1. Turn off the infected computer.
2. Insert the Rescue Disk into the drive.
3. Turn the computer on.
   A gray window with several options appears.
4. Choose the option that best suits your needs by pressing the Function keys (F2, F3, etc).
   Note: Rescue Disk starts automatically in 60 seconds if you do not press any of the keys.

Updating a Rescue Disk

It is a good idea to update your Rescue Disk regularly. To update your Rescue Disk, follow the same instructions for creating a new Rescue Disk.

Automatically Reporting Viruses

You can anonymously send virus tracking information for inclusion in our World Virus Map. Automatically register for this free, secure feature either during VirusScan Online installation (in the Virus Map Reporting dialog box), or at any time in the **Virus Map Reporting** tab of the VirusScan Online Options dialog box.

Reporting to the World Virus Map

To automatically report virus information to the World Virus Map:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**. The VirusScan Online Options dialog box opens.
2. Click the **Virus Map Reporting** tab (see Figure 10).

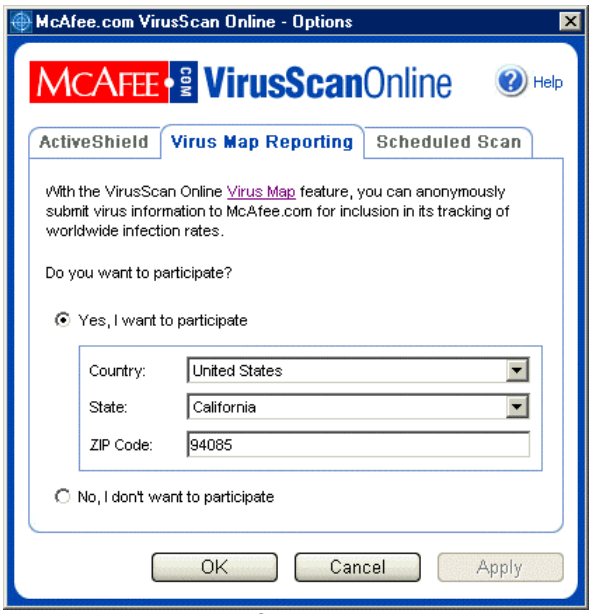

Figure 10

3. Accept the default **Yes, I want to participate** to anonymously send your virus information to McAfee.com for inclusion in its World Virus Map of worldwide infection rates. Otherwise, select **No, I don't want to participate** to avoid sending your information.
4. If you are in the United States, select the state and enter the zip code where your computer is located. Otherwise, select the country where your computer is located.
5. Click **OK**.

Viewing the World Virus Map

Whether or not you participate in the World Virus Map, you can view the latest worldwide infection rates via the McAfee.com McAfee.com icon in your Windows system tray.

To view the World Virus Map:

Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **World Virus Map**.

The McAfee.com World Virus Map Web page appears (see Figure 11).

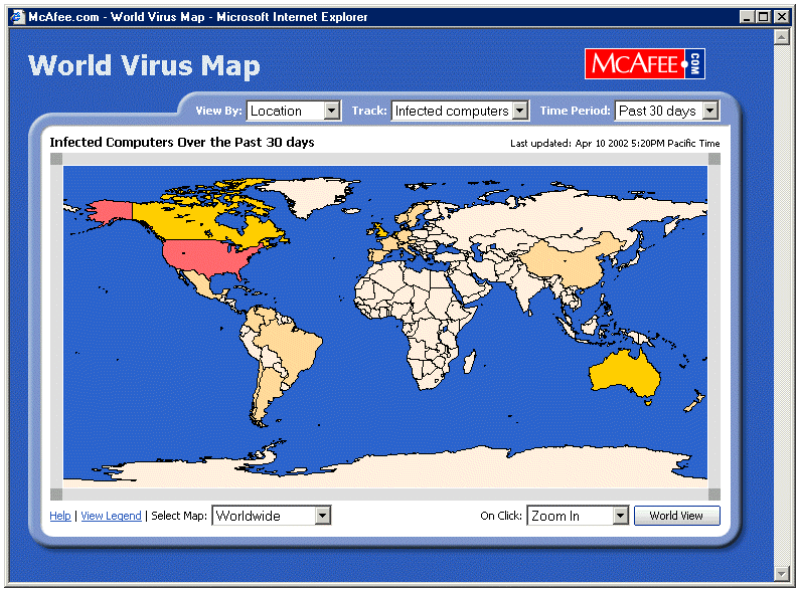

Figure 11

By default, the World Virus Map shows the number of infected computers worldwide over the past 30 days, and also when the reporting data was last updated. You can change the map view to show the number of infected files, or change the time period to show only the results over the past 7 days or the past 24 hours.

The Virus Tracking section lists cumulative totals for the number of scanned files, infected files, and infected computers that have been reported since the date shown.

Updating VirusScan Online

Updating VirusScan Online provides you with the latest information and protection. VirusScan Online automatically checks for updates every four hours when you are connected to the Internet. If a product update or virus outbreak occurs, an alert appears. Once alerted, you can then choose to update VirusScan Online to remove the threat of a virus outbreak.

Automatically Checking for Updates

You must be connected to the Internet for VirusScan Online to check for available updates. If an update is available, an alert appears (similar to Figure 12).

