

COX Security Suite

Powered By **McAfee™** 2008

VirusScan Plus, Privacy Service, SiteAdvisor

User Guide

Table of Contents

Getting Started with VirusScan Plus	4
SecurityCenter	5
Features	5
Using SecurityCenter	7
Header	7
Left column	7
Main pane	8
Understanding SecurityCenter icons	8
Understanding the protection status	9
Fixing protection problems	16
Getting Started with Privacy Service	17
Features	17
The Administrator	18
Launching Privacy Service	21
Removing and re-installing Privacy Service	22
Getting Started with SiteAdvisor.....	25
Benefits.....	26
Features	27
How SiteAdvisor works.....	28
SiteAdvisor Configuration and Support	32

Cox Security Suite includes VirusScan Plus, Privacy Service, and SiteAdvisor. It offers proactive PC security to prevent malicious attacks, so you can protect what you value as well as go online with confidence. It continuously delivers the latest software so your protection is never out-of-date. Moreover, improved performance allows it to protect, without disturbing you.

Cox Security Suite includes Privacy Service which helps prevent sensitive information from being hijacked by cybercriminals and provides controls for managing your family's Internet experience. Easy to use, Privacy Service gives you ability to control what content and images are displayed so your children cannot view objectionable material.

Also, it includes SiteAdvisor technology which helps protect you from dangerous sites that engage in "social engineering" attacks such as adware, spam, and phishing scams. SiteAdvisor adds intuitive red, yellow and green icons to sites and search results to help keep you safe as you search, browse, and transact online.

CHAPTER 1

Getting Started with VirusScan Plus

Cox Security Suite powered by McAfee™ includes VirusScan Plus which protects your computer and files from viruses, spyware, and hackers. You can surf the Web and download files safely and confidently, knowing Cox Security Suite is always on, always updating, and always protecting you. Cox Security Suite's trusted protection blocks threats and deters hackers automatically, keeping your computer healthy and secure. Cox Security Suite also makes it easy to view your security status, scan for viruses and spyware, and ensure your products are up-to-date using the redesigned SecurityCenter. Plus, you will receive the latest Cox Security Suite software and updates with your subscription automatically.

VirusScan Plus includes the following programs:

- SecurityCenter
- VirusScan
- Personal Firewall

CHAPTER 2

SecurityCenter

SecurityCenter is an easy-to-use environment where Cox Security Suite users can launch, manage, and configure their security subscriptions.

SecurityCenter also acts as a source of information for virus alerts, product information, support, subscription information, and one-click access to tools and news.

Features

SecurityCenter provides the following new features and benefits:

Redesigned protection status

Easily review your computer's security status, check for updates, and fix potential security issues.

Continual updates and upgrades

Automatically install daily updates. When a new version of Cox Security Suite software is available, you get it automatically at no charge during your subscription, ensuring that you always have up-to-date protection.

Real-time alerting

Security alerts notify you of emergency virus outbreaks and security threats, and provide response options to remove, neutralize, or learn more about the threat.

Convenient protection

A variety of renewal options help keep your Cox Security Suite protection current.

Performance tools

Remove unused files, defragment used files, and use system restore to keep your computer running at peak performance.

Real online help

Get support from Cox Security Suite's computer security experts, by Internet chat, e-mail and telephone.

Safe surfing protection

If installed, the SiteAdvisor browser plug-in helps protect you from spyware, spam, viruses, and online scams by rating Web sites you visit or that appear in your Web search results. You can view detailed safety ratings that show how a site tested for e-mail practices, downloads, online affiliations, and annoyances such as pop-ups and third-party tracking cookies.

CHAPTER 3

Using SecurityCenter

You can run SecurityCenter from the Cox Security Suite SecurityCenter in the Windows notification area at the far right of the taskbar or from your Windows desktop.

When you open SecurityCenter, the Home pane displays your computer's security status and provides quick access to updating, scanning and other common tasks:

Header

Help

View the program help file.

Left column

Update

Update your product to ensure protection from the latest threats.

Scan

If VirusScan is installed, you can perform a manual scan of your computer.

Common tasks

Perform common tasks including returning to the Home pane, viewing recent events, managing your computer network (if on a computer with management capability for this network), and maintaining your computer. If Cox Security Suite Data Backup is installed, you can also back up your data.

Components installed

See which security services are protecting your computer's security.

