WEBROOT® SOFTWARE

A GUIDE TO SECURITY FOR SMALL & MEDIUM BUSINESS

webroot SOFTWARE

Companion Guide to
State of Internet Security: Protecting the SMB
Full report available at www.webroot.com

Table of Contents

Are You an SMB?

Small and medium-sized businesses (SMBs) are generally companies with fewer than 1,000 employees, while some groups include companies with up to 5,000 employees in their definition. The U.S. and Canadian governments define small businesses as those with less than 500 employees. Many private sector companies, including some prominent industry analyst firms, such as Forrester, Gartner and IDC, define small businesses as those with fewer than 100 employees. These same firms define mid-size or medium businesses as those with 100 to 999 employees.

While the precise definitions vary somewhat, there is global consensus that SMBs are a significant part of the economic landscape. These companies are significant contributors to the world's economies in terms of both revenue generation and employment.

According to the U.S. Small Business Administration (SBA), 99.7% of the companies in the U.S. have 500 or less employees, and these companies:

- Produce half of the private, non-farm gross national product (GNP)
- Provide half of all private-sector jobs and 45% of the U.S. private payroll

According to the Canadian government, businesses with less than 100 employees:

- Comprise 95% of Canada's 2.2 million business entities
- Represent roughly a third of the gross domestic product (GDP)
- Employ about 40% of all working Canadians

Why the Focus on Internet Security?

Small and medium-sized businesses (SMBs) face a complex Internet security landscape that includes:

- Pervasive Internet use
- Home-based and remote workers
- Valuable information
- Regulatory requirements
- High infection rates
- Underestimation of certain threats
- Budget and resource constraints

Pervasive Internet Use

Virtually every small and medium-sized business uses the Internet. Wide-spread network access, declining costs of bandwidth and the expanse of Internet resources have made it easier for entrepreneurs and business owners to launch and grow their companies.

Network connectivity enables small and medium sized business to more easily:

- Communicate with customers and suppliers
- Market their services to a global audience
- Research product strategies
- Access Web-based distribution channels, such as Amazon® and eBay®

While the Internet has served as a key driver in the growth and vibrancy of the SMB sector, those network connections also expose SMBs to new security threats.

Home-Based and Remote Workers

Many SMBs start out or remain home-based businesses. Often these businesses lack information technology expertise and specialized personnel to monitor and maintain security.

Internet connectivity also allows employees to work remotely from their homes more easily. SMBs can onboard home-based employees more rapidly and minimize the overhead costs of large office spaces.

While working remotely has become the norm in many companies, it is generally more difficult to maintain security on remote PCs. It's common for employees to use unauthorized mobile devices to access sensitive corporate data, or to rely on open, unsecured wireless networks to connect to work. This creates even more routes for malicious software to infect computers and company networks.

Valuable Information

Personal information about customers and employees has a monetary value in the ecosystem of net criminals. Patent notes, trade secrets and other business intellectual property also have monetary values, and thus have a market of would-be criminals.

In addition to stealing information that can be easily sold or used in identity theft and similar crimes, many spyware infections also aim to gain control of a PC so that it can be exploited, without the user's knowledge, to distribute adware and spam.

Whether distributed via a web site, email, instant messaging or some other means, these spyware programs then seek to use the Internet connection as a means to communicate back to the source and/or to download additional spyware onto the computer.

High Infection Rates

In a recent survey of SMBs based in the U.S. and Canada conducted by Webroot Software, approximately 6 out of 10 respondents reported a virus infection in the past year, in spite of 97% responding that they have an antivirus solution installed.

Approximately 7 out of 10 of the SMBs surveyed indicated their business had a spyware infection in the past year. These results only reflect self-reported infections of spyware, and do not include those infections that may have gone undetected.

The Anti-Spyware Coalition defines spyware as technologies deployed without appropriate user consent and/or implemented in ways that impair user control over:

- Material changes that affect their user experience, privacy, or system security;
- Use of their system resources, including what programs are installed on their computers; and/or
- Collection, use, and distribution of their personal or other sensitive information.

The ongoing misappropriation of system resources and theft of sensitive information make this high rate of spyware infections particularly alarming.