Figure 12

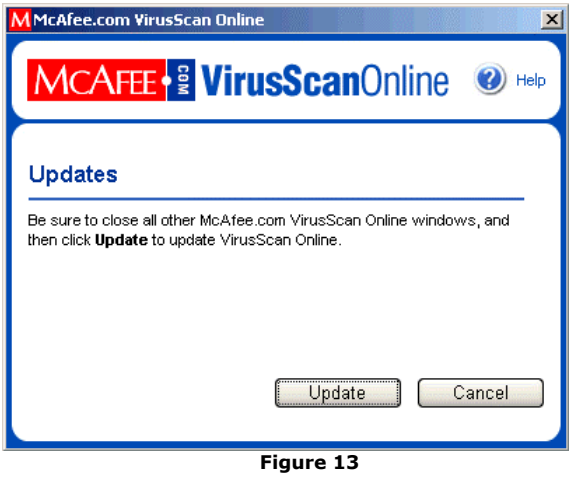

Figure 13

To update VirusScan Online:

1. Click **Update now** on the Update Available alert (see Figure 12).
   The Updates dialog box opens (see Figure 13).
2. Click **Update**.
3. Log on to the McAfee.com Web site if VirusScan Online prompts you to do so. The update downloads automatically.
4. Click **Finish** on the Completing the VirusScan Online Wizard dialog box when the update is finished installing.

   Note: In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

If you are too busy to update VirusScan Online when the alert appears, you can postpone updating:

- Click **Be reminded later** on the Update Available alert (see Figure 12), select a time delay for your next update reminder, and then click **OK**. You can select from 10 minutes, 20 minutes, 30 minutes, 1 hour, 2 hours, or 4 hours (the default).

  - or -

- Click **Continue what I was doing** to close the alert without taking any action.

Manually Checking for Updates

In addition to automatically checking for updates every four hours when you are connected to the Internet, you can also manually check for updates at any time.

To manually check for VirusScan Online updates:

1. Make sure your computer is connected to the Internet.
2. Right-click the McAfee.com icon, and then click **Updates**.
   The SecurityCenter Updates dialog box opens.
3. Click **Check Now**.
   If an update exists, the VirusScan Online Updates dialog box opens (see Figure 13). Click **Update** to continue.

   If no updates are available, a dialog box tells you that VirusScan Online is up-to-date. Click **OK** to close the dialog box.
4. Log on to the Web site if prompted. The Update Wizard installs the update automatically.
5. Click **Finish** when the update is finished installing.
   Note: In some cases, you will be prompted to restart your computer to complete the update. Be sure to save all of your work and close all applications before restarting.

Chapter 3 – Troubleshooting

Missing or Corrupt Components

Unfortunately, a few situations might cause VirusScan Online to install incorrectly:

- Your computer does not have enough disk space. See "System Requirements" to verify that your computer has the necessary resources to run our software.
- Your computer's memory resources are low. See "System Requirements" to verify that your computer has the necessary resources to run our software.
- Your Internet browser is incorrectly configured. See "Configuring Microsoft® Internet Explorer" to verify your settings.
- You have a faulty Internet connection. Check your connection; otherwise, simply try to connect again later.

The best solution is to resolve any of the above issues, and then download and reinstall VirusScan Online.

Slow Performance

If ActiveShield is set to use the **All files** option, your computer might slow down considerably. The best solution is to set ActiveShield to the default **Program files and documents only (recommended)** option.

To set ActiveShield to scan program files and documents only:

1. Right-click the McAfee.com icon, point to **VirusScan Online**, and then click **Options**. The VirusScan Online Options dialog box opens.
2. Click **Program files and documents only (recommended)**, and then click **OK** to save your settings and close the dialog box.

Your computer should run normally now. Otherwise, see "System Requirements" to verify that your computer has the necessary resources to run our software. The VirusScan Online features might not work correctly if these requirements are not met.

ActiveShield Fails to Detect the EICAR Test File

1. Verify that ActiveShield is enabled.
2. Verify that you are using the correct test file. ActiveShield only detects the eicar.com file as you try to open or download it from the Web site. The eicar.txt file isn't meant to be detected as a virus, and the other two files are used for testing Scan (see "Testing VirusScan Online").
3. Uninstall VirusScan Online (see "Uninstalling VirusScan Online").
4. Verify that your computer meets the system requirements to run our software. The VirusScan Online features might not work correctly if these requirements are not met.
5. Verify that Internet Explorer is configured correctly (see "Configuring Microsoft® Internet Explorer").
6. Reinstall VirusScan Online (see "Downloading and Installing VirusScan Online").
7. Test ActiveShield again. If it still doesn't detect the EICAR test file, contact McAfee.com Technical Support at http://www.mcafee.com/support/.

Scan Fails to Detect One or More of the EICAR Test Files

1. Verify that you selected all of the options in the Scan Options box (see "Scanning Your Computer for Viruses").
2. Verify that you scanned the correct folder or drive.
3. Uninstall VirusScan Online (see "Uninstalling VirusScan Online").
4. Verify that your computer meets the system requirements to run our software. The VirusScan Online features might not work correctly if these requirements are not met.
5. Verify that Internet Explorer is configured correctly (see "Configuring Microsoft® Internet Explorer").
6. Reinstall VirusScan Online (see "Downloading and Installing VirusScan Online").

7. Test Scan again. If it still doesn't detect the EICAR test files, contact McAfee.com Technical Support at http://www.mcafee.com/support/.

Virus Cannot Be Cleaned or Deleted

For some viruses, your computer's operating system might impose restrictions requiring you to manually clean your system if it's infected.