Main pane

Protection Status

Under Am I Protected? see the overall level of your computer's protection status. Below it, view a status breakdown by protection category and type.

SecurityCenter Information

See when the last update of your computer occurred, when the last scan occurred (if VirusScan is installed), as well as when your subscription expires.

Understanding SecurityCenter icons

SecurityCenter icons appear in your Windows notification area, at the far right of the taskbar. Use them to see whether your computer is fully protected, view the status of a scan in progress (if VirusScan is installed), check for updates, view recent events, maintain your computer, and get support.

Open SecurityCenter and use additional features

When SecurityCenter is running, the SecurityCenter icon appears in your Windows notification area, at the far right of the taskbar.

To open SecurityCenter or use additional features:

Right-click the main SecurityCenter icon, and click one of the following:

- Open SecurityCenter
 - Updates
 - Quick Links
 - The submenu contains links to Home, View Recent Events, Manage Network, Maintain Computer, and Data Backup (if installed).
 - Verify Subscription
 - (This item appears when at least one product subscription is expired.)
 - Upgrade Center
 - Customer Support

Check your protection status

If your computer is not fully protected, the protection status icon appears in your Windows notification area, at the far right of the taskbar. The icon can be red or yellow based on the protection status.

To check your protection status:

- Click the protection status icon to open SecurityCenter and fix any problems.

Check the status of your updates

If you are checking for updates, the updates icon appears in your Windows notification area, at the far right of the taskbar.

To check the status of your updates:

- Point to the updates icon to view the status of your updates in a tool tip.

Understanding the protection status

Your computer's overall security protection status is shown under Am I Protected? in SecurityCenter.

The protection status informs you whether your computer is fully protected against the latest security threats, or whether problems require attention and how to resolve them. When one problem affects more than one protection category, fixing the problem can result in multiple categories returning to fully protected status.

Some of the factors that influence your protection status include external security threats, the security products installed on your computer, products that access the Internet, and how these security and Internet products are configured.

By default, if Spam Protection or Content Blocking are not installed, these non-critical protection problems are automatically ignored and not tracked in the overall protection status. However, if a protection problem is followed by an Ignore link, you can choose to ignore the problem if you are sure that you do not want to fix it.

Am I protected?

See the overall level of your computer's protection status under Am I Protected? in SecurityCenter:

- Yes appears if your computer is fully protected (green).
- No appears if your computer is partially protected (yellow) or not protected (red).

To resolve most protection problems automatically, click Fix next to the protection status. However, if one or more problems persist and require your response, click the link following the problem to take the suggested action.

Understanding protection categories and types

Under Am I Protected? In SecurityCenter, you can view a status breakdown consisting of these protection categories and types:

- Computer and Files
- Internet and Network
- E-mail and IM
- Parental Controls

The protection types shown in SecurityCenter depend on which products are installed. For example, the PC Health protection type appears if Cox Security Suite Data Backup software is installed.

If a category does not have any protection problems, its status is Green. If you click a Green category, a list of enabled protection types appears on the right, followed by a list of already ignored problems. If no problems exist, a virus advisory appears in place of any problems. You can also click Configure to change your options for that category.

If all of the protection types within a category have a status of Green, then the status of the category is Green. Likewise, if all of the protection categories have a status of Green, then the overall Protection Status is Green.

If any protection categories have a status of Yellow or Red, you can resolve the protection problems by fixing or ignoring them, which changes the status to Green.

Understanding Computer and Files protection

The Computer and Files protection category consists of these protection types:

- **Virus Protection**—Real-time scanning protection defends your computer against viruses, worms, Trojan horses, suspect scripts, hybrid attacks, and other threats. It automatically scans and attempts to clean files (including .exe compressed files, boot sector, memory, and critical files) when they are accessed by either you or your computer.
- **Spyware Protection**—Spyware protection quickly detects, blocks, and removes spyware, adware, and other potentially unwanted programs that might gather and transmit your private data without your permission.
- **SystemGuards**—SystemGuards detect changes to your computer and alert you when they occur. You can then review these changes and decide whether to allow them.
- **Windows Protection**—Windows protection provides the status of Windows Update on your computer. If VirusScan is installed, buffer overflow protection is also available.

One of the factors that influence your Computer and Files protection is external virus threats. For example, if a virus outbreak occurs, does your antivirus software protect you? Also, other factors include the configuration of your antivirus software and whether your software is continuously being updated with the latest detection signature files to protect your computer from the latest threats.