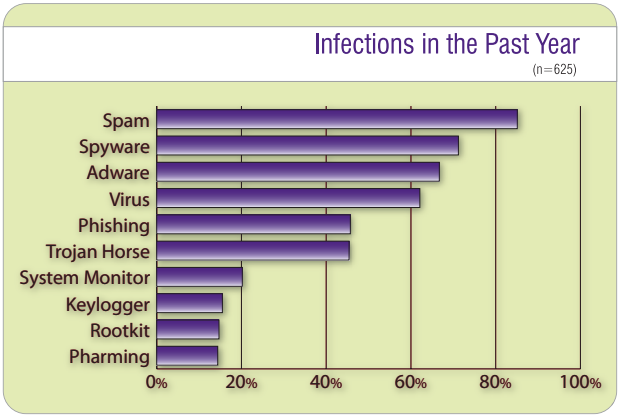


Figure 1 – Source: Webroot Software, SMB Survey, 2007

Regulatory Requirements

Governments in many parts of the world have instituted additional data protection measures to compel companies to adequately protect the sensitive customer data in their possession. For example, the Health Insurance Portability and Accountability Act (HIPAA) legislation requires that the privacy of medical information be adequately protected against unauthorized access and misuse. In the financial sector, the Gramm-Leach-Bliley Act requires that organizations which maintain credit information for customers be held accountable if that data is accessed or compromised by an unauthorized
third party.

All public companies must comply with Sarbanes-Oxley (SOX) which includes attesting to the risk assessment and audit controls required by the Act. Incidents of unauthorized network access, system monitors and Trojans can bring the authenticity of reporting into question, and will raise concerns of SOX non-compliance.

Compliance with these measures can be challenging and expensive for SMBs. However, the potential legal liability and negative publicity for companies that fail to comply can be significantly more costly.

Underestimation of Certain Threats

In some cases, SMBs may also be underestimating the consequences of certain infections. For example, 85% reported spam attacks, yet less than one third identified those as very or extremely serious. While most would agree spam by itself is more of a nuisance than a serious threat, often spam is a carrier for more serious threats, such as spyware, viruses and worms.

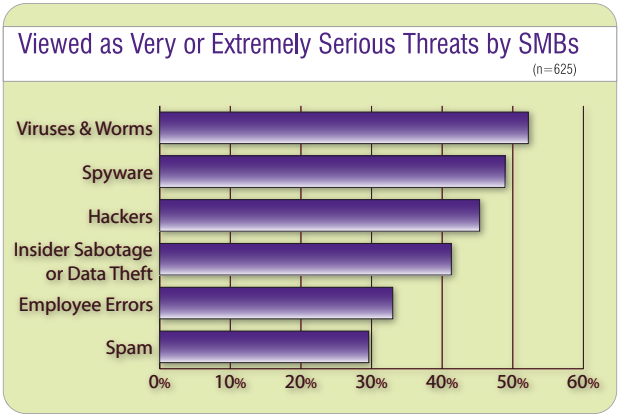


Figure 2 – Source: Webroot Software, SMB Survey, 2007

Spam is cheap for companies. There is almost zero cost associated with mass junk mailings. This makes it an easy and cheap delivery mechanism for malicious attacks. Users who click ads in spam, or even look at a spam e-mail in their preview pane, may be at risk of downloading spyware – commonly referred to as a drive-by download.

A particularly harmful type of spam is phishing. The appearance of these emails, and fake sites they link to, are made to look identical to valid, trustworthy companies, however the scam then asks for personal information, such as credit card, bank account, PIN, or Social Security numbers.

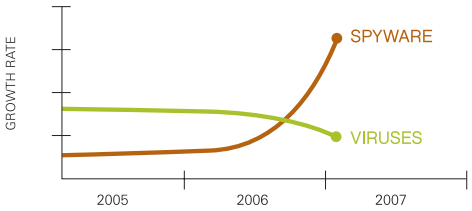


Figure 3 – A 2006 report from ScanSafe indicated that the number of new spyware threats increased by 254% last year while viruses were on the decline.

Similarly, over 70% of respondents reported spyware infections while less than half consider spyware to be a very or extremely serious threat. This is particularly concerning. Spyware purveyors are constantly releasing new programs designed to defy detection, resist removal and morph frequently. Unlike viruses, spyware is financially motivated which provides incentive and funds to drive rapid technological innovation and broad distribution.