If your computer cannot clean or delete a virus, please consult the Virus Information Library at http://vil.mcafee.com/ for instructions on manually deleting the virus.

If the virus prevents you from using your Internet connection or from using your computer at all, try using a Rescue Disk to start your computer. In many cases, the Rescue Disk can start a computer if a virus disables it. See "Creating a Rescue Disk" for details.

If all of the above fails, please call McAfee.com Customer Support at (408) 992-8599 for your fee-based telephone options.

Uninstalling VirusScan Online

In some situations, you might need to uninstall VirusScan Online as part of a troubleshooting strategy.

Note: Users must have Administrator rights to uninstall VirusScan Online.

To uninstall VirusScan Online:

1. Save all your work and close any open applications.
2. Open Control Panel:
   - Windows 95, 98, Me, and 2000 users: On your Windows taskbar, click **Start**, point to **Settings**, and then click **Control Panel**.
   - Windows XP users: On your Windows taskbar, click **Start**, and then click **Control Panel**.
3. Open the Add/Remove Programs dialog box:
   - Windows 95, 98, Me, and 2000 users: Double-click **Add/Remove Programs**.
   - Windows XP users: Click **Add or Remove Programs**.
4. Select **McAfee.com VirusScan Online** from the list of programs, and then click **Change/Remove**.
5. When you are asked to confirm the uninstallation, click **Yes**. The uninstallation begins.
6. When you are prompted to reboot your system, click **Close**.
7. From the Add/Remove Programs dialog box, select **McAfee.com SecurityCenter**, and then click **Change/Remove**.
8. Click **Reboot** when you are prompted to reboot your system.
   Your computer will restart so that the uninstallation works properly. When your computer restarts, VirusScan Online will have been uninstalled.

For reinstallation instructions, please see "Downloading and Installing VirusScan Online."

Configuring Microsoft® Internet Explorer

McAfee.com uses ActiveX controls and cookies in its applications. These technologies require specific Internet browser configurations to ensure the applications are installed correctly and work properly on your computer.

Most Internet browsers will already have the proper settings to install VirusScan Online. To avoid any problems with the installation, we suggest that you verify that your Internet browser settings are correct before you try to install VirusScan Online.

First, determine which version of Internet Explorer you are using:

1. Open Internet Explorer.
2. On the Internet Explorer menu bar, click **Help**, and then click **About Internet Explorer** to open the About Internet Explorer dialog box.
3. Look for the line labeled **Version:** and note the first three numbers.

   Example: *Version: **5.50**.4807.2300*. The bold numbers indicate where you should look. This version of Internet Explorer is 5.50, so you would follow the steps in "Configuring Internet Explorer 5.x."

Configuring Internet Explorer 5.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options** to open the Internet Options dialog box.
2. Click the **Security** tab (see Figure 14). Make sure that you are in the **Internet** Web content zone and that the security level for this zone is set to **Medium** (the default setting) or **Low**.
3. If you are not sure whether your security options are correct, click **Default Level** to set the zone to **Medium** (recommended).
4. If you are an advanced user who wants to customize your security settings, click **Custom Level** to open the Security Settings dialog box. McAfee.com requires that the following options must be enabled.
    a. Select **Enable** for these ActiveX controls and plug-ins options:
        - **Download signed ActiveX controls**
        - **Run ActiveX controls and plug-ins**
        - **Script ActiveX controls marked safe for scripting**
    b. Select **Enable** for the **Active scripting** option under the Scripting settings.
5. When you are done, click **OK**, and then click **Yes** to confirm the changes.
6. Click **OK** to close the Security Settings dialog box.
7. Click **OK** to close the Internet Options dialog box.
8. Exit Internet Explorer.

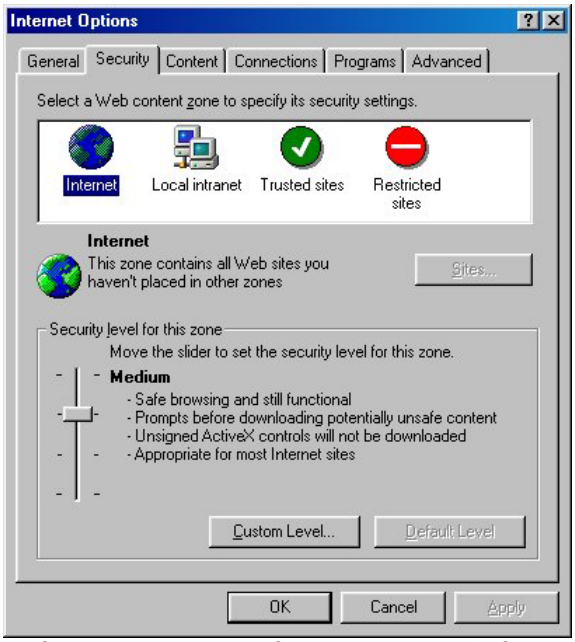

Figure 14. Internet Explorer 5.x Internet Options

Configuring Internet Explorer 6.x

1. Open Internet Explorer. On the **Tools** menu, click **Internet Options** to open the Internet Options dialog box.
2. Click the **Security** tab (see Figure 15). Make sure that you are in the **Internet** Web content zone and that the security level for this zone is set to **Medium** (the default setting) or **Low**.
3. If you are not sure whether your security options are correct, click **Default Level** to set the zone to **Medium** (recommended).
4. If you are an advanced user who wants to customize your security settings, click **Custom Level** to open the Security Settings dialog box. McAfee.com requires that the following options must be enabled.
    a. Select **Enable** for these ActiveX controls and plug-ins options:
        - **Download signed ActiveX controls**
        - **Run ActiveX controls and plug-ins**
        - **Script ActiveX controls marked safe for scripting**
    b. Select **Prompt** for these ActiveX controls and plug-ins options:
        - **Download unsigned ActiveX controls**
        - **Initialize and script ActiveX controls not marked as safe**
    c. Select **Enable** for the **Active scripting** option under the Scripting settings.