Open the Computer and Files configuration pane

When no problems exist under Computer & Files, you can open the configuration pane from the information pane.

To open the Computer and Files configuration pane:

- 1 In the Home pane, click Computer & Files.
- 2 In the right pane, click Configure.

Understanding Internet and Network protection

The Internet and Network protection category consists of these protection types:

- **Firewall Protection**—Firewall protection defends your computer against intrusion and unwanted network traffic. It helps you manage inbound and outbound Internet connections.
- **Wireless Protection**—Wireless protection defends your home wireless network against intrusion and data interception. However, if you are currently connected to an external wireless network, your protection varies based on the security level of that network.
- **Web Browsing Protection**—Web browsing protection hides advertisements, pop-ups, and Web bugs on your computer when you browse the Internet.
- **Phishing Protection**—Phishing protection helps block fraudulent Web sites that solicit personal information through hyperlinks in e-mail and instant messages, pop-ups, and other sources.
- **Personal Information Protection**—Personal information protection blocks the release of sensitive and confidential information over the Internet.

Open the Internet and Network configuration pane

When no problems exist under Internet & Network, you can open the configuration pane from the information pane.

To open the Internet and Network configuration pane:

- 1 In the Home pane, click Internet & Network.
- 2 In the right pane, click Configure.

Understanding E-mail and IM protection

The E-mail and IM protection category consists of these protection types:

- **E-mail Protection**—E-mail protection automatically scans and attempts to clean viruses, spyware, and potential threats in inbound and outbound e-mail messages and attachments.
- **Spam Protection**—Spam protection helps block unwanted e-mail messages from entering your Inbox.
- **IM Protection**—Instant Messaging (IM) protection automatically scans and attempts to clean viruses, spyware, and potential threats in inbound instant message attachments. It also blocks instant messaging clients from exchanging unwanted content or personal information over the Internet.
- **Safe Surfing protection**—If installed, the SiteAdvisor browser plug-in helps protect you from spyware, spam, viruses, and online scams by rating Web sites you visit or that appear in your Web search results. You can view detailed safety ratings that show how a site tested for e-mail practices, downloads, online affiliations, and annoyances such as pop-ups and third-party tracking cookies.

Open the E-mail and IM configuration pane

When no problems exist under E-mail & IM, you can open the configuration pane from the information pane.

To open the E-mail and IM configuration pane:

- 1 In the Home pane, click E-mail & IM.
- 2 In the right pane, click Configure.

Understanding Parental Controls protection

If your children use your computer, you can configure Parental Controls for them. You use Parental Controls to help regulate what your children can see and do while they browse the Web.

With Parental Controls, you can:

- Enable or disable image filtering - image filtering blocks potentially inappropriate images from displaying when a child browses the Web.
- Choose a content rating group - this determines the kind of content and Web sites that are accessible to a child, based on the child's age group.
- Set Web browsing time limits, the Web browsing time limits define the days and times a child can access the Web.

Parental Controls also lets you filter (block or allow) certain Web sites for all children.

Note: You must be an Administrator to set up Parental Controls.

Open the Parental Controls configuration pane

When no problems exist under Parental Controls, you can open the configuration pane from the information pane.

To open the Parental Controls configuration pane:

- 1 In the Home pane, click Parental Controls.
- 2 In the right pane, click Configure.

Configuring Users

To configure Parental Controls, you assign permissions to SecurityCenter users. By default, SecurityCenter users correspond to the Windows users that you have set up on your computer.

Note: To configure users, you must log in to SecurityCenter as an administrator.

Working with windows users

To configure Parental Controls, you must assign permissions to users which determine what each user can see and do on the Internet. You add a user, edit a user's account information, or remove a user under Computer Management in Windows.

Adding a new SecurityCenter user

- 1 Log in to SecurityCenter as the Administrator user.
- 2 Open the Users Settings pane.
 - Under Common Tasks, click **Home**.
 - On the SecurityCenter Home pane, click **Parental Controls**.
 - In the Parental Controls information section, click **Configure**.
 - On the Parental Controls Configuration pane, click **Advanced**.
- 3 On the Users Settings pane, click **Add**.
- 4 Follow the on-screen instructions to set up a user name, password, account type, and parental controls.
- 5 Click **Create**.

