SPYWARE

Though our computers have become an aspect of our everyday lives at work and home, our computers are not safe in the world of the Internet when spyware is used to find out about YOU!

Removal Tricks & Advice to Keeping your Computer Safe

Spyware Removal Tricks and Advice

Contents

Chapter 1

What is Spyware?

It is normal to see pop-up ads while surfing the net, right? What a lot of people don't realize is that those ads could have made their way onto their computers through spyware. By the time that you figure out what is behind the ads, the spyware pop-ups may have gotten so bad that your only choice is to completely reconfigure your computer and just hope that the pop-ups don't come back. And, if your only mechanism to fight against the spyware is hope, the pop-up ads *will* return.

What is Spyware Exactly?

Spyware is a type of software which gets onto your computer and is generally used to gather your personal information and then send advertisements to you, normally in the form of a pop-up ad. Spyware software can also change your computer configuration as well as many other potentially harmful things. Even though the term spyware may suggest that the software is simply monitoring action in a secretive way, the purpose of spyware usually goes well beyond this. The party responsible for creating and distributing the spyware are often profiting greatly through targeted advertising or selling off your personal information.

When spyware software is on a computer, it generally is hidden from the user. In 2005, a study carried out by AOL and the National Cyber-Security Alliance showed that 61% of user's computers were infected with spyware. Of all of these users, 92% of them were not aware that their computers were even infected. 91% of the users claimed that they had not granted permission for the spyware software to be installed. Since then, spyware has become increasingly sophisticated and is often impossible to detect on a user's computer. Even worse, once detected, some spyware is impossible to remove.

Difference between Spyware and Adware

The terms spyware and adware are often used interchangeably. Both of these terms are used to describe software which can display advertisements. However, there is one major difference between these two: spyware gets onto the user's computer through illicit means.

With adware, the user agrees to have the adware program installed in exchange for something else. For example, the program Eudora will allow users access to shareware for free but they must agree to receive advertisements. The key word here is “agree.” Adware will not attempt to mislead users and is offered in exchange for a service.

An example of adware includes the file sharing program Eudora. Rather than asking users to pay a registration fee, it asks them to agree to receive advertisements. On the other hand, Gator software is a type of spyware. When users visit certain websites, spyware is installed on the users’ computer through some sort of deceptive manner. The company behind Gator as well as the website where the spyware was installed will both receive revenue.

Chapter 2

How is Spyware different from Viruses &Worms?

Today, there are an incalculable number of “health” problems that a computer can be at risk for. Generally, these risks can be broken down into spyware, viruses and worms. It is easy to confuse these different types of computer problems because they have many similarities.

Spyware, viruses and worms all get onto a user’s computer with permission or by using deceptive means. Once on the computer, they cause harm to the computer and impair functions. Spyware, viruses and worms are all designed to be difficult, if not impossible, to detect. They often are designed in a certain way that prohibits them from being removed in normal manners. Recently, there have been many viruses and worms which have been, as spyware is, created for profit.

Compared to viruses and worms, spyware is a relatively new problem. Viruses have been around since the 1980s and worms almost as long. Spyware didn’t become a major issue until 2000.

The major difference between spyware and viruses and worms is that spyware doesn’t seek to replicate once on your computer. It also doesn’t seek to infect other computers. Both viruses and worms, on the other hand, actively replicate themselves and can spread to other computers through means such as email.

Another big difference between spyware, viruses and worms is objective. Spyware is always used for some form of monetary gain such as through advertisements. Modern viruses and worms can also be used for monetary gain. However, viruses and worms are often created in an attempt to gain fame.

Some virus and worm creators have claimed their motivation was to show how far virus creation has advanced. Other creators desire to "outdo" the creators of anti-virus and anti-worm software. As in the case with the Bagel and Netsky viruses, the creators of the viruses wanted to outdo each other.

Additionally, viruses and worms are often created specifically to do damage to a computer through a type of web espionage. An example of this is the Conflicker worm which spread in 2008. It made its way into the defense systems of France and Britain as well as about 15 million computers around the world and creating severe damage to the computers' health. Spyware, however, does not want to cause severe damage to the computer. That is because it relies on the computer's health in order to send advertisements to users.

Is there a Spy-Vir-Orm Hybrid?

It is getting increasingly difficult to distinguish between spyware, viruses and worms. As all three of these computer health issues become increasingly sophisticated, they have taken on properties of one another and often rely upon one another for functioning.

There are many instances when spyware is spread through a virus or visa versa. There are also many instances of spyware, worms or viruses creating openings for other types of harm to enter a user's computer. Because of this crossover between the spyware, viruses and worms, it is important that countermeasures are taken against all forms of computer infections.

Chapter 3

Can I Just Ignore Spyware?

Because spyware doesn't progressively destroy a computer's functioning like viruses and worms do, it may be possible to simply ignore the fact that your computer is

infected. Many people figure that it is better to simply keep closing all those annoying pop-up ads rather than bother with antispyware software, some of which can be very expensive. Ignoring the fact you have spyware is a temporary solution but it can end up costing you in the long run.

Much of the spyware software now will disable firewalls, disable anti-virus software, and change browser security settings to low. This allows for further infection of your computer by other spyware software or viruses and worms. At first, you may just have a few pop-up ads. Later, this may progress to the point where the pop-ups come faster than you can click to close them or your computer is getting destroyed by a cocktail of viruses as though your computer has an immune deficiency disease.

Spyware software makers were aware that this change in security settings would allow other spyware to get into the computer. Because spyware companies are in competition against each other, some spyware actually destroys other spyware which is on your computer. This also keeps users from taking action against spyware because the problem never seemingly gets too bad. The spyware maker Avenue Media actually sued one of its competitors called Direct Revenue because the company disabled its spyware. The two companies settled the dispute by agreeing not to disable each other's products.

Aside from the lowered security settings that many spyware programs create, you may have gotten a virus or worm with your spyware in a bundled package. This cocktail of computer infections can do serious and even irreversible damage. Even if you don't have an additional problem other than spyware, you can never be sure exactly what the spyware is doing and what information of yours it is accessing – such as your credit card numbers.

By ignoring the threat of spyware, you are setting up your computer for a potential disaster. Antispyware programs can be very expensive however, if you take the time to educate yourself, there are plenty of free antispyware programs. Even if you opt for the paid versions, it is better to spend that money now than to pay to have your computer completely reconfigured in the future after the spyware problem gets out of control.

Chapter 4

What Damage Can Spyware Do?