5. When you are done, click **OK**, and then click **Yes** to confirm the changes.
6. Click the **Privacy** tab on the Internet Options dialog box (see Figure 16), and then click **Advanced** to open the Advanced Privacy Settings dialog box.
7. Make sure that **Override automatic cookie handling** and **Always allow session cookies** are selected, and then click **OK** to close the Security Settings dialog box.
8. Click **OK** to close the Internet Options dialog box.
9. Exit Internet Explorer.

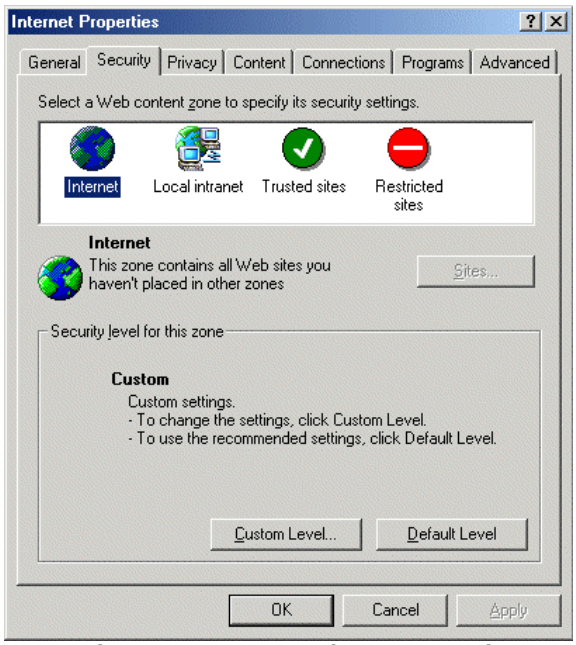

Figure 15. Internet Explorer 6.x Security

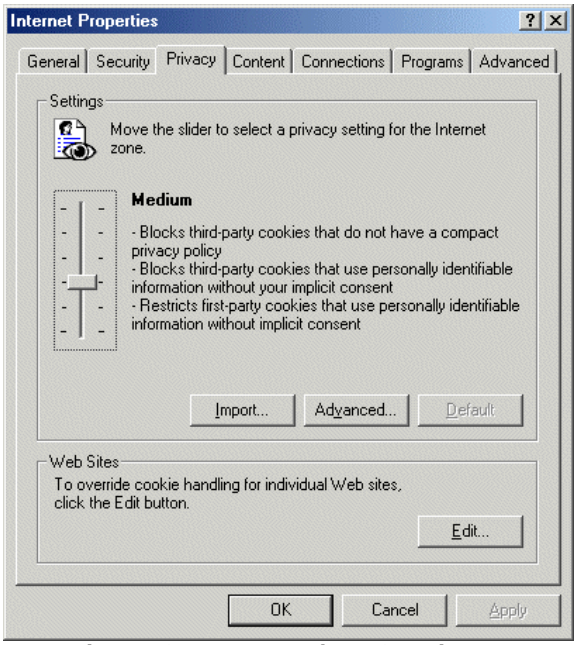

Figure 16. Internet Explorer 6.x Privacy

About ActiveX Controls

ActiveX controls are software modules based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package. Modules can be interchanged but still appear as parts of the original software.

On the Internet, ActiveX controls can be linked to Web pages and downloaded by an ActiveX-compliant browser, such as Internet Explorer 5.0 or later. ActiveX controls turn Web pages into software pages that perform as any other program launched from a server.

McAfee.com uses ActiveX controls in its applications, and you must download the specific ActiveX components required for each application. Once these components are loaded, you do not need to download them again unless upgrades or updates become available.

Appendix A - General Virus Information

Defining Viruses

Viruses are small programs written with the intent of damaging or taking control of computers. They are known for their ability to attach to a "host" program so that when the host program is run, the virus is also run. They are also known for their ability to replicate themselves.

A virus starts its life hidden within another program or file and launches when that file launches. At this point, the virus is active and your computer is infected. Once active, viruses work differently depending on their type.

A *direct-action virus* works immediately to run its program, cause any damage—often called "delivering its payload"—and to replicate itself. A *resident virus*, however, sits in the background as a memory-resident program, using the terminate-and-stay resident procedure (TSR) allowed by the operating system.

Resident viruses can be programmed to do almost everything the operating system can do because TSR programs have a wide range of activities they perform such as launching programs, watching for input from pointing devices and keyboards, scanning disks, and backing up files.

About Viruses

More than 50,000 computer viruses exist, and experts estimate that virus authors create more than 1,000 new viruses every month. Some viruses are very harmful, while many are not. Many create minor annoyances or are even invisible to users. Others damage files, consume CPU resources, or reformat drives. Because viruses are capable of damaging computers, consider all viruses threatening.