Budget and Resource Constraints

SMBs, particularly those with 200 to 5,000 employees, are large enough to attract attention as a target for cyber criminals, yet they may lack the same technical expertise about Internet security issues that is typically found in larger firms.

In March 2007, the National Federation of Independent Businesses (NFIB) and Visa® USA announced the results of a survey of companies with fewer than 250 employees which found:

- 61% have never sought information about how to properly handle and store customer information
- 57% did not see securing customer data as something that requires formal planning
- 52% keep at least one type of sensitive customer information
- 39% rely on "common sense" to keep data safe

SMBs have far fewer information technology (IT) staff to support their computer and network needs. In the Webroot SMB Survey, 63.5% of the respondent companies have fewer than 10 people in their IT departments to staff all their IT needs – desktop, software and server support – as well as to handle Internet security matters.

These organizations are likely to have remote offices and/or remote workers without any on-site or dedicated IT support or management. Even SMBs with larger, mature IT organizations, often lack a dedicated or centralized security team.

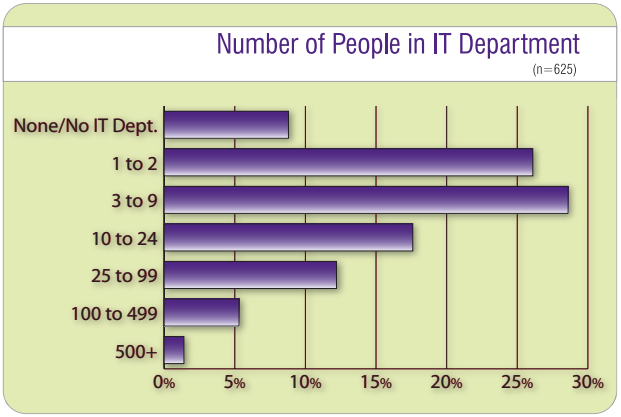


Figure 4 – Source: Webroot Software, SMB Survey, 2007

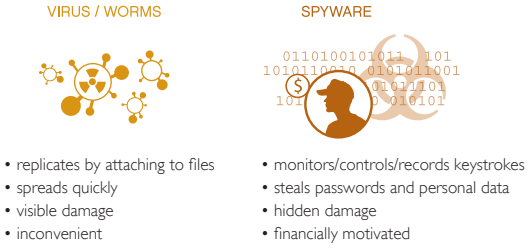
What are the Risks?

Many large corporations have significantly strengthened their network security infrastructure. Like all criminals, spyware purveyors will concentrate on the easiest marks, making SMBs prime targets.

- There are many more SMBs than large companies in the world.
- Most all SMBs hold sensitive personal information about their employees and customers.
- Yet, SMBs often lack the financial and human resources available at larger companies to combat spyware.

Online criminals use sophisticated tools to find unprotected and vulnerable networks and computers. In addition, many of today's online threats are much more difficult to detect and remove unless specialized antispyware software has been installed and configured properly.

In contrast to viruses, that typically make their presence known by spreading across many systems simultaneously and seriously impacting machine functionality, the success of spyware programs depends on their stealth nature. Given the significant financial incentives to stealing sensitive data or serving nuisance advertising, spyware program writers are adept at covertly infiltrating a system and installing programs deep within a computer or network.



In the Webroot survey, the majority of SMBs surveyed indicated spam, spyware, adware and/or virus infection during the past year. Of these, spyware and viruses most threaten to result in the taking or destruction of sensitive information. These infections can have numerous negative business effects including:

- Loss of sensitive information
- Slowed system performance
- Employee downtime
- Costly computer repairs
- Legal fees if there is a data breach lawsuit
- Brand/reputation damage
- Company closure