Edit a SecurityCenter user's account information

You can change a user's password, account type, or automatic login ability or remove the user following the same in

- 1 Log in to SecurityCenter as the Administrator user.
- 2 Open the Users Settings pane.
 - Under Common Tasks, click **Home**.
 - On the SecurityCenter Home pane, click **Parental Controls**.
 - In the Parental Controls information section, click **Configure**.
 - On the Parental Controls Configuration pane, click **Advanced**.
- 3 On the Users Settings pane, click a user name, and then click **Edit**.
- 4 Follow the on-screen instructions to edit the user's password, account type, or parental controls.
- 5 Click **OK**.

Remove a SecurityCenter user

You can remove a McAfee user at any time.

To remove a McAfee user:

- 1 Log in to SecurityCenter as the Administrator user.
- 2 Open the Users Settings pane.
 - Under Common Tasks, click **Home**.
 - On the SecurityCenter Home pane, click **Parental Controls**.
 - In the Parental Controls information section, click **Configure**.
 - On the Parental Controls Configuration pane, click **Advanced**.
- 3 On the Users Settings pane, under **Cox Security Suite User Accounts**, select a user name, and then click **Remove**.

Fixing protection problems

Most protection problems can be resolved automatically. However, if one or more problems persist, you must resolve them.

Fix protection problems automatically

Most protection problems can be resolved automatically.

To fix protection problems automatically:

- Click Fix next to the protection status.

Fix protection problems manually

If one or more protection problems are not resolved automatically, click the link following the problem to take the suggested action.

To fix protection problems manually:

- Do any of the following:
 - If a full scan of your computer has not been performed in the last 30 days, click Scan to the left of the main protection status to perform a manual scan. (This item appears if VirusScan is installed.)
 - If your detection signature (DAT) files are out-of-date, click Update to the left of the main protection status to update your protection.
 - If a program is not installed, click Get full protection to install it.
 - If a program is missing components, reinstall it.
 - If a program must be registered to receive full protection, click Register now to register it. (This item appears if one or more programs are expired.)
 - If a program is expired, click Verify my subscription now to check your account status. (This item appears if one or more programs are expired.)

CHAPTER 4

Getting Started with Privacy Service

Cox Security Suite powered by McAfee™ includes Privacy Service™ which offers advanced protection for you, your family, your personal data, and your computer.

Features

This release of Privacy Service includes the following features:

- Internet time usage rules - Specify days and times when users can access the Internet.
- Custom keyword filtering - Create keyword rules that permit or block users from accessing Web sites.
- Privacy Service backup and restore - Save and restore Privacy Service settings at any time.
- Web bug blocker—Block Web bugs (objects obtained at potentially harmful web sites) so that they are not loaded within browsed web pages.
- Shredder—Protects your privacy by quickly and safely erasing unwanted files.
- Parental Controls—Content Blocking prevents users from viewing unwanted Internet content by blocking potentially harmful Web sites. Users' Internet activity and usage can also be monitored and limited.

The Administrator

The Administrator specifies which users can access the Internet, when they can use it, and what they can do on the Internet.

NOTE: The Administrator is considered an adult and as such can access all web sites but is prompted to allow or prevent the transmission of added personal identifiable information (PII).

Setting up Privacy Service

The Setup Assistant allows you to create the Administrator, manage global settings, enter personal information, and add users.

Remember your Administrator password and security answer so that you can logon to Privacy Service. If you cannot logon, you cannot use Privacy Service and the Internet. Keep your password secret so only you can change Privacy Service settings. Some Web sites require that cookies are enabled to work properly.

NOTE: If your PC includes a pre-installed copy of Privacy Service, some steps described in this documentation may not appear. For more information, see [Setting up a Pre-installed version of Privacy Service](#) and your PC manufacturer's documentation.

Setting up a Pre-installed version of Privacy Service

If Privacy Service is pre-installed on Windows XP, you must logon to Windows with a Windows Administrator account to set up the product.

To configure a pre-installed version of Privacy Service:

- 1 If you have not done so already, launch the Setup Assistant using one of the following methods:
 - Right-click the Cox Security Suite icon in the Windows system tray, point to **Privacy Service**, and then select **Setup Privacy Service**.
 - From the Windows **Start** menu, point to **Cox Security Suite**, and then select **Privacy Service**.
 - Double-click the **Privacy Service** desktop icon.
 - Launch SecurityCenter, click the **privacy service** tab, and then **Setup Privacy Service** to launch the Setup Assistant.
- 2 Proceed to and complete each step that is provided.