Bombards You with Advertisements

Spyware is known for displaying advertisements, usually in the form of pop-ups. Each spyware software program works a bit differently with its advertising. Some display ads every couple of minutes, for example, while others will display every time you open a new browser window. The newest trend amongst spyware is to track what the user is doing online. Then, this information is relayed so specific, targeted ads are displayed. For people vulnerable to advertising, these targeted ads can be a great threat.

These pop-up ads can be a great nuisance. Also, pornography pop-up ads are a very common issue with spyware and they are considered particularly heinous because children could be exposed to the porn ads.

Another way in which spyware may advertise is to take over the banner ads. Instead of seeing the advertisement which the site's creator put up, the viewer sees a spyware ad instead. Because many websites are funded by ads, the spyware is stealing profit from the website owner as well as annoying the viewer with the banner ad.

Slower Computer

When a computer is infected with spyware, it must process the spyware applications. All of the tasks that spyware can do from displaying pop-up ads to tracking users are very demanding on a computer's system. This results in the computer going slower and sometimes drastically slower. If the spyware problem gets out of hand, it is possible for the computer to crash because it can't handle all of the applications that are being requested from it.

Identity Theft and Fraud

True to its name, there are new versions of spyware which can literally spy on the user. The spyware will take pictures of the websites that a user visits and then relay the pictures back to the spyware source. Since website pages can contain banking information and other personal information, spyware can lead to identity theft. These types of spyware are rare but they still exist.

With dial-up internet access, there is also the risk of wire fraud. This occurs when spyware resets a modem to dial up numbers at a premium rate rather than the usually number for the ISP. This results in large phone bills for the user.

Changing Settings

One of the common things that spyware does is to change a computer's configurations. Generally, the web browser homepage will be changed along with the search engine. Spyware can also change security levels and even prevent a user from installing or running antivirus or antispyware programs. Once these changes have been made by the spyware, it is usually very difficult to get the settings back to normal.

Stealware

For affiliates selling products online, spyware can pose risk for a different type of fraud. When a sale is made through an affiliate, the spyware will fill in the affiliate's tag with the tag of the spyware operator. Instead of the legitimate affiliate getting paid for the sale, the spyware operate benefits instead. In this case, only the spyware operate is benefiting from the illicit software. The New York Times dubbed this type of affiliate fraud "stealware."

Virtual Spying

Spyware has been used to virtually spy on people in several cases. In some cases, spyware was put onto a computer so that the activity of the user could be monitored. The software Loverspy is an example of this type of spyware which was marketed towards people suspecting that their spouse/partner was infidel. There are also instances when spyware was used to turn on webcams so the spyware operator could spy on the user. Depending on the areas where it is used, this type of spyware monitoring may be illegal, even if used by a spouse.

Chapter 5

How does Spyware Get onto Your Computer?

You Install It

In most cases, spyware gets onto your computer because you have installed it unknowingly. This is how it works: when you find some sort of free program or file online, you download it and it comes bundled together with spyware. This is also the case with shareware. For spyware creators like Claria, which is the largest spyware company, this method of spyware transmission is very profitable. Claria had revenues of $35 million just last year.

Spyware as a profitable business really began to surge when free internet applications became available online. Since applications such as Web browser, email, and instant messaging were free, it didn't take long before users *expected* free software as well. Software makers were having a hard time selling software for even low prices and they had trouble battling against illegal file sharing as well. Instead of trying to increase sales, the software makers decided to offer free software but include spyware bundled with it.

A spyware company will pay a software company for every time the software is installed. Then, the spyware uses targeted ads on the user. When a user clicks on the ad or makes a purchase through the ad, the spyware company profits.

An example of this is the free file sharing application Kazaa which comes bundled with spyware from the company Claria. Kazaa gets paid by Claria every time its program is installed. Then, the Claria spyware creates targeted pop-up ads for users and profits each time one of those ads is clicked on. If you visit the Dish Network homepage, a pop-up ad for DirecTV will appear.

This method of spyware distribution occurs with all sorts of free downloads including software and file sharing. Often, the terms and conditions for downloading a free application will mention that spyware is included with the download. However, not many people take the time to read through the terms and conditions. It is also common for the information about spyware to be deceptively hidden in a very long and confusing terms and conditions statement. The downloader simply clicks "Accept" and gets the spyware.

Fake Windows Security Boxes

To start downloading spyware, sometimes all it takes is a click of a link. One of the most common ways that spyware makers get users to click on their links is by disguising them as Windows security boxes.

The boxes look just like a normal Windows security box. However, when you click on them, the link causes your security settings to change and spyware to be installed on your computer without your knowledge. For example, a box might read, “Optimize your internet access.” Even if you hit the “No” button, you will still trigger the spyware.

Security Holes

If you do not have high security on your computer, you run the risk of spyware finding its way inside. Some of the newer spyware programs have even learned to find their way through holes in firewall and antispyware software. Spyware is often distributed with a virus. First, a virus is sent to a computer. Instead of replicating and possibly destroying a computer’s system like a normal virus, its job is instead to create a hole for the spyware to enter.

There are several other illicit ways in which spyware can enter a computer. For example, there are spyware programs which are spread through emails. Even if the email gets tagged as potentially dangerous and the user doesn’t read it, the spyware can still be spread just by having it displayed in a preview pane.

Chapter 6

How to Prevent Spyware

Because there are so many different ways for spyware to enter a computer, it is almost impossible to avoid infection. Avoiding certain activities, such as downloading, can reduce the risk but there are still many ways for spyware to enter. That is why preventative and real-time counteractive measures need to be taken.

The first step to preventing spyware infections (and re-infections after spyware is removed) is to educate yourself. By understanding why spyware exists, you can start to identify possible threats while you are online. So, if you skipped the first five chapters of this eBook, now would be a good time to go back and read them before continuing on.

Research Before You Download

Even though downloading any sort of free file or software is one of the biggest risks when it comes to getting spyware or other computer infections, most people are not

going to stop downloading. There are simply too many desirable free programs and files out there. However, you can greatly reduce the risk of an infection by researching the freebie first.

Whenever downloading free software, type its name into a reputable search engine along with the word spyware. Chances are, if that program comes bundled with spyware, you won't be the first to get it. If you type in "Kazaa spyware" into Google, for example, the first several pages of results all mention the infamous spyware as well as how to remove it.

Change Your Settings

Some of the preventative steps against spyware are very simple to take. For example, you can use Mozilla Firefox instead of Microsoft's browsers which have several security holes which are easy for spyware programs to enter through. Also, switching to a Mac or Linux operating system will greatly reduce your risk of various computer infections because most are targeted at Windows. However, this is not such an easy change to make.