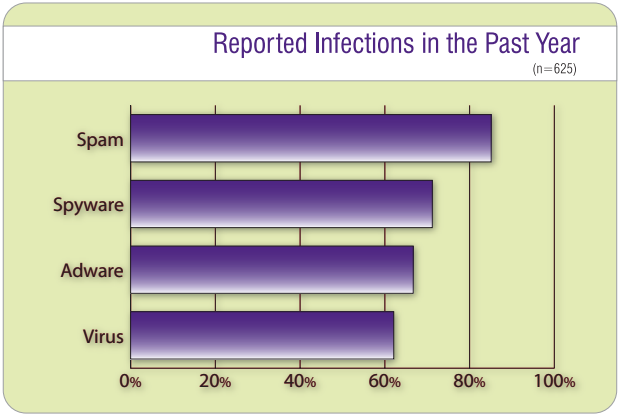


Figure 5 – Source: Webroot Software, SMB Survey, 2007

SMBs that have experienced infections over the past year, shared information about the impacts of those infections on their business.

Impact of Infections in the Past Year *(n=625)*

Type of Issue	A lot / A great deal		Some / A Little		Not at all / Don't Know	
	Spyware	Viruses	Spyware	Viruses	Spyware	Viruses
Slowed System Performance	**36.6%**	**27.6%**	48.1%	47.2%	15.4%	25.3%
Drained IT resources or increased help desk time to repair spyware damage	**24.9%**	**21.5%**	52.4%	49.1%	22.7%	29.5%
Reduced employee productivity	**24.6%**	**19.9%**	55.3%	50.7%	20.0%	29.4%
Disrupted business activities	**23.4%**	**18.6%**	49.7%	48.4%	26.8%	33.2%
Threatened sensitive online transactions	**14.5%**	**13.8%**	36.1%	32.6%	49.3%	53.6%
Compromised confidential information	**12.9%**	**14.2%**	37.2%	32.0%	49.8%	53.7%
Caused loss of sales	**9.8%**	**10.7%**	30.1%	29.3%	60.2%	60.0%

Figure 6 – Source: Webroot Software, SMB Survey, 2007

How to Protect Your Company

For the many SMBs that accept credit card payments, there is strong guidance about best practices provided by the Payment Card Industry (PCI) Data Security Standard. These same guidelines are equally important for all SMBs, even those that do not process credit card payments.

The PCI standard states that companies should:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The PCI standard provides details about how to best fulfill each of these objectives. Specific elements of the standard, such as ensuring that antivirus programs can protect against other forms of malicious code such as spyware and adware, are important guidance for all companies, even those that do not accept credit cards as a form of payment.

Central to effectively protecting SMBs are the technological tools to defend against malware and hackers. SMBs need technical tools that provide:

- Seamless, scalable deployments
- Centralized, customizable user management, including coverage for laptops and remote employees
- Assure accurate threat detection that minimizes false positives
- Delivers comprehensive removal in real-time
- Advances in technology to provide proactive defenses

Tips for Protection

Webroot is a founding member of the Anti-Spyware Coalition which assembled these tips for protecting networks and mitigating spyware in organizations. Additional information about the Anti-Spyware Coalition can be found at www.antispywarecoalition.org

Protect Company PCs from Spyware

- Maintain up-to-date detection patterns and software updates.
- Select desktop security software that can be centrally deployed and managed.
- Maintain current operating system and browser patches to minimize vulnerability to security exploits.
- Ensure web browsers are set to at least "medium" in the security and privacy settings.
- Do not allow users to surf the Internet while logged on with "administrator" privileges to the network.
- Maintain a list of allowable software and/or executable files and run a weekly scheduled check against PCs in the network. Check results for non-standard entries and take appropriate actions to remove unapproved programs.
- Consider re-imaging chronically spyware-infected PCs.

Block Spyware at the Gateway

- Configure gateway proxies and firewalls to prevent:
    - "drive by" downloads (non-approved CAB and OCX files).
    - executable downloads from known spyware sites (identified by content filtering lists).
    - executable downloads from suspected/high-risk sites (sites in categories with high incidents of spyware)
    - PC communication to known spyware "phone home" sites and report which PCs are likely infected with spyware.
- Scan files at the gateway for known spyware code.
- Maintain strong anti-spam protection.

Educate Employees and Other Network Users

- Require network users to agree to an Acceptable Use Policy indicating unauthorized programs can be blocked.
- Teach employees and other computer users to understand that many "free" programs and services on the Internet install spyware that drastically slows PCs, installs annoying pop ups, and steals private and corporate information.
- Ensure IT support staff is trained to recognize the less overt spyware symptoms, including very long boot up, slow and erratic application performance and frequent computer crashes so that proper remediation can be taken.