NOTE: To cancel configuration, click **Cancel**.

Retrieving the Administrator Password

If you forget the Administrator password, you can access the password using the security information you entered when you created the Administrator profile.

To retrieve the Administrator password:

- 1 Right-click the Cox Security Suite icon in the Windows system tray, point to **Privacy Service**, then select **Sign In**.
- 2 Select **Administrator** from the **User Name** pull-down menu.
- 3 Click **Forgot your password?**
- 4 Enter the answer to the security question that appears, and then click **Get Password**. A message appears containing your password. If you forget the answer to the security question, you must remove Privacy Service from Safe Mode (Windows 2000 and Windows XP only).

Removing Privacy Service with Safe Mode

To remove Privacy Service with Safe Mode:

- 1 Click **Start** and point to **Shut Down**. The **Shut Down Windows** dialog box appears.
- 2 Select **Shut down** from the menu and then click **OK**.
- 3 Wait until the **It is now safe to turn off the computer** message appears, and then turn the computer off.
- 4 Turn the computer back on.
- 5 Begin immediately pressing the **F8** key, every other second, until the **Windows Startup** menu appears.
- 6 Select **Safe Mode** and press **Enter**.
- 7 When Windows starts, a message appears explaining Safe Mode. Click **OK**.
- 8 Proceed to **Add or Remove Programs**, located in the Windows Control Panel. When you are done, reboot the PC.
- 9 Re-install Privacy Service and specify the Administrator password. Make a note of the password you specify.

NOTE: You can remove Privacy Service in Safe Mode in Windows 2000 or Windows XP only.

The Startup user

The Startup user is automatically signed in to Privacy Service when the computer is started.

For example, if a user is on the computer or Internet more than the others, you can make that user, including the Administrator, the Startup user. When the Startup user uses the computer, the user is not required to sign in to Privacy Service.

If you have young children, you can also set the Startup user to the youngest. This way, when an older user uses the computer, they can log off from the young user's account and then log in again using their own user name and password. This protects younger users from seeing inappropriate Web sites.

Configuring the Administrator as Startup User

To configure the Administrator as Startup user:

- 1 From the **Please Sign In** dialog, select your user name from the **User name** pull-down menu.
- 2 Enter your password in the **Password** field.
- 3 Select **Make this user the Startup User**, and then sign in.

CHAPTER 5

Launching Privacy Service

After you install Privacy Service, the Cox Security Suite icon appears in the Windows system tray, which is located near the system clock. From the Cox Security Suite icon, you can access Privacy Service, SecurityCenter, and other related products installed on your computer.

NOTE: If your product is pre-installed, you must first set it up. For more information, see *Setting up a Pre-installed version of Privacy Service*.

Launching and signing in to Privacy Service

- 1 Right-click the Cox Security Suite icon in the Windows system tray, point to **Privacy Service**, and then select **Sign In**.
- 2 Select your user name from the **User name** pull-down menu.
- 3 Enter your Password in the **Password** field.
- 4 Click **Sign In**.

Disabling Privacy Service

You must be logged in to Privacy Service as the Administrator to disable it.

To disable Privacy Service:

- Right-click the Cox Security Suite icon, point to Privacy Service, and then select Sign Out.

NOTE: If **Sign In** is in the place of **Sign Out**, then you are already signed out.

Updating Privacy Service

SecurityCenter regularly checks for updates to Privacy Service while your computer is running and connected to the Internet. If an update is available, SecurityCenter prompts you to update Privacy Service.

To manually check for updates:

- Click the **Updates** icon located in the top pane.

Removing and re-installing Privacy Service

You must be logged in to Privacy Service as the Administrator to un-install the product.

If this Cox Security Suite product is pre-installed on your computer, see your PC manufacturer's documentation for information about removing and re-installing Privacy Service.

NOTE: Removing Privacy Service erases all Privacy Service data.