How Viruses Spread

Viruses can travel through infected floppy disks, or they can be downloaded from a network or the Internet as a part of a larger download (as macros for specific applications, as email attachments, or as downloaded shareware files). Because file infectors only require association with executable files, they can be increasingly found on storage media such as Zip and Jaz drives and recordable CD-ROMs.

Viruses and Email
Viruses usually enter as part of an infected program file (boot sector, .com, .exe). This means an email message itself cannot be a virus. Because viruses themselves are programs, the computer must activate the virus in order for the virus to run. A virus delivered as an email attachment, therefore, does nothing until you open the attachment. Seeing an attachment icon included in an email message does not mean you have opened it. To open most attachments, you must double-click the icon. Therefore, a simple way to protect your computer is by not opening executable files (.exe or .com) or data files for programs with macro-writing features.

Types of Viruses

Boot Sector Viruses
Boot sector viruses reside in the boot sector area of a floppy disk or hard disk—the area read and executed when computers are started (booted). True boot sector viruses infect only the DOS boot sector, but an *MBR virus* infects the master boot record. A computer reads both of these hard disk areas during the boot process. It is during the boot time that the boot sector virus gets loaded into memory. A computer infected with a boot sector virus might require a virus-free rescue disk before an anti-virus program can clean the computer.

File Infectors
More common than boot sector viruses are *file infectors*, or *parasitic viruses*. These viruses attach themselves to executable files (.exe and .com files). File infectors usually wait in memory for the user to run another program and use the event as a trigger to infect and replicate. This means file infectors replicate simply through active use of the computer.

Macro Viruses

A newer form of virus is the *macro virus*—sometimes called a *Word macro virus*, after its infection of Microsoft Word files. A macro virus uses the built-in programming languages of several different software applications. Companies include these languages to help users create automated tasks, called macros, for simplifying repetitive tasks within the application.

A macro virus is simply a malicious macro. When a document or template containing the macro virus is opened in the target application, the virus runs, does its damage, and copies itself into other documents. Continual use of the program results in the spread of the virus. A well-known type of macro virus is the Melissa macro virus. Aliases and variants include Melissa, Melissa.a, and W97M/Melissa.a@mm.

Macro viruses are becoming more common and dangerous. In addition to Word, most of Microsoft's applications support the Visual Basic for Applications (VBA) programming language. This allows viruses to infect a file from one application and possibly use a different application to spread. Melissa, for instance, infected Word files and used Outlook to spread copies to individuals in the Outlook address book. While Microsoft has installed safety features in its programs, some crafty viruses can now circumvent these defenses.

People not using Microsoft products can also experience macro viruses as other software manufacturers begin using and incorporating built-in programming languages into their products.

Malicious Software Types

The term *virus* is used broadly to describe a host of malicious software, or *malware*. Authors intentionally design malware to run without the user's knowledge and to commit destructive actions inside the user’s computer. Malware includes not only viruses, but also Trojan horses, worms, and droppers.

Trojans

Unlike viruses, Trojan horse programs do not replicate. Like the Trojan horse from Greek mythology, a Trojan horse program—or Trojan—hides inside a seemingly harmless or desirable program. When the harmless program runs, the Trojan launches and performs unwanted actions. Back Orifice is a Trojan horse program.

Worms

Worms replicate but do not infect other programs like viruses. A *host worm* uses a network to copy itself onto other machines. A *network worm* spreads pieces of itself across a network and relies on the network connections to run its various components. Worms can work on non-networked computers by copying themselves to various locations on the hard disks. Worms can spread by email or through Internet Relay Chat (IRC). PrettyPark is a common worm and is sometimes designated W32/Pretty.worm. Newer worms include the Code Red and SirCam worms.

Droppers

Virus authors often use droppers to transport and install viruses. Droppers wait for a trigger event, and then launch themselves to infect the computer with the contained virus. Droppers sometimes use encryption to avoid detection by anti-virus software.

Bombs

Bombs are not technically malware, but are often used as a means to trigger a malicious program. They rely on specific trigger events to activate. Some bombs rely on the system clock, and they can be programmed for various tasks such as deleting information or displaying a message on a specific date. Other bombs are activated by other events or conditions—for example, the sixth launch of a program or a specific keystroke pattern.

Virus authors often combine several malware ideas into their programs. A virus author might use a dropper to install a virus. When a virus attaches to an existing program, a virus effectively turns the program into a Trojan horse. A bomb might be used to trigger the actions of a virus once a certain event or condition is satisfied, and a worm might be used to replicate the virus.

Tips for Preventing Infection

Invest in Anti-virus Software
Anti-virus software constantly searches your files and compares information on these files with virus signature files (.dat files) for signs of viruses and other malware. Most companies provide regular updates to their virus signature files. As researchers find viruses, they add the virus signatures to the .dat files so users have constant, up-to-date protection. Of course, the best defense against infection is having anti-virus software, like VirusScan Online, running before you are infected.

If you think you have a virus, use an anti-virus application to scan your computer. If you are a VirusScan Online user and you have a virus that the AVERT (Anti-Virus Emergency Response Team) already knows about, VirusScan Online will detect and remove it. If you think you have an unknown virus, visit McAfee.com at http://www.mcafee.com/anti-virus/ for information about submitting virus samples.

Check Floppy Disks and CD-ROMs
When you insert a floppy disk in the drive, use anti-virus software, such as the Scan utility in VirusScan Online, to scan the disk before you use it. This also applies to files downloaded from a network, the Internet, and from other media such as Zip and Jaz drives and recordable CD-ROMs (CD-R and CR-RW).