Finding the Best Solution

Freeware is Not Really Free

Freeware is a software program that can be downloaded free of charge. While this approach may be tempting to SMBs with tight budgets, the adage, "you get what you pay for" comes to mind. Typically organizations offering freeware rely on voluntary contributions to create and update their software. These programs lack robust functionality, centralized management capabilities and daily updates – all critical to ensuring an effective level of protection.

There may also be legal implications for companies relying on freeware. Many of these solutions are intended for individual consumer desktops, and are not intended for deployment on multiple company computers. Often the user agreements reveal that using the software in a corporate environment does require a licensing fee.

Firewalls are Only Part of the Solution

While gateway protection in the form of firewalls can help to block certain kinds of malicious code, they leave a very significant vulnerability. Spyware is typically embedded in legitimate traffic, such as email or on web sites with other valid purposes. Further, once installed on a system most spyware programs disguise themselves as trusted programs, allowing them to communicate freely with the Internet over ports that are often left unprotected by firewalls.

Spyware and other malicious programs can infect a computer from a range of entry points including Internet-based applications, peer-to-peer sharing channels and removable media. Regardless of how it arrives, spyware must execute on the desktop or laptop to infect the computer. Thus, to detect, block and remove spyware and prevent damage to the network and other computers in the company, there should be antispyware software on every desktop that is part of an overall, centrally-managed solution.

One Size Does Not Fit All

Security software programs that claim to do it all for all kinds of companies can not deliver the specialized expertise needed to address the most serious threats. Spyware in particular is uniquely developed to bury itself in a computer file structure, making it both hard to detect and even harder to remove without causing other damage to the computer. Extensive experience and dedicated research teams are critical to the development of the most effective solution.

Select a Specially Designed Product to Address the Problem

To ensure that SMBs are fully protected, their Internet security solution should include an antispyware program that provides:

Regular definition updates – Many free antispyware software downloads do not provide adequate protection against spyware programs because they are not supported by ongoing threat updates. This leaves PCs open to attack from newly evolved or introduced malicious spyware programs. Regular updates to your threat database protects you from newly introduced or changed applications, as well as the latest worms and its family of variants.

Refined spyware detection – Some antispyware software scans yield false positives giving the appearance that they are detecting more traces of spyware than they truly are. Truly useful and beneficial antispyware software only finds and removes true spyware.

Proactive protection – Detection and removal of spyware programs is only half of the antispyware software solution. It's equally important to stop spyware programs before they reach your computer. Proactive protection prevents spies from installing and defends system and browser elements while simultaneously guarding your information and privacy.

Designated threat research team – Often, it's not financially possible for companies that offer free antispyware software to house a team of dedicated threat researchers. Updates may be erratic, poorly programmed or non-existent. A threat research team knows what to look for, and how to most effectively find and remove spyware from a user's PC.

Customer service – Most free antispyware software is not backed by expert customer support, e-mail support or online help sections. Dependable companies not only provide software that removes spyware, they also offer customer support resources to help users with any spyware-related issues they encounter.

Easy-to-use interface – It takes several versions to determine the best and most user-friendly interface. Like research teams, interface improvement is not always an area of focus for providers of free antispyware software.

Stable company to back up the software – It's important to identify credible anti-spyware software that is backed by an established company so you have recourse if you encounter a problem with your purchase or software functionality.

Glossary

Adware

Adware is advertising-supported software that displays pop-up advertisements. Adware is usually available via free downloads from the Internet. Adware is often bundled with or embedded within freeware, utilitarian programs like filesharing applications, search utilities, information-providing programs (such as clocks, messengers, alerts, weather, and so on), and software such as screensavers, cartoon cursors, backgrounds, sounds, etc. Although seemingly harmless, some adware programs may track your Web surfing habits. Deleting adware may result in the deletion of the bundled freeware application.

Antispyware software

Antispyware software protects a PC from spyware infection. Spyware protection software will find and remove spyware without system interruption.