If working on Windows Explorer, you will want to install Windows XP Service Pack 2. This service pack solves many of the security holes in Internet Explorer and it also has a built-in pop-up blocker. There are also features like the add-on manager which will allow you monitor which programs are running with Internet Explorer. You can download Windows XP Service Pack 2 here:
http://www.microsoft.com/windowsxp/sp2/default.mspx

You will also want to change your Security Zone settings on Internet Explorer to block harmful sites. The settings have the options of listing sites as Trusted, Restricted, Local Internet, or Internet. If you list a site as restricted, you are still able to visit that site but the security settings will prevent the site from harming your computer. Some antispyware tools like Spyware Blaster and Spybot Search and Destroy will add automatically add harmful sites to the restricted setting.

If your computer internet is connected to a dial-up modem, you will want to unplug the modem when you aren't using it. This will prevent spyware from committing dial fraud by calling premium numbers.

Chapter 7

What is Antispyware & How Does it Work?

There are a few different types of antispyware software. The most common type will run a scan of your computer and determine if there are any spyware programs there. You can usually choose how often the scan will be done such as on a daily or weekly basis. Generally, these are the areas which get checked in a spyware scan:

- Window's registry
- Operating system files
- Files which have been installed through programs

Some antispyware scanning software will allow you to do "smart scans" where only the computer files which are commonly infected with spyware will be scanned. This type of scan is much faster than a full scan though it is not as accurate.

If spyware software is detected on your computer, there are antispyware software programs which will attempt to delete them. There are also antispyware software programs which will work in real time to block any attempts to infect your computer as they happen.

The real time antispyware blockers work in a few different ways. Some of them have mass lists of known spyware software which they will automatically block. Others will locate any suspicious program which is attempting to download on your computer. The antispyware blocker will not automatically block the download. Rather, it will send the user an alert. Then the user can make a choice as to whether to allow or deny the download.

There is also antispyware software which will intercept programs that attempt to install startup items or change browser settings. The best antispyware protection comes from having all three of these elements: detection through scanning, spyware removal, and real time protection.

Many computer security software programs contain antispyware programs. However, do not assume that they do. It is important that you are getting full coverage against spyware and many of the computer security software programs only fight against viruses and worms.

Chapter 8

Can I Use "All-Around" Computer Security Software?

When a virus enters a computer, it can do a lot of damage, especially in terms of overall health. Once the "immune system" of a computer has been harmed by a virus, it becomes much easier for other forms of malware to enter the system. Some viruses are even specifically designed to penetrate a computer's security simply to make a hole for spyware to enter. Because of these factors, it is important that your computer also have antivirus in addition to antispyware software.

Many people have the mistaken belief that their antivirus or computer security software contains antispyware software as well. However, this is often not the case. Many antivirus makers are reluctant to include antispyware at all. That is because they worry that their antispyware could block a legitimate software or advertising program and then they would be subject to a lawsuit.

Even when antispyware is included with an antivirus, it is generally not enough protection. An article from Wired magazine from June 25th, 2004 explored this problem. A test was performed by purposely attempting to infect a computer with spyware while running antivirus software which also had antispyware capabilities:

> "All the antivirus programs popped up a warning when they detected an attempt to install spyware. In most cases, all the antivirus programs successfully deleted the spyware they spotted after it was installed, but none could fully repair the damage -- they were unable to remove toolbars installed by some of the spyware, or restore registry settings.
>
> In some cases, with more virulent pieces of spyware, Symantec, McAfee and Trend Micro's antivirus applications were unable to fully purge the software from the infected machine. Although the system was reported as clean, the spyware reactivated after a reboot."

Because the awareness and risks of spyware have increased since the Wired article, there have been some major improvements in the development of all-around computer protection. However, it is still best to have separate antivirus software to accompany your antispyware software.

Chapter 9

Free Antispyware Software

One of the reasons that spyware is spread so quickly is because of all the free downloads which have spyware software bundled in with them. Obviously, many people are not willing to pay for software- especially antispyware software. Luckily, there is now a lot of free antispyware software available.

One of the ways to get free antispyware software is simply to download it from the internet. However, it is very common that the free antispyware software actually comes with spyware bundled in with it. You can read the next chapter to find out about this risk. Here is a list of some of the best antispyware software programs available for free online.

Free Spyware Protection

- **Windows Defender:** Before any software can be installed, it has to pass a Windows Genuine Advantage test. This antispyware software works in real time. It takes up little running space and can be put on a schedule for scanning a computer system. However, it is not the best choice of software for stopping all spyware.
- **Spybot Search & Destroy:** This is one of the most well-known antispyware software programs. It has been around since 2000 and is regularly updated. It has an immunization feature which will add malicious sites to your Restricted Sites list to protect you in case your computer is hijacked and taken to a harmful site.
- **Ad-Aware:** Ad-Aware is another one of the most popular free antispyware software. It can be downloaded for free. However, there is also a commercial version of Ad-Aware which offers even higher levels of protection. It also includes antivirus.
- **AVG Anti-Spyware Free Edition:** AVG is popular became popular as antivirus software and now has created antispyware software as well. There is a commercial and a free version available. AVG is one of strongest in terms of overall computer protection. However, like all free antispyware software, it does not contain a built-in firewall.

- **Avast! antivirus Home Edition:** This software is a combination of antivirus, antispyware and anti-rootkit. It is made for Windows and is free for home use.
- **Panda Cloud Antivirus:** This program also includes antispyware
- **Microsoft Malicious Software Removal Tool:** Called MSRT for shot, this software is available for free so long as your Windows is genuine. There are free monthly updates of MSRT available for users on the first Tuesday of each month.
- **Comodo Internet Security:** The Comodo company makes several software programs including antispyware, antivirus, and a firewall. You can download each of these separately for maximum protection. There is also a paid version called Comodo Internet Security Pro. Comodo is one of the strongest when it comes to battling computer infections. However, the software may be a bit difficult for beginners to operate and the free version doesn't have any customer support.
- **Spyware Blaster:** This software does not remove spyware infections. Its goal is to prevent spyware infection and has a list of thousands of malicious sites which can be added to your Restricted Sites list. It also has a feature which will allow you to lock your Internet Explorer homepage so it can't be altered.

Free Spyware Removal Tools

- **SuperAntiSpyware:** If you already have a spyware infection, this software has been reported as effective in removing the spyware.
- **HijackThis:** This freeware utility works a bit differently than most spyware removal tools because it doesn't just perform a simple scan based on a list of spyware. Instead, it scans the computer and looks for all suspicious items. Then, HijackThis will ask the user what to do with those items. Users should be very careful while using HijackThis to not delete any useful or essential items.
- **Removal Restrictions Tool:** Also known as RRT, this tool is used to restore permissions in situations where spyware has locked users from the Control Panel, Task Manager or Regedit.

