Read Me

About the Product

Webroot Spy® Sweeper™ helps you protect your privacy and your computer from the threat of spyware, adware and other potentially unwanted programs. Spy Sweeper searches for many types of potentially unwanted programs from those that monitor all of your computer's activities (system monitors), to those that can steal or destroy data (Trojan horses). It also detects programs that pop up advertising on your computer (adware) and cookies that may contain personal information (tracking cookies).

Spy Sweeper "sweeps" your computer looking for evidence of potentially unwanted programs, such as spyware, adware, and suspect programs, reports its findings, and lets you decide whether to quarantine the item or keep it. The quarantine function disables the item until you decide to delete it completely or restore it.

If you have Spy Sweeper with AntiVirus, it also looks for viruses during sweeps.

Software Detected by Webroot Spy Sweeper

Adware
Adware is a type of software that may display advertisements on your system. Some adware may also hijack Web searches, meaning it may reroute your Web searches through its own Web page. It may change your default home page to a specific Web site. Adware generally propagates itself using dialog boxes, various social engineering methods, or through scripting errors. Adware and BHOs are often bundled with various free software programs, such as clocks, messengers, alerts, and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Removing adware bundled with free software programs may cause the software to stop operating. These adware programs may also cause slowing of your Web browser and system performance issues.

System Monitor Software
System monitors, typically non-commercial, may monitor and capture your computer activity, including recording all keystrokes, e-mails, chat room dialogue, instant message dialogue, Web sites visited, usernames, passwords, and programs run. This program may be capable of taking screen shots of your desktop at scheduled intervals, storing the information on your computer in an encrypted log file for later retrieval. These log files may be e-mailed to a pre-defined e-mail address. This program can run in the background, hiding its presence. These programs typically install via other threats, such as music downloads, and Trojan downloaders. These system monitors may allow an unauthorized, third party to view potentially sensitive information, such as passwords, e-mail, and chat room conversation

Trojan Horse
A Trojan horse may manage files on your computer, including creating, deleting, renaming, viewing, or transferring files to or from your computer. It can utilize a program manager that allows a hacker to install, execute, open, or close programs. The hacker can gain remote control of your cursor and keyboard and can even send mass e-mails from your infected computer. It can run in the background, hiding its presence. A Trojan is usually disguised as a harmless software program and may also be distributed as an e-mail attachment. Opening the program or attachment may cause an auto-installation process that loads the downloader onto your computer and download third party programs on your computer, resulting in the installation of unwanted programs without your knowledge or consent, jeopardizing your privacy if it downloads another Trojan or a system monitor. Trojans may open a port on your computer that may enable a hacker to gain remote control of your computer.

Potentially unwanted program
A potentially unwanted program is a program that may change the security or privacy state of your computer and online activities. These programs can (but do not necessarily) collect information about your online activities and send it to a third party without your knowledge or consent. A potentially unwanted program may arrive bundled with freeware or shareware, various social engineering methods, or by someone with access to your computer. Users may decide to remove these programs by using desktop security product.

Virus
A virus is a self-replicating program that can infect computer code, documents, or applications. While some viruses are purposefully malignant, others are more of a nuisance, replicating uncontrollably and inhibiting system performance.

New in Spy Sweeper 5.2

- Now you can choose a quick, full, or customized sweep without changing your sweep options. In addition, you can schedule any or all of the three sweep types.
    - Choose a quick sweep to do a short scan and diagnosis of your computer. If Spy Sweeper finds potentially unwanted programs or viruses, it recommends that you perform a full sweep..
    - Run a full sweep on a weekly basis to ensure the maximum protection from potentially unwanted programs and viruses.
    - For more pinpointed searches, customize your sweep to have Spy Sweeper skip files by folder or extension.

- Improved sweep configuration allows you to exclude sections of your computer from the sweep by viewing your file system and selecting exclusions, or by file extension such as .xls or .mpg.

- If you have Spy Sweeper with AntiVirus, you also have protection against viruses. You can tell Spy Sweeper to search for viruses during sweeps and to continuously monitor your computer for the types of actions that viruses typically take, by using shields.

System Requirements

Spy Sweeper or Spy Sweeper with AntiVirus
V5.2
Download size: 11.9 MB
German: V5.2 Größe: 37.7 MB
Dutch: V5.2 Groote: 37.7 MB
Spanish: V5.2 Tamaño: 37.7 MB
Italian: V5.2 Dimensione: 37.7 MB
French: V5.2 Taille: 37.7 Mo
Japanese: V5.2サイズ: 37.7 MB

Windows 2000 or XP (Professional, Home, Media Center, or XP Tablet)
300 MHz processor
15 MB hard drive space
256 MB RAM
Supports Internet Explorer 5.5 or higher

Webroot Contact Information

Webroot World Headquarters

Mailing Address
P.O. Box 19816
Boulder, CO 80308-2816
USA

Office Address
2560 55th Street
Boulder, CO 80301
USA

Advanced Technology Development Center

1200 Villa Street
Mountain View, CA 94041
USA

Support & Sales: (866) 612-4227

Fax: (303) 442-3846

United Kingdom

Webroot Limited
EMEA Enterprise Headquarters
3000 Hillswood Drive
Chertsey
Surrey
KT16 ORS
England

Consumer Support: +44 (0) 845 838 1130

Enterprise Post Sales Support: +44 (0) 845 838 1160

Contact: +44 (0) 870 3516 788

Fax: +44 (0) 870 3516 789

Deutschland

Webroot GmbH
Biedrichstraße 8
D 61200 Wölfersheim
Deutschland

Support: +49 (0) 6036 9836 783

Kontakt: +49 (0) 6036 989 70

Fax: +49 (0) 6036 904 321

France

Webroot France

120 rue Jean Jaurès
F-92300 Levallois-Perret
France

Support: +33 (0) 1 70 98 77 86

Contact: +33 (0) 1 70 98 78 08

Fax: +33 (0) 1 70 98 78 09

Italia

Webroot Italia
Via Volta 18
I-20094 Corsico Milano
Italia

Supporto: +31 (0) 20 201 4129

Contatto: +39 02 45865576

Fax: +31 (0) 20 45 86 2418

Nederland

Webroot BV
Kingsfordweg 151
1043 GR Amsterdam
Nederland

Support: +31 (0) 20 201 4134

Contact: +31 (0) 20 570 8975

Fax: +31 (0) 20 491 7231

Japan

□□□□□□□□□□□□□□□□
150-0043 □□□□□□□□□ 1-12-1
W 22F, 1-12-1Dogenzaka
渋谷マークシティ W22F

□□□□□□□□ jpcustomer@webroot.com

About the Company

Mission
Foster peace-of-mind through leading privacy, performance and protection software solutions for individuals and enterprises around the globe.

Company Overview
Webroot Software, Inc., a privately held company based in Boulder, Colorado, with offices worldwide, creates innovative privacy, performance and protection products and services for millions of customers in 223 countries, ranging from enterprises to small businesses and home users.

Founded in 1997, the company provides best-of-breed anti-spyware solutions that protect personal information and corporate assets from online and internal threats. Webroot consistently receives top ratings and recommendations by respected third-party media and product reviewers. Webroot

currently has 280 employees worldwide.

Webroot is a privately held company with a strong executive management team with several years of experience at leading security companies. In February 2005, the company accepted its first outside investment of $108 million from a syndicate of leading technology venture capital firms, including Technology Crossover Ventures (TCV), Accel Partners and Mayfield. Prior to February 2005, Webroot established and expanded its business through the reinvestment of cash generated from operations.