Removing Privacy Service

To remove Privacy Service:

- 1 Save all of your work and close any open applications.
- 2 Open the Control Panel:
- 3 Windows 98, Windows Me, and Windows 2000 users-Select Start, point to **Settings**, and then click **Control Panel**.
- 4 Windows XP users-On your Windows taskbar, select **Start**, and then click Control Panel.
- 5 Open the **Add/Remove Programs** dialog box:
- 6 Windows 98, Me, and 2000 users-Double-click **Add/Remove Programs**.
- 7 Windows XP users-Click **Add or Remove Programs**.
- 8 Select Privacy Service from the list of programs, and then click **Change/Remove**.
- 9 When asked to confirm the operation, click **Yes**.
- 10 When you are prompted to restart your system, click **Close**. Your computer re-starts to complete the un-installation process.

Installing Privacy Service

To install Privacy Service:

- 1 Click the **Download** link on the Privacy Service page.
- 2 Click **Yes** on any messages that appear asking if you want to download files from the web site.
- 3 Click **Start Installation** on the Privacy Service Installation window.
- 4 When the download is complete, click **Restart** to restart your computer. Or, click **Close** if you need to save any work or quit any programs, then restart your computer as you normally would. You must restart your computer in order for Privacy Service to work properly.

After the computer restarts, you need to create the Administrator again.

If this Cox Security Suite product is pre-installed on your computer, see your PC manufacturer's documentation for information about re-installing Privacy Service.

Configuring Parental Controls

Filtering potentially inappropriate Web images

By default, new users are added to the Adult group and image filtering is disabled. If you want to block potentially inappropriate images from appearing when a particular user browses the Web, you can enable image filtering. Each potentially inappropriate Web image is automatically replaced with a static Cox Security Suite image.

- 1 Open the user setting pane.
- 2 Go to the SecurityCenter Home Pane click on **Parental Controls**
- 3 In the Parental Controls information section click **Configure**
- 4 On the configure pane, click **Advanced** then **User Settings**
- 5 On the Users Settings pane, click a user name, and then click **Edit**
- 6 In the Edit User Account window, under Image Filtering, click **On**
- 7 Click **OK**

Setting the content rating group

By default, a new user is added to the Adult group, which allows the user to access all Web content. You can then adjust the user's content rating group according to the individual's age and maturity level.

- 1 Go to the SecurityCenter Home pane, click on **Parental Controls**
- 2 In the Parental Controls information section click **Configure**
- 3 On the configuration pane, click **Advanced**
- 4 click **User Settings**
- 5 On the User Settings pane, click a user name, and then click **Edit**
- 6 In the Edit User Account window, under **Content Rating**, click the age group you want to assign to the user.
- 7 Click **OK**.

Setting Web browsing time limits




You can use the Web browsing time limits grid to restrict a child's Web browsing to specific days and times.

- 1 Go to the SecurityCenter Home Pane, click on **Parental Controls**
- 2 In the Parental controls information section click **Configure**
- 3 On the configuration pane, click **Advanced**
- 4 Click on **User Settings**.
- 5 On the User Settings pane, click a user name, and then click **Edit**
- 6 In the Edit User Account window, under **Internet Time Limits**, drag your mouse to specify the days and times that this user cannot browser the web.
- 7 Click **OK**

CHAPTER 6

Getting Started with SiteAdvisor

Cox Security Suite powered by McAfee™ includes SiteAdvisor which helps protect you from dangerous sites that engage in “social engineering” attacks such as adware, spam, and phishing scams. SiteAdvisor adds intuitive red, yellow and green icons to sites and search results to help keep you safe as you search, browse, and transact online.

	Safe: We tested the site and didn't find any significant problems.
	Caution: Our tests revealed some minor security or nuisance issues. Also applies to sites which have previously had (directly or through corporate affiliation) past security issues.
	Warning: Our automated tests and/or our manual analysis revealed some serious issues to consider before using the site at all. (Example: the site sent us lots of spammy emails, bundled adware with a download, or has a business relationship with a company know for bad past practices).

SiteAdvisor's safety ratings are grounded in a massive proprietary database containing test results from millions of automated Web site visits, download installations, and email registrations. SiteAdvisor's automated tests are supplemented by feedback from volunteer reviewers, comments from Web site owners and input from SiteAdvisor analysts.

SiteAdvisor's safety tests of sites representing about 95% of Web traffic have resulted in:

- Red ratings for about 5% of sites
- Yellow ratings for about 2% of sites

Many popular Web categories (examples: screensavers, free games, contests) have a much higher percentage of red and yellow sites. Every month users unknowingly click on an estimated 175 million “red” sites in search engine results alone.