There are a lot more free antispyware programs available with new ones constantly becoming available. However, it is important to note that many of these are not completely effective in preventing or removing spyware. Usually, they each have a few loopholes which spyware makers are aware of and exploit.

One way to get around the loopholes is to use multiple free antispyware software programs at once. What one program misses will generally be picked up by another

program. The only real downside to this method is that using multiple antispyware programs can make your computer run slower.

Also, it needs to be pointed out that many of the free antispyware which is advertised online is actually rogue antispyware. This software actually contains spyware which will infect your computer.

Chapter 10

Rogue Antispyware Software

You need to be really careful when choosing antispyware to install. There are an increasing number of fake antispyware software programs out there and they all appear legitimate at first.

The way that antispyware usually strikes is with a pop-up window that reads something like, “Your Computer is Infected!” In one scenario, the user would then be guided through a step-by-step process for purchasing the antispyware software and have all of the “alleged” spyware and viruses cleaned. In this situation, the user is tricked out of money and may also have his/her credit card information stolen.

In another scenario, users are tricked into downloading software which is completely free. Instead of getting free antispyware, this software actually contains spyware.

Even though these rogue antispyware software programs look just like legitimate software at first, they are pretty easy to detect.

How to Detect Fake Antispyware

There are many sites out there which give lists of legitimate and rogue antispyware software. While this can be a surefire way to see if a program is legit, this method isn’t recommended for a few reasons. First of all, the amount of legit and fake software is changing all the time. It is hard to know if the list you are looking at is updated or not. Also, you may not know for sure if the list is even legit. Plus, looking at a list means that you have to go through a huge amount of software names. Since many of the fake antispyware software have names which mirror legitimate software, it can be confusing to distinguish the two.

The quickest and easiest way to determine if software is legit or not is by simply typing its name into a reputable search engine. The internet community is generally pretty quick to respond whenever new spyware software hits. The results you get from the search will be fairly simple to interpret.

For example, if you type into Google's search engine "Windows Care Tool," which is rogue internet security software, you get results like this:

> **_Windows Care Tool_ - how to remove**
> 9 Feb 2011 **...** *Windows Care Tool* is a malicious program that was designed for the one big purpose which is to rip users off. As any other representative **...**
> *www.2-viruses.com/remove-**windows-care-tool***
>
> **Remove _Windows Care Tool_ (Uninstall Guide)**
> 9 Feb 2011 **...** This page contains free removal instructions for *Windows Care Tool*. Please use this guide to uninstall *Windows Care Tool* and any associated **...**
> *www.bleepingcomputer.com/virus-removal/remove-**windows-care-tool***
>
> **Remove _Windows Care Tool_, removal instructions**
> *Windows Care Tool* is a rogue anti-spyware program that displays fake security alerts and fake threats. This rogue is installed through the use of.
> *www.2-spyware.com/remove-**windows-care-tool**.html*

Obviously, Windows Care Tool is a rogue antispyware program because the internet would not be flooded with information on how to remove a useful program. Compare these results to the search results for "Spybot Search and Destroy," which is very useful antispyware software:

> **_Spybot Search & Destroy_**
> Searches whole computer or just a certain file for malicious software commonly missed by anti-virus programs. Can be used to clean usage tracks.
> *www.safer-networking.org/* - Cached - Similar
>
> **_Spybot - Search & Destroy_©® - The home of _Spybot_-S&D!**
> *Spybot - Search & Destroy* detects and removes spyware, a relatively new kind **...**
> *www.safer-networking.org/en/**spybot**sd/* - Cached
> Show more results from safer-networking.org
>
> **_Spybot - Search & Destroy_ - Free software downloads and software ...**
> Review by CNET Staff - Nov 7, 2008
> *Spybot - Search & Destroy* has been in the antispyware game for a long time offering features we've come to expect in the best apps in the category, **...**
> *download.cnet.com/**Spybot-Search**...**Destroy**/3000-8022_4-10122137.html* - Cached - Similar

If you are still not sure about whether software is legitimate or rogue, you can seek out the software company's website. All legitimate software should have a website where you can find information about it.

It takes less than 30 seconds to type a software name into a search engine. You shouldn't skip this step because you could end up infected with spyware!

Chapter 11

Choosing Antispyware Software

There are a lot of antispyware software programs out there and all of them offer different levels of security. Before you antispyware software, you should at least take a few minutes to do some research and find out more about the software. You can easily get lists of the "best" antispyware software from blogs and websites. Then, use these lists for further investigation.

Here is what you should be finding out about the antispyware before downloading:

- **Who makes the antispyware:** There are a lot of well-known companies which make antispyware, such as Microsoft. However, this doesn't mean that the big brand names are offering the best products. What is important is that the company has a good reputation for antispyware software. Some of the best companies have been around for a long time. Since they have been dealing with spyware issues for so long, they may be adept at fighting against the threat.
- **Are there any complaints about the company:** Generally, you can easily uncover any complaints about an antispyware company simply by typing its name into a search engine. You may also want to try searching for the company's name followed by "complaints." If there are more negative comments than positive ones, you can be sure that there are major issues with that software program. To really be sure about the company's reputation, you can visit the website for the Better Business Bureau. There, you will find out if there are any unresolved complaints against the company.
- **How are its reviews:** There are countless blogs and other websites which have reviews of antispyware software. Some of these are left by users while others

are by professionals in the field. To make sure that the reviews are accurate, you might want to check out reviews at sites like CNET.com which specialize in tech news. :

Keep in mind that there is no one best antispyware software program. Rather, it matters which antispyware is best suited for your needs. Here are some other factors you should take into consideration:

- How easy is the antispyware to use?
- Does the antispyware come with customer support?
- Will the antispyware slow down your computer?
- Is the antispyware effective in prevention?
- Is there real time prevention?
- How effective is the software in spyware removal?
- Do you need to update and, if so, are updates free?
- What scanning options are there?
- Does the antispyware include antivirus as well?
- How much does the antispyware cost?

Almost all antispyware software today comes with a free trial period. It is highly recommended that you take advantage of this option in order to see how you like the antispyware before you decide to buy it.

Chapter 12

Do You Need to Update Antispyware?

Spyware is constantly becoming more sophisticated. As antispyware makers find ways to prevent the attacks, the spyware makers are finding holes in the systems through which they can send infections. The antispyware which was effective just one year ago will not likely be effective against the newer strains of spyware. Because of this, it is important that you regularly update your antispyware software.

How to Update Antispyware

If you have a paid subscription to an antispyware software program, then you will be able to update during the subscription period. Some companies will give you free updates for life if you buy their antispyware software. In these cases, the software will generally have an alert system which will pop up a warning when you need to upgrade. Or, it may automatically do the update for you depending on what your settings are.