Use Email Precautions
Be smart when receiving email messages. Email from unknown senders might include attached viruses. If you don't know the source, be careful about opening attachments. Unexpected emails from familiar sources might also contain viruses. Newer viruses can open a user's electronic address book and send copies of itself to a portion of or all the contacts. If you receive an unexpected or questionable message, check with the sender before opening it. The best advice is to delete the message, but if you must open the attachment, make sure you scan the attachment with your anti-virus software before you open it.

Research Viruses and Hoaxes
Educate yourself on viruses and virus hoaxes. If you receive an email message about a virus, check with a reputable source to see if the warning is real. Even if an email message quotes a seemingly credible source, visit McAfee.com's Virus Hoax page, http://vil.mcafee.com/hoax.asp, to learn about the hoaxes and the damage they cause. Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so be careful.

For information about viruses and other malware, consult the McAfee.com Virus Information Library at http://vil.mcafee.com/.

Appendix B - McAfee.com Privacy Policy

McAfee.com is committed to protecting your privacy as a consumer. As a data security company, we understand better than most the need for you to maintain control over your personal data when using the Internet. We maintain your privacy through the enforcement of strict internal polices that exceed industry standards. You can also find the Privacy Policy at http://www.mcafee.com/copyright/privacy.asp.

McAfee.com is a licensee of the TRUSTe Privacy Program. TRUSTe is an independent, non-profit organization whose mission is to build users' trust and confidence in the Internet by promoting the use of fair information practices. Because this Web site wants to demonstrate its commitment to your privacy, it has agreed to disclose its information practices and have its privacy practices reviewed for compliance by TRUSTe. By displaying the TRUSTe trustmark, this Web site agrees to notify you of:

- What personally identifiable information of yours or a third-party is collected from you through the Web site
- The organization collecting the information
- How the information is used
- With whom the information can be shared
- What choices are available to you regarding collection, use, and distribution of the information
- The kind of security procedures that are in place to prevent the loss, misuse, or alteration of information under McAfee.com's control
- How you can correct any inaccuracies in the information

If you have any questions or concerns regarding this statement, please send them to privacy@mcafee.com. For questions or concerns regarding non-privacy statement issues, please visit our Support Center. If you do not receive acknowledgment of your inquiry or your inquiry has not been satisfactorily addressed, you should then contact TRUSTe at http://www.truste.org/users/users_watchdog.html. TRUSTe will then serve as a liaison with the Web site to resolve your concerns. McAfee.com is committed to protecting your privacy!

McAfee.com is vigilant about protecting your privacy as a consumer. As a data security company, we understand better than most the need for you to maintain control over your personal data when using the Internet. We maintain your privacy through the enforcement of strict internal polices that exceed industry standards.

We Protect Your Right to Privacy
McAfee.com respects your privacy. Our guidelines for protecting the information you provide us during a visit to our Web site appear below. Furthermore, McAfee.com is a registered licensee of TRUSTe. TRUSTe is an independent, non-profit initiative whose mission is to build users' trust and confidence in the Internet by promoting the principles of full disclosure and informed consent. Because we want to demonstrate our commitment to your privacy, we have agreed to disclose our information practices and to have our privacy practices reviewed and audited for compliance by TRUSTe. These include:

- What information we gather/track
- How we use the information
- With whom we share the information
- Our opt-out policy
- Our policy on correcting and updating personally identifiable information
- Our policy on deleting or deactivating your name from our database
- Our policy regarding children who visit our site

Privacy Statement
This statement discloses the privacy practices for www.mcafee.com. We have designed McAfee.com so that no personal identifying information is displayed online or is accessible to the general public.

What Information We Gather/Track
We collect and store some or all of the following information about our users: name; email address; and billing information, such as address, phone number, and credit card number. If you do not want to have your credit card number stored for billing purposes, please contact Customer Service. We also receive and may store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses McAfee.com.

In order to tailor our subsequent communications to you and continuously improve our products and services (including registration), we may also ask you to provide us with information regarding your personal or professional interests, demographics, experience with our products, and more detailed contact preferences. You will have the option of choosing not to provide us with this information.

Use of Data
McAfee.com uses your information to better understand your needs and provide you with better service. Specifically, we use your information to help you complete a transaction, including fulfillment of promotional offers, to communicate back to you, to update you on service and benefits, to personalize our web sites for you, and to manage and renew your subscription(s). Credit card numbers are used only for payment processing and fraud protection, and are not used for other purposes without your permission.

Web Applications
Certain online applications, such as the various elements of the McAfee.com Clinic, store some components on your hard drive. The software employs proprietary technology to scan your computer system and retrieve information regarding your installed software and hardware. The information that is retrieved is used to provide the services you have chosen to subscribe to or use. In addition, unless you indicate you do not want this service, the information will be used to generate advertising that is appropriate for you. The information gathered by these applications is used only to generate output directed to you and is not aggregated or used for any other purpose. It is not stored along with any identifying information about you, nor is it sold, rented, or shared with any outside parties in any form whatever. TRUSTe is currently developing a program to address the collection of data through downloadable consumer software. However, as this program is not yet ready for implementation, TRUSTe does not yet cover data collected in this manner. As soon this program is put in place, McAfee.com looks forward to working with TRUSTe to address this data practice.