Botnet

A botnet is a collection of computers running remote control software programs and under a common command and control infrastructure via a public or private network. Botnets can be used for sending spam remotely, installing more spyware without consent, and other illicit purposes.

Browser Hijackers

Sometimes called Home Page Hijackers, browser hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, browser hijackers may redirect your searches to "pay-per-search" Web sites.

Cookie (or Adware Cookie)

Cookies are pieces of information that are generated by a Web server and stored on your computer for future access. Cookies were originally implemented to allow you to customize your Web experience. However, some Web sites now issue adware cookies, which allow multiple Web sites to store and access cookies that may contain personal information (surfing habits, usernames and passwords, areas of interest, etc.), and then simultaneously share the information with other Web sites. Adware cookies are installed and accessed without your knowledge or consent, and in some cases this sharing of information allows marketing firms to create a user profile based on your personal information and sell it to other firms.

Dialer

Dialers have the ability to disconnect your computer from your local Internet provider and reconnect you to the Internet using an expensive pornographic, toll, or international phone number. They do not spy on you, but they have the ability to run in the background, hiding their presence. Dialers may rack up significant long distance phone charges.

Distributed Denial-of-Service (DDoS) Attack

A means of burdening or effectively shutting down a system by bombarding it with an overwhelming amount of traffic. DDoS attacks are often launched using botnets. A vulnerability in one computer system can be exploited to make it the DDoS master.

Drive-by download

When programs are downloaded without the user's knowledge or consent. Most often accomplished when the user clicks to close or eliminate a random advertisement or other dialogue box.

Encryption

Encryption is the scrambling of data so it becomes difficult to unscramble and interpret.

Exploit/Security Exploit

A piece of software that takes advantage of a hole or vulnerability in a user's system to gain unauthorized access to the system.

Firewall

A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules. Firewalls provide effective protection against worm infection, but not against spyware like Trojans, which hide in legitimate applications, then install secretly on a user's PC when the application is launched.

Hijackers (Home Page Hijacker or Browser Hijacker)

Hijackers have the ability to change your default home page as well as other Web browser settings. Common behavior also includes adding advertising, pornographic, or other unwanted bookmarks, creating pop-up advertisements, and redirecting mistyped or incomplete URLs. Additionally, home page hijackers may redirect your searches to "pay-per-search" Web sites.

Information Privacy

The interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

Host File

The host file stores the Internet Protocol address of a device connected to a computer network. Some spyware can change a host file in order to redirect users from a site that they want to visit to sites that the spyware company wants them to visit.

Keylogger

A keylogger is a type of system monitor that has the ability to record all keystrokes on your computer. Therefore, a keylogger can record and log your e-mail conversations, chat room conversations, instant messages, and any other typed material. They have the ability to run in the background, hiding their presence. In some cases, a third party may be able to obtain private information such as usernames, passwords, credit card numbers or Social Security numbers.

Operating System

The operating system is usually the underlying software that enables you to interact with the computer. The operating system controls the computer storage, communications and task management functions. Examples of common operating stems include: MS-DOS, Macintosh, Linux, Windows. Also: OS, DOS.

Personally Identifiable Information (PII)

Information such as name, address, phone number, credit card information, bank account information, or social security number.

Privacy

A privacy policy outlines the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary.

Privacy Policy

A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules. Firewalls provide effective protection against worm infection, but not against spyware like Trojans, which hide in legitimate applications, then install secretly on a user's PC when the application is launched.

Registry

A computer registry is a database integrated into certain operating systems which stores information, including user preferences, settings and license information, about hardware and software installed on a user's computer. Spyware often changes registry values in order to take control of parts of the system. These changes can impair the regular function of the computer.

"Remove Me"

Remove me is an option often included in spam which is fake. That is, if you respond to request removal, you very well may be subjecting yourself to more spam, because by responding, the sender knows that your email account is active. A 2002 study performed by the FTC demonstrated that in 63% of the cases where a spam offered a "remove me" option, responding either did nothing or resulted in more email.

Rootkit

A rootkit is a program that fraudulently gains or maintains administrator level access that may also execute in a manner that prevents detection. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection. Rootkit commands replace original system command to run malicious commands chosen by the attacker and to hide the presence of the Rootkit on the system by modifying the results returned by suppressing all evidence of the presence of the Rootkit.