With free antispyware software, you generally have to do the updating manually. That means remembering to periodically visit the site and download the newest version of the antispyware.

Antispyware with No Updating

There are a few antispyware software programs which don't require updating. These ones don't use the typical scanning method for finding spyware threats. Instead, they observe the history of the user's Window registry and browser. These specific parameters are monitored. Whenever anything attempts to change these parameters, the antispyware will alert the user. Then, the user decides what action to take.

While this type of antispyware is beneficial because it doesn't need updating, it has its drawbacks. Instead of offering suggestions about whether a program is harmful, the user must make that decision. This might require more time on the user's part rather than just allowing the antispyware software to make decisions.

Chapter 13

How to Get Rid of Spyware

If you have a spyware infection, then your best bet is to use antispyware software in order to find then remove the malicious software. If you already have antispyware software which didn't detect the attack, then you may need to use a different program in addition to this one.

Even though some antispyware defense systems are great, not one of them is impenetrable. Generally, the best method of preventing and getting rid of spyware is to use at least two antispyware programs. What one program misses will generally be picked up by the other program.

The two free antispyware programs Ad Aware and Spybot Search & Destroy will almost always take care of a spyware problem when used together. For particularly heinous spyware attacks, you may need to use a commercial product. Spy Sweeper and Pest Patrol are both fairly good products.

If you still can't remove the spyware from your computer, then you will have to explore manual removal options.

Chapter 14

Spyware Removal in Safe Mode

If you can't remove a spyware infection with antispyware, then removal in safe mode is generally your next step. When Windows is run in Safe Mode, it is running using a minimal amount of drivers and services as well as isolating the computer from the internet.

The reason that safe mode is effective in spyware removal is because spyware is often hidden in the computer's memory. Antispyware generally focuses on the computer's hard disk rather than the memory. Thus, the spyware modules load while the antispyware attempts to clean it out. While in safe mode, the spyware in the memory won't be able to load and the antispyware will be able to effectively clean it out.

Running Antispyware in Safe Mode

Before you clean your computer in safe mode, you will need to boot your computer normally and download the most recent version of antispyware. If your computer isn't too badly infected to impede its functioning, you may want to download several different versions of antispyware.

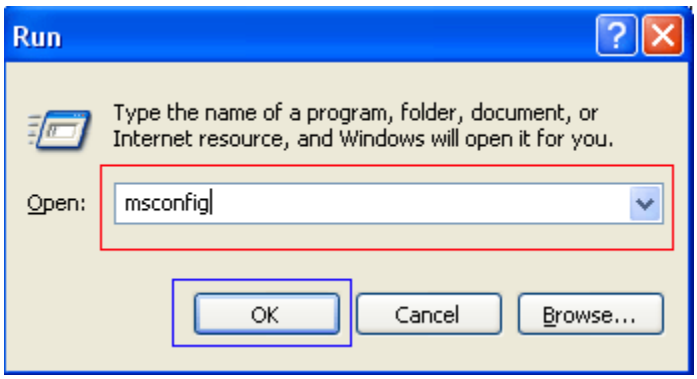
After downloading the latest antispyware software, restart your computer. When the computer starts again, you will first see some information about equipment, hard drives, and so forth. Then, you will see a black screen with a white bar on the bottom which says "Starting Windows." When you see this, repeatedly tap the F8 button until an Advanced Options Menu appears.

Use the arrow keys on your computer to select the Safe Mode option then press enter. The computer will then boot in safe mode. Once in safe mode, you can run your antispyware software and this will hopefully take care of the problem.

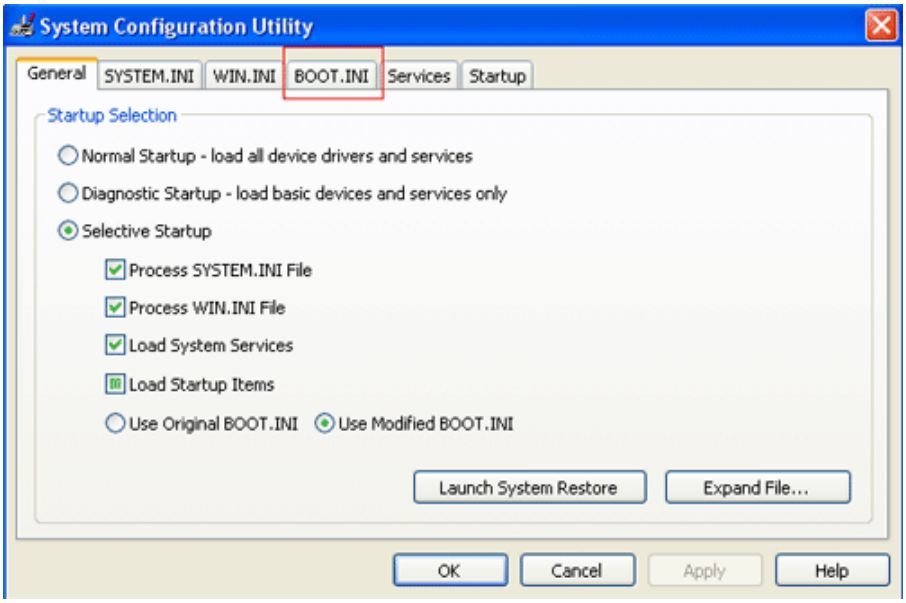
Using the System Configuration Method to Enter Safe Mode

If you can't get into Safe Mode with the F8 method, then you should try this method instead.

First, close any programs which are running. Then, click on the Start button and select Run. You should type msconfig in the Run field as seen in the picture below.



When you click OK, the System Configuration Utility will start.



Click on BOOT.INI. Then, in the area where it says Boot Options, put a checkmark in the /SAFEBOOT box. When you click Ok, you will be given an option to restart the computer. Click the Restart button. Your computer will restart in Safe Mode.

You will then be able to run the antispyware software in Safe Mode. When you finish, you will need to make sure that you follow the same steps as before but uncheck the /SAFEBOOT option. Then, under the General tab, you will need to select Normal Startup.

Chapter 15

Manual Removal of Spyware

There are many types of spyware which your antispyware will be able to detect but will not be able to remove. When this happens, your best bet is to remove the spyware manually. Be warned that this is often a very tedious process which takes careful examination of your computer system. Since spyware often exist with viruses, you may remove all of the spyware but miss a virus. Then, the spyware is able to quickly reappear through a hole that the virus made. However, if your antispyware system fails you, then this may be your best option.