Use of Your Email Address
If you provide us with your email address when you register as a customer or make a purchase from us, we will occasionally send you email with recommendations or notices of new products, prices, and services. This email may include paid advertisements from third parties. You may block future email of this type, simply by following the instructions at the bottom of the update messages.

Separately, we send service notifications via email to keep you informed about the status of your service orders or accounts and to provide updates and technical notices. These messages are essential to the maintenance of your subscription and the functionality of our services. Therefore no opt-out is available for service notifications, and these messages cannot be blocked.

Who We Share It With
McAfee.com will not sell, rent, or lease your personally identifiable information to others. Unless we have your permission or are required by law, we will only share the personal data you provide online with other McAfee.com entities and/or business partners who are acting on our behalf for the uses described in "Use of Data". By contract, third parties such as CyberSource and Digital River must comply with their own privacy policies with regard to the renting, selling, or sharing of information. As partners of McAfee.com, they must also offer McAfee.com customers the chance to opt out of information sharing. For advertising purposes, visitor and customer information is statistically aggregated and reported to advertisers. However, we do not disclose to these entities any information that could be used to personally identify you, such as your name, email address, account, password, or transaction history.

Special Relationships
McAfee.com has a number of relationships with business partners. These business partners provide a number of different services.

CyberSource and Telecheck are intermediaries in the purchasing process for McAfee.com. CyberSource provides credit card transaction services for McAfee.com. Telecheck provides electronic check processing services for McAfee.com. Both CyberSource and Telecheck verify your purchase information, such as credit card number or checking account number, and authorize your transaction. In doing so, CyberSource and Telecheck have access to sensitive data about users. They do not use this information for any other purpose. Read CyberSource's privacy policy.
Read Telecheck's privacy policy.

Digital River powers the McAfee Store, and in doing so collects information about users, including credit card information. When a user purchases a product from the McAfee Store, information about the customer and the purchase are shared with McAfee.com. Digital River may occasionally notify you of special offers, new products, services, promotions, and other similar information. McAfee.com users can opt out of receiving such mail from Digital River by calling 1-800-656-5426 and asking to be removed from future emails.
Read Digital River's privacy policy.

Affiliates
When a user or a company signs up to be a McAfee.com affiliate, they do so through LinkShare. LinkShare does share personally identifiable information about affiliates with McAfee.com. This information is not sold, shared, or rented to any third-party, and is used internally only to manage and maintain relationships with affiliates.

Links
McAfee.com contains links to other Web sites. Please note that when you click one of these links, you are 'clicking' to another Web site. We encourage you to read the privacy statements of these linked sites, as their privacy policies may differ from ours.

Cookies
McAfee.com uses software tags called "cookies" to identify customers when they visit our site. Cookies are used to remember user preferences and maximize performance of our services. Additionally, cookies help us to identify returning users so that we don't ask them to enter their email and McAfee.com password with every visit. The information we collect with cookies is not sold, rented, or shared with any outside parties. We also ask that you fill in your first name and last name in a box so that our customer support services can identify and assist you in case of login problems. We cannot provide subscription services to users whose browsers are set to reject all cookies.

We may use third-party advertising companies to serve ads on our site. These companies may employ cookies and action tags (also known as single pixel gifs or web beacons) to measure advertising effectiveness. Any information that these third parties collect via cookies and action tags is non-personal and anonymous. DoubleClick.net sets cookies in McAfee.com visitors' browsers. McAfee.com does not require that users accept cookies from DoubleClick.net in order to access our services. McAfee.com does not have access to the information contained in advertisers' cookies. If you would like more information about this practice and your choices, click here http://www.networkadvertising.org/optout_nonppii.asp.

McAfee.com uses the services of Engage for the serving and/or targeting of ads, promotions and other marketing messages. To do this, Engage collects anonymous data through the use of cookies. To learn more about Engage, including your ability to opt out of the Engage system, go to http://www.engage.com/privacy.

McAfee.com also uses the services of DoubleClick for the serving and/or targeting of ads, promotions, and other marketing messages. To do this, DoubleClick collects non-personal data through the use of cookies about the types of sites you visit and other non-personally identifiable information about you in order to deliver advertisements about goods and services that may be of interest to you. In the course of serving advertisements or providing other marketing services, DoubleClick may place or

recognize a unique, non-personally identifiable cookie in your browser. In providing these services, DoubleClick does not link personally identifiable information (such as your name, land address or telephone number) to your Web site visits. If you would like more information about DoubleClick, its business practices, and its privacy policies, please click here. To opt out of this anonymous online preference marketing service, please click here.

Log Files
McAfee.com maintains log files of the traffic that visits the McAfee.com site. We do not link any information gathered in these log files to personally identifying information. Log files are used to manage traffic loads and information technology requirements for providing reliable service. Information collected includes IP addresses and browser types.

Feedback
We collect user feedback. We do not typically respond to user feedback in the form of email. We do cull testimonials that appear on the site from our feedback form, but only after we have obtained permission from the senders. Users who want a response to specific questions concerning the service or their subscriptions are directed to the customer service area. These questions will be respond to as quickly as possible. We read all of our customer service queries and use the information contained therein only to resolve the question at hand. We also post surveys on our site, ranging from one to ten questions. These surveys are optional and all information is collected anonymously. The information is collected to better understand our user population. It is not sold or transferred to any third-party.