Benefits

- Protects you from adware, spyware, spam, viruses and phishing scams.
- Advises you about the safety of sites using a colored button in your browser toolbar.
- Enhances your online search by placing safety ratings next to search results.
- Warns you about dangerous sites and search results with clear messages.
- Provides you with all the details about a site's safety rating on request.
- Updates automatically to protect against new threats.

Features

Safe search

When using popular search engines like Google, Yahoo!, MSN, AOL, or Ask.com, SiteAdvisor's safety ratings appear next to search results.

Safe browse

When browsing, a small button in your browser toolbar changes color based on SiteAdvisor's safety results. Menu options on SiteAdvisor's toolbar let you customize SiteAdvisor or see a Web site's detailed test results.

Roll your mouse over any SiteAdvisor safety rating to see more information about the Web site. You can also visit any site's 'report page' for complete detailed safety information and to read what users have to say.

Advanced phishing protection

Real-time scanning combined with checks against SiteAdvisor's database help warn you about phishing sites designed to steal your identity.

Know in advance

Warnings inform you about threatening Web sites with real-time alerts.

Transact safety

SiteAdvisor's advanced phishing protection uses a combination of database checking and real-time analysis to help identify scam sites that try to steal your personal information and, ultimately, your identity.

Real Advice

SiteAdvisor has already tested sites representing more than 95% of the world's web traffic. SiteAdvisor provides real and objective advice that is based on automated tests and enhanced by human feedback and analysis.

How SiteAdvisor works

SiteAdvisor uses a system of automated robots to test every Web site, download, and e-mail sign-up form on the Web.

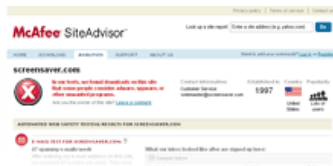


Enter the following for your chance to win!
NOTE: Fields marked with an asterisk (*) are REQUIRED.

Your first name -
E-Mail Address -

REVIEWER COMMENTS (3)

Adware, Spyware, or Viruses
This site has some serious security flaws
Posted at 8:44 AM on February 7, 2006 by Dr. ...
Member since July 2006 (Reputation score: 98 of 1...



Is it safe to browse?

Web sites are tested for 'phishing' and other online scams, affiliations with dangerous sites, excessive pop-ups, and browser exploits. We've tested sites representing more than 95% of worldwide Web traffic.

Is it safe to download?

Downloads are tested for viruses and bundled adware, spyware or other unwanted programs. We've tested more than 5 million to date.

Is it safe to submit?

Sign-up forms are completed using a one-time use e-mail address so any subsequent spam can be tracked. Our bots receive mail from more than 7 million places already.

What do others say?

Feedback from individual users and analysis by SiteAdvisor staff provide insight into the site's current and past practices as well as its corporate affiliations.

Show me the details.

Site Report pages document every SiteAdvisor test. (See an example)

What we've tested

We've already tested most of the sites on the Internet. To date, we have:

- Evaluated Web sites covering 95% of Web traffic
- Downloaded and tested more than 1.6 million pieces of software (as of July 2006)
- Provided unique e-mail addresses for more than 5.5 million registration forms (as of July 2006)
- SiteAdvisor hasn't scanned everything yet, but we're well on our way, and we continue to perform tens of thousands of new tests every day.

Re-testing

We retest sites on a regular basis, so our bots can tell if a site changed its behavior for better or worse. We like to see bad guys get better. Because we revisit and retest every site over time, Web sites that engage in malicious activity have a chance to clean up their acts. But don't expect our ratings to change overnight. The only way for ratings to change is to get clean and stay clean.

Phishing

"Phishing" is a practice where scammers try to collect credit card or other information by mimicking reputable Web sites. For example, phishers might send a spam e-mail purporting to be from a reputable bank, and indicate that "Account information needs to be updated- click here." The link would lead to a fake site which would try to entice the victim to provide credit card or other financial information. Because they are illegal and are often shut down quickly, phishing sites may remain active for only a few days or a few hours.

SiteAdvisor's software does not currently provide automated or real-time phishing detection. This feature is currently under development. However, SiteAdvisor reviewers can report sites which they believe to be conducting phishing or other online scams, using the user comments area of any site's report page.