Luckily, there are special tools for removing some of the most common spyware which are resistant to antispyware methods. One example of this tough strain of spyware is called Cool Web Search. The spyware will invade a user's system and then hijack the home page. Then, it will load the computer system with various Trojan viruses. Cool Web Search is very common but antispyware software makers have been having trouble combating it because there are countless forms of it.

For Cool Web Search, you can download a special tool called CWShredder. However, the strains of Cool Web Search spyware keep getting stronger and the new ones are resistant to CWShredder. For newer variations of the spyware, a utility called CoolWWWSearch Smart Killer will do the job. However, by the time you read this, this utility might already be useless against the newest strain of the spyware.

Manual Removal of Spyware Files and Entries

Unfortunately, not all spyware types have utility tools made specifically to combat them. Instead, you will have to destroy the spyware files and entries one by one. First, you must find out through your antispyware which type of spyware you have. Then, you can type in its name to a search engine and you should get lists of sites offering removal

instructions or tools. There are a lot of great sites out there which will give you detailed descriptions of how to remove spyware software.

For example, the site www.spywareremove.com has great detailed instructions on just about every type of spyware. As new spyware is introduced, the site updates information so users can combat the spyware by manually deleting it.

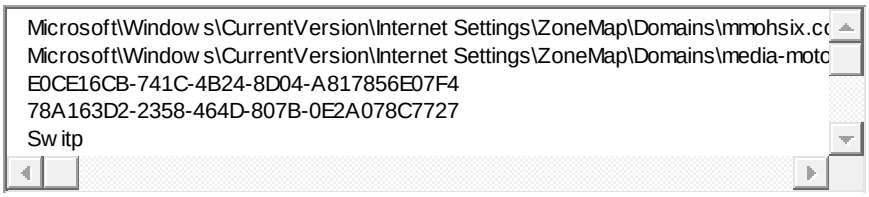
Here is an example of what spyware removal instructions look like for a new type of spyware called MediaMotor:

Step 1: Use Windows Task Manager to Remove MediaMotor Processes

Remove the **"MediaMotor"** processes files:

Step 2: Use Registry Editor to Remove MediaMotor Registry Values

Locate and delete **"MediaMotor"** registry entries:



Step 3: Detect and Delete Other MediaMotor Files

Remove the **"MediaMotor"** processes files:

Step 4: View the MediaMotor Components with its MD5s

Remove the **"MediaMotor"** components:

File Name	File Size	MD5
adsetup_silent.1.53[1].exe	118755	dc4a55fd8625e43e271188696431df97
tdopkpif.exe	36864	921ef076fb6745a727626d050ea4c735
thiselt.exe	42784	ec0590d49b53b51d24af35232d71a895

In order to carry out these instructions, you will need to write down or print all of the files and entries associated with the spyware. Then, you will turn on the computer in safe mode and manually remove all of the spyware files and entries. Since the list is so long, this will obviously be a tedious task. That is why it is best to wait until you have tried several types of antispyware software before manual removal.

It is also good to read some of the user comments which are generally posted after spyware removal instructions. This will give you an idea of what problems people are coming up against. And yes – there will almost always be some sort of problem!

Warning about Manual Spyware Removal

Keep in mind that you should always back up your PC before you attempt to remove any spyware or make any changes. It is very easy to remove the wrong files because spyware is often designed to mirror files which should be on a normally-functioning computer.

If you are not familiar with your computer's functions, it is best that you leave it to the professionals to remove spyware. There is too much of a risk that you could end up accidentally deleting an important file or entries and thus completely impairing your computer's ability to function. One option is to hire a professional to teach you how to remove certain files and make sure that they are really deleted.

Even though this seems like a really futile cycle, there isn't much that regular internet users can do about it. As a new spyware is created, a specialized utility for combating the spyware is released. Then, the spyware creators seek holes in that new utility and exploit them for the next strain of spyware.

Chapter 16

Manual Spyware Removal without Instructions

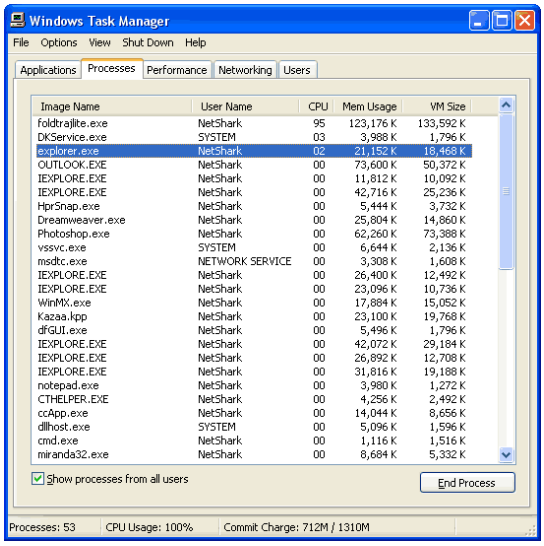
When you have the name of the spyware which your computer is infected with, it is easy to find instructions for the spyware's removal. All you need to do is type in the spyware's name and you will get detailed instructions and users' comments to guide you through the process.

However, in order to get the name of the spyware, your antispyware needs to be able to detect it. Some spyware are so well hidden that your antispyware may not be able to find it at all. Also, if you don't have any antispyware and become infected, the spyware may not allow you to use antispyware. In this situation, you also won't be able to find the name of the spyware and look up its removal instructions online. Manual spyware removal is still possible in safe mode. However, you will have to find out where the spyware is located on your own.

There are seemingly millions of places where spyware can hide in your computer's system. Luckily, finding out where the spyware is hiding is not as hard as it used to be in the past.

First, you will want to start your computer in safe mode. Once in safe mode, press CTRL+ALT+Delete. The Task Manager will come up. Then, click on the processes tab. You will see a list of all of the processes which are essential to the Windows operating system. Make a list of all of these processes.

Next, restart your computer so you boot Windows normally. Then, look at the processes in Task Manager again. Make a list of these processes and compare it to your first list.



The second list from when Windows was booted normally should be longer than the first. From the second list, cross off any processes which were running in safe mode. Then cross of any processes which you may recognize.

What are left on the list are higher-level Windows processes, ad-on applications, spyware and any other infection your computer may have.

Now, you will need to go to www.processlibrary.com. At this site, you will be able to type in the name of the processes in order to find out what they are. This will keep you from deleting any potential vital processes from your computer. Process Library is good at keeping the list of processes updated so you should be able to find everything on your list. Any unidentified processes are likely spyware.

After finding out which of the processes are likely to be spyware, you should download a utility called StartupList. This utility can be used to show you which programs are launching when you boot Windows. This information will further help you identify any spyware on your computer as well as viruses or worms. You can find the utility here: http://www.spywareinfo.com/~merijn/downloads.html.