Correct/Update/Delete User Information
Users can update, correct, or delete their personal information on McAfee.com by clicking on the "My Account Info" link. Users may cancel their accounts by accessing the "How to Update your Automatic Renewal and Subscription Status" page at http://clinic.mcafee.com/clinic/membership/cancel.asp.

Our Privacy Policy Regarding Children who Visit our Site

What Information Is Collected?
It's our policy to create website content that requires minimum collection of information from children visiting our site. From time to time, however, we may request limited personally identifiable information (e.g. a child's email address and/or email address of parent or guardian), as explained below, in order to conduct online contests or sweepstakes or offer other online activities. McAfee.com does not condition a child's participation in any of our online activities on the disclosure of more information than is reasonably necessary to participate in the activity.

McAfee.com will not sell, rent, or lease this information to others. Unless required by law, we will only share the personal data provided online with other McAfee.com entities and/or business partners who are acting on our behalf for the uses described in "Use of Data" or for purposes of conducting a contest or sweepstakes.

- **Contests and Sweepstakes**
  McAfee.com occasionally offers contests and sweepstakes, which may be entered online. To participate in a contest or sweepstakes, a **child is asked to provide his or her first name, last name, email address and age. If the child is 13 years old or younger, the last name and the email address are deleted immediately**. He or she is also required to enter the name of a parent and the email address of a parent. We then send the child's parent an email within two business days informing him or her of the child's entry. **The parent must respond and approve the child's entry into the contest or the child's information will be deleted from our records**. All the information collected by McAfee.com is securely maintained and used only for the purpose of conducting the contest or sweepstakes and notifying the winner(s). The parent will be notified if their child wins the contest if the child is under 13, otherwise the child will be contacted. Once the contest or sweepstakes is finished, we then delete any personal information collected.

Information for Parents

- **How to Update Your Child's Information**
  Please use the link provided in the email that we send you following your child's enrollment in our contest OR send an email to kidsinfo@mcafee.com. The email should contain your child's name and email address, as well as which information you would like updated.
- **How to Prevent Use of Your Child's Information (Request Deletion of Record)**
  Please send an email to kidsinfo@mcafee.com with your child's name and email address, along with the request that your child's name should be deleted from our records.
- **How to Contact Us**
  Privacy Coordinator
  McAfee.com Corp
  535 Oakmead Parkway
  Sunnyvale, CA 94085
  USA
  Tel: (408) 992-8100
  Email: privacy@mcafee.com

Information Security
All information gathered on the McAfee.com site is stored and maintained in secure facilities that limit access to authorized personnel only. This personnel can only access the information through a series of access-control procedures. All McAfee.com employees are briefed about the company's privacy and security policies on a regular basis. The McAfee.com Web site is regularly tested for security breaches to ensure that all information collected is secure from unauthorized viewing.

Notification of Changes
If we change our privacy policy, we will post a notice on our site so our users are aware of the change in what information we collect, how we use it, and/or under what circumstances, if any, we disclose it. If at any point we decide to use personally identifiable information in a manner different from that stated at the time it was collected, we will notify users by email. Users will have a choice as to whether or not we use their previously submitted information in this different manner. Users may choose to have their information used in accordance with the privacy policy under which the information was collected.

Appendix C - General Privacy and Security Guidelines

The following guidelines provide good information about security and privacy issues on the Internet. They are provided as general information. For specific information regarding McAfee.com and its Web site, please see the "McAfee.com Privacy Policy" appendix of this user guide, or the McAfee.com privacy policy at http://www.mcafee.com/copyright/privacy.asp.

Privacy Statements
Thoroughly read the posted privacy statements of Web sites. A privacy statement is a legally binding document that describes what personal information Web sites gather, how it is collected, and with whom it will be shared. Make sure you understand how businesses will use your information before you do business with a Web site.

Third-Party Approval Seals
These seals indicate an outside agency, such as TRUSTe, monitors the privacy policies of a Web site. In other words, a neutral agency ensures the Web site's owners adhere to their online privacy statement. They also act as a third party that you can contact if you feel that your privacy has been violated.

Third-party seals usually link to the Web site's privacy statement and to the outside agency's Web site. If you cannot find a Web site's privacy policies, contact the site directly and ask for a copy of its privacy collection and dissemination practices.

Passwords

- Don't create passwords similar to your real name, commonly used nickname, or online screen name.
- Always protect your online passwords. Never offer it to anyone who asks for it, even to someone who says that he or she is calling on behalf of your Internet service provider.
- Change your passwords often.
- Don't store your passwords near your computer or in your desk.

Aggregate Information
Aggregate information might be collected by a Web site but is not "personally identifiable" to you. Aggregate information includes demographic data, domain names, Internet provider addresses, and Web site traffic. As long as companies do not link this information to a user's personal information, the data is considered aggregate.

Security and Credit Cards
Only place credit card orders through secure servers. Most online merchants alert you when you are entering their secure servers. In addition, see if the URL (Web address) begins with "https" rather than "http"; this indicates that you have entered the secure area. Some browsers represent secure areas by either a closed lock or a solid key symbol in the status bar at the bottom of the browser.

The same consumer protection laws that apply in stores apply on the Internet. Using credit cards allows you to contest any charges if the merchandise does not live up to the promotion. In addition, federal law limits your liability to $50 for purchases made with stolen credit card information.

Common Sense
Don't disclose information you wouldn't disclose over the phone or in person.

You can always contact the Web site for more information about its privacy and security practices before you make a purchase.

Index