In general, if a site purporting to be from an established financial institution or large company is asking for financial or extensive personal information, and SiteAdvisor's safety button indicates that it has NOT yet been tested by us, you should be very cautious. SiteAdvisor has tested sites representing more than 95% of Web traffic, so it is extremely unlikely that a popular site (such as from a large bank or one of the Web's largest online retailers) would not have been tested if it is truly authentic.

Email Spamminess

Spamminess may sound like a whimsical word, but the spamminess scores we attribute to Web sites are based on hard facts and data. To determine an e-mail's spamminess score, SiteAdvisor starts with a software program called SpamAssassin. SpamAssassin rates e-mails on a variety of criteria and assigns ratings based on whether the e-mail is more or less likely to be what most people would consider spam. For example, SpamAssassin evaluates an e-mail's commercial content and whether the e-mail employs tricks known to be used by spammers attempting to get through anti-spam filters. The e-mail we receive may not qualify as spam under current industry and legal definitions because SiteAdvisor affirmatively opts to receive the e-mail we get. Our goal is to be able to tell you what might happen if you sign-up too. We use SpamAssassin to provide you with a spamminess score to help you make an informed judgment about whether to supply a site with your e-mail address or not.

Adult Content

Our goal is to protect your online experience by testing and reporting Web sites that contain or refer to malicious content. We test for overall security and online nuisances. We do not test for potentially offensive content. For this reason, Adult sites will receive green ratings if they pass our safety tests.

Please do not equate a green safety rating as an endorsement of a particular site's content, or as a general quality rating.

File Types

SiteAdvisor does not test certain file types such as graphic files like .jpg or .gif, audio or video files like .mp3 or .mpg, or document files such as .doc. We continually increase the types of files we test and update our site details page as we compile new data.

Because there are plenty of examples of .jpg files and other file formats being used to conduct exploits, you should continue to employ traditional security defenses like anti-virus and firewall programs. Our exploit detection will prevent some of these attacks as well, but a multi-tiered defense is essential to browsing safety.

We do not yet systematically test for a variety of e-commerce scams or frauds. Because of this, those who purchase from online pharmacies, download ring tones, or sign up for work at home programs are vulnerable to a variety of scams. We are increasing our coverage of Web sites that engage in these kinds of frauds by manually researching sites and soliciting feedback from our reviewers and respected fraud researchers.

Browser Exploits

Browser exploits are rare but extremely dangerous security threats caused by a Web site which uses malicious code to exploit certain vulnerabilities in your web browser. These exploits have a wide range of possible effects such as:

- Installing spyware or adware on your computer
- Installing keylogging software which can steal account information and passwords
- Running malicious code which can disable or take control of parts of your computer

If you try to browse to a site that has attempted exploits during SiteAdvisor safety testing, you will be redirected to a warning page. If you decide that you still want to visit the site, you can add the site to the SiteAdvisor **Do Not Warn list**. To do this, click the SiteAdvisor icon in your browser's toolbar and select **Do Not Warn list**. Type the URL of the site and click **Add**. You can then close the dialog box and browse to the site. You will no longer be redirected to the warning page for that site.

CHAPTER 7

SiteAdvisor Configuration and Support

Supported Browsers

SiteAdvisor supports both Internet Explorer and Firefox. SiteAdvisor for IE and SiteAdvisor for Firefox are each compatible with one another on the same computer. You can install our extension for each browser and not expect an incompatibility issue to arise.

SiteAdvisor is currently only supported for use with Microsoft Internet Explorer and Mozilla Firefox. Support for other browsers is planned for future releases; however there is no timetable available for this functionality.

SiteAdvisor works in stand-alone instances of Internet Explorer and Firefox. To browse the Internet with SiteAdvisor in Internet Explorer or Firefox while online with AOL or MSN, please open a separate Internet Explorer or Firefox browser window.

Search Engines

Given that most of the threats that SiteAdvisor protects against are not search engine specific, we are interested in supporting all of the search engines that people use. We prioritize supporting search engines based on the number of users that would benefit from our adding support. At this point, we do not have concrete plans for search engines other than Google, Yahoo! or MSN, but we are constantly re-evaluating how to best support our users.

Footprint

SiteAdvisor is extremely lean, at about 500K for the Internet Explorer version and 40K for Firefox. It takes about 30 seconds to install. The software calls on Cox Security Suite powered by McAfee™'s central database of safety results to provide safety ratings, so data is always up to date and never has to be transferred to the individual user.