You should now have a list of all of the spyware files and entries. Then, you can go through your computer in safe mode and delete them all. This can be a very tedious procedure which is just made worse if you try to rush. Take your time to make sure that you remove all of the illicit files and entries.

Chapter 17

Combating Browser Hijackers

It seems like almost all new spyware software programs are now browser hijackers. These types of spyware will change your browser start page, search page, and/or favorite settings. The reason that this is done is to get extra traffic for the sites of certain websites. Since websites depend on traffic for success, browser hijacking is becoming a very large problem.

In some cases, you can return your browser setting back to normal with just a few clicks of the mouse.

1. In Internet Explorer, click on the Tools heading. Then click on Internet Options. Under the general tab, you will find a place to type in what you want to be your home page when your web browser starts up.

2. You will need to reset the search page. Do this by clicking on the Menu tab called Programs. Then, click on the button labeled as Reset Settings. You will get a prompt asking if you want to proceed. There is a box in the right-hand corner that says Reset Start Page. By clicking on this box before proceeding, you can reset your settings.

3. Open up the Favorites section in Internet Explorer. Delete all the spyware bookmarks.

Unfortunately, not all browser hijackers are this easy to fix. If the settings keep on going back to the spyware hijacked settings, then you will have to change it in the registry following these steps.
1. Click the Start button on your computer and then select Run. Type in the command **regedit** and then hit enter.
2. Your registry editor will appear. You need to find the Start Page which will be located in this path:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main
3. Double click on the Start Page entry. You will be able to enter the startup page that you want.
4. Now, you will need to reset your search pages. They are located in the same area as the registry editor and are labeled as such:

- Search Page

- Search Bar

5. Fill in the entries for the Search Page and Search Bar.
6. You will also need to check these paths and make sure that they are set to the right search engine:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\SearchURL

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Search

To save you the trouble of doing this each time your registry gets hijacked, you can download the tool anti-jack.reg. This is a file which will edit your Windows registry. The file will contain paths for the files which you changed above. Just change the files in anti-jack.reg to reflect your preferences. Whenever you want to default back to those settings, you can just double click on the anti-jack.reg file.

Running Hijack This Against Registry Hijacking

There are a few reasons that registry hijacking is such a nuisance. First of all, many antispyware software programs don't reset your browser to something which is safe. Then, when you go to open up Internet Explorer, you are directed to the malicious site and your computer is instantly re-infected with the spyware program.

After running antispyware, you should NEVER open up your internet until you have changed your browser settings. Another option is to run the antispyware tool called Hijack This first. The utility will reset your Internet Explorer back to the original settings.

Hijack This is also a great tool for removing any bits of spyware which other antispyware software may have missed. Hijack This is a completely free antispyware tool. Its only downside is that it is a bit difficult for novices to use. However, you can find a great tutorial that will take you through the processes of using Hijack This here: http://hjt.wizardsofwebsites.com.

Chapter 18:

Spyware that Prevents You from Running Antispyware

One of the most common new complaints with spyware is that it actually prevents the user from running antispyware against it. There are a few ways that this problem shows itself such as the user cannot visit antispyware sites, cannot download any antispyware software and/or cannot update antispyware software.

These traits are not just limited to spyware. The famous Conflicker worm will restrict a user's access to websites dealing with computer security. This prevents the user from gathering information which is necessary to fight the infection. Some of the websites which Conflicker blocked include AVG, McAfee, Symantec and F-secure. Other infections may give users restricted access to security sites and thus prevents them from downloading or updating any security-related software.

There are a few options that can be used to cure this type of spyware infection:

1. The easiest option would be to use an uninfected computer to download antispyware software. Then, use a removable disc to transfer the download onto your computer. If you know what type of spyware you are infected with, it is also recommended that you spend some time in forums to find out which antispyware software programs were effective against the type of infection you have.

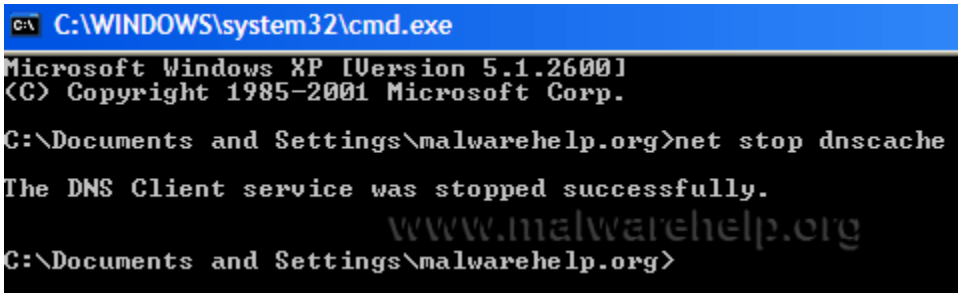
2. The next easiest solution is to simply try another browser. Internet Explorer, for example, has many security holes which another browser may not have. You may want to try Mozilla Firefox, Opera or Google Chrome. These browsers may allow you access to security sites and downloads.

3. If you still don't have any luck, you can try launching your computer in Safe Mode with Networking. Safe mode will only start the core files and drivers which are necessary for running Windows. Because of this, most spyware will not open in safe mode. With the Safe Mode with Networking option, you can still get online and download any antispyware updates you need.

4. Another option is to try finding the antispyware software from alternative websites. Chances are that the spyware infection is only blocking websites which are related to computer security issues (it may be blocking them based on keywords found on the sites' descriptions). Instead, try looking for antispyware at free software download sites. Also, if you only need the antispyware software definitions, you can go to one of these sites: MajorGeeks.com, Softpedia.com, or FileHippo.com.
5. Some types of spyware will redirect your DNS queries. You can stop this by turning off DNS caching.

- In Windows XP, click Start and then Run.

- Type in **cmd** and then click OK.
- In the prompt field, type in **net stop dnscache** and click Enter.
- You should see a message saying, “The DNS Client Service was stopped successfully.” You can now type in Exit and click Enter.



For Windows Vista and Windows 7, you will have to turn off DNS caching in a slightly different manner:

- Click Start and then type in **cmd** into the search field.
- Click on **cmd** and then select the option, “Run as administrator.”
- Select Continue when you get the User Account Control prompt.
- From here, follow the same steps as with Windows XP.

6. The last option for removing antispyware which won’t let you download antispyware is to check for hosts file hijacking. The spyware may have changed or replaced the host’s file of your system in a way that prohibits you from viewing security-related websites.