Shareware

Software distributed for evaluation without cost, but that requires payment to the author for full rights is commonly called shareware. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is pirating.

Spam

Spam is the common name for unsolicited commercial email. It is sent, usually in bulk, through "open-relays" to millions of persons. Spam is cost-shifted advertising. It takes a toll on Internet users' time, their resources, and the resources of Internet Service Providers (ISP). Most recently, spammers have begun to send advertisements via text message to cell phones.

Spyware

Spyware is any application that makes potentially unwanted changes to your computer while collecting information about your computer activities. This information may then be sent to a third party for malicious purposes, without your knowledge or consent. Spyware can be distributed by bundling with freeware or shareware, through e-mail or instant messenger, as an ActiveX® installation, or by someone with access to your computer. Unlike traditional personalization or session cookies, spyware is difficult to detect, and difficult (if not impossible) for the average user to remove without the use of an effective anti-spyware program.

System Monitor

System monitors have the ability to monitor all computer activity. They range in capabilities and may record some or all of the following: keystrokes, e-mails, chat room conversations, instant messages, Web sites visited, programs run, time spent, and even usernames and passwords. The information is gathered via remote access or sent by e-mail, and may then be stored for later retrieval. In some cases, a third party may be able to gain access to private information such as usernames, passwords, credit card numbers or Social Security numbers.

Trojan Horse (also known as Trojan or Backdoor Trojan)

A Trojan horse is a program that allows a hacker to make changes to a computer without the user's knowledge. Unlike a virus, a Trojan does not replicate itself. It is generally disguised as a harmless software program and distributed as an e-mail attachment. Once you open the attachment, the Trojan may install itself on your computer without your knowledge or consent. It has the ability to manage computer files, including creating, deleting, renaming, viewing, or transferring files to or from the computer. It may utilize a program manager that allows a hacker to install, execute, open, or close software programs. The hacker may have the ability to open and close your CD-ROM drive, gain control of your cursor and keyboard, and may even send spam by sending mass e-mails from your infected computer. Trojans have the ability to run in the background, hiding their presence.

Virus

A program or code that replicates, that is infects another program, boot sector, partition sector or document that supports macros by inserting itself or attaching itself to that medium. Most viruses just replicate, many also do damage.

Worm

A program that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. The name is an acronym for "write once, read many."

Zombie

A zombie machine is one that has been taken over using remote control software. Zombies are often used to send spam or to attack remote servers with an overwhelming amount of traffic (a Distributed Denial of Service Attack). A collection of many zombies comprise a botnet.

Appendix: Symptoms of a Spyware Infection

Some common visible symptoms of a spyware infection include:

- A barrage of unsolicited pop-up ads
- Browser hijacking so that the website that appears is not the one types in the address bar
- Sudden or repeated changes to the computer's Internet homepage not made by the user
- New, unexpected or unrequested toolbars
- New, unexpected or unknown icons appearing on the desktop or in the tray at the bottom of the screen
- Problems with keys malfunctioning or not working at all
- Random error messages
- Performance degradation with long delays in opening programs or saving files
- Anti-spyware or anti-virus software is turned off, or malfunctioning
- Unidentified toll charges on your phone bill

It is important to note that often the most dangerous forms of spyware will not display any visible signs, as they are designed to be stealth and remain on the computer unnoticed by the user.

About Webroot Software

Webroot Software, Inc. provides industry leading security software for consumers, enterprises and small and medium-sized businesses worldwide. Webroot security software consistently receives top ratings by respected third–party media and has been adopted by millions globally.

Webroot Antispyware Corporate Edition (formerly Spy Sweeper® Enterprise) is a comprehensive, centrally managed enterprise solution that aggressively blocks, detects and eradicates spyware on desktops across the network. Webroot Antispyware Corporate Edition with Antivirus offers combined protection for spyware and viruses. Webroot products can be found at www.webroot.com and on the shelves of leading retailers worldwide.

To find out more visit www.webroot.com or call 800.870.8102.

2560 55th Street • Boulder, CO 80301 • USA
Telephone: 800.870.8102 • Fax: 303.476.2222
www.webroot.com