The hosts file is generally found in the folder Windows\System32\drivers\etc. Enable the “show hidden files and folders” option. Then, uncheck the option “hide protected operating system files”. This will be found in the Folder Options Control Panel.

Unless you have customized your hosts file, then all entries which do not have a # symbol at their start should be considered suspicious. The exceptions to this are: 127.0.0.1 localhost and ::1 localhost.

You can use an automatic tool from Microsoft in order to restore the hosts file back to its

default setting. However, spyware often changes the hosts file in a way which makes it difficult to restore. In this case, you should use a program such as HostXpert to restore the hosts file. HostXpert is free and you can use it without even installing it. After

downloading HostXpert, click OK. Then, click on Restore MS Hosts file and your hosts file should be restored.

Chapter 19

Spyware that Prevents You From Starting in Safe Mode

Running an antispyware software in safe mode will usually fix a spyware infection because most malware do not auto start while in safe mode. Thus, you can safely remove them before they start again automatically. However, many of the newer spyware programs have found a way to combat this method of removal. They actually prohibit you from opening in safe mode at all.

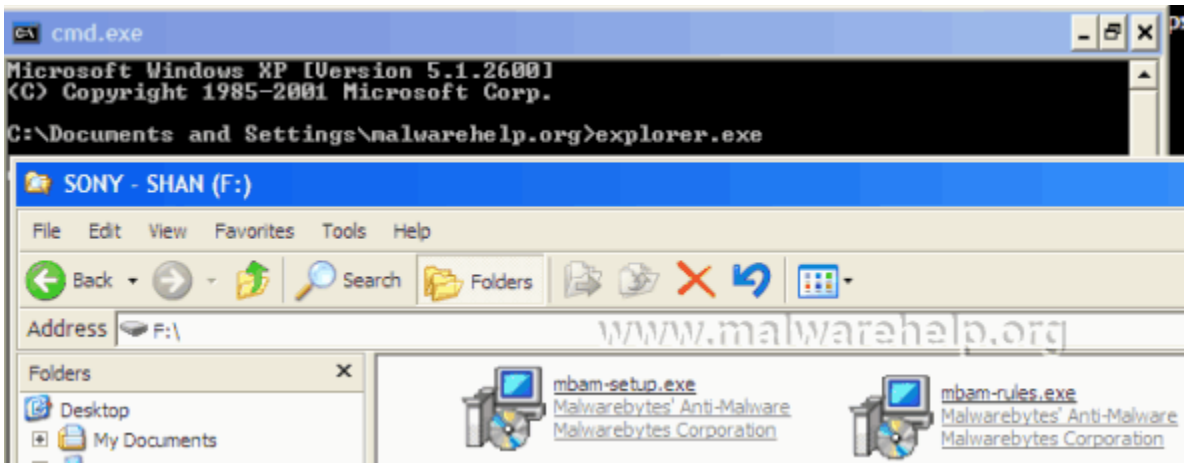
If you cannot enter in regular safe mode because of a computer infection, you should first try to start the computer with the "safe mode with command prompt" option. This will start Windows only with core drivers and then launch the command prompt.

You will then have to run an antispyware with the command prompt. Here are brief instructions on how to do so:

1. First, use an uninfected computer to download MalwareBytes's Anti-Malware. Then, you will need to download the Malwarebytes's Anti-Malware Malware definitions. You can use different antispyware software as well but this one has been effective. Put both of these downloaded files onto a removable disc.

2. Open Windows and, using the F8 key, boot in Safe Mode with Command Prompt.

3. You will receive a command prompt. Type in "explorer.exe" and then press Enter. Windows Explorer will open. Then, use the "My Computer" area to find your removable disc with the antispyware tools you downloaded.



4. You will need to install both files. Then, launch the Malwarebytes's Anti-Malware. Choose "Perform Full Scan" from the tab labeled Scanner. After the scan is finished, click on the option "Show results." Make sure that all of the spyware software is check marked and click on the "Remove Selected" option. You may be prompted to restart your computer in order to finish the spyware removal.

5. Restart your computer in normal mode. Then, scan again using Malwarebytes's Anti-Malware.

Can't Get into "Safe Mode with Command Prompt"

Some particularly heinous spyware software won't even let users get into safe mode with command prompt. This happens when spyware deletes registry contents for the key **HKLMSystemCurrentControlSetControlSafeboot.** If this is the case, you have several options:

1. Use an anti-virus rescue disk to restore your computer.

2. You can use a program from Didier Stevens which is designed to defeat this sort of spyware by recreating a "undeletable safeboot key."

3. From sUBs, you can get a program to repair the Safe Mode key: SafeBootKeyRepair.exe

4. ElPiedra makes a registry file which can be used for repairing safe mode. You can find it here: SafeBootKeyRepair.

5. The antispyware program SuperAntiSpyware Free edition gives users an option that allows them to restore a SafeBoot key. To do this, just open the antispyware program

and click on the Preferences tab. Then, click on Repairs and you will see an option for "Repair Broken SafeBoot key."

6. Depending on the type of PC you have, you may already have a restore CD which can be used to recover the key.

7. The last couple of options are for users who are more advanced with combating spyware. You may need to install the Recovery Console or try to Repair Install Windows XP, Vista or Windows 7.

Chapter 20

The Future of Spyware

There have been numerous attempts to regulate spyware use by law. Some states, such as Utah, are fervent in their objections to spyware and have created strict legislature against all types of contextual advertising based on which website's a person visits unless that person agrees ahead of time based on a full disclosure. The law goes on to say that this disclosure must include everything from the type of data transmitted to ad examples. Additionally, the ad software must be easily removable.

The federal government in the United States is following Utah's example with House Resolution 2929, The Spy Act. However, spyware is a global problem and legislation alone likely won't fix the problem. That is because the legislation doesn't address the root problem of why spyware must exist in the first place.

Spyware exists because software makers needed a way to make money off of their products. Since fewer and fewer people are willing to spend $29.95 on software, including advertisements with free software seemed like the only choice.

What is interesting is that many people become enraged over the idea of ads being included with software. However, almost all other free applications online come with advertisements: email services, instant messengers, search engines, and so forth. The difference between these ads and the spyware ads is simple but major: the spyware brings ads to users in covert means.

Because of the covert manner in which spyware is installed, the entire spyware industry has gotten a bad name. However, there are many cases in which people would even choose to have spyware. For example, a person may knowingly agree to receive occasional pop-up ads in exchange for access to free software programs.

Antispyware legislation is one step in the right direction but this is not enough. People are going to have to reconsider what “free” really means on the internet and businesses will have to rethink their marketing strategies. Until some major changes occur which leaves software makers and users happy, the only feasible choice is going to be for people to protect themselves with antispyware software.