This Report Brought To You By:

Richard Rossbauer

RichardPresents.com

Visit Us At: http://www.RichardPresents.com

ANTI-SPYWARE 2008

SEND THIS GUIDE TO A FRIEND

Hi,

I have written this guide to help you to understand what Spyware, and Adware are.

I am sure you will find the guide useful in the context of understanding what they are and combating them.

If you have never heard of nor fully understood what these nasty software bugs are then keep reading...

A little while ago I was not so smart on the subject either. I often heard of people talking about Spyware and Adware and often pretended I knew exactly what they were talking about. In fact I knew very little!

That was until recently, when I got infected!

That's when I found out what I know today, after spending many hours and days trying to get rid of the Adware that infected my PC.

I have decided to share what I have found with you so you are better equipped as these horrible little programs are NOT going to stop.

The fact it is, they are on the increase, and according to statistics **92% of computers are infected** and most people don't even know their computers are!

That is a lot of computers. If you haven't got any protection or even if you have there is a good chance you are still infected.

That is because not all anti-spyware programs check for the same things! This means usually you would need a couple of anti-spyware type programs installed.

BUT, this slows down your machine drastically. Always updating, both running together, and some programs find the other as being spyware itself.

Trust me, I know, I've tried them...

http://www.antispyware2008.net/scan

Anyway, let me start and describe what protection Windows comes with.

Windows Firewall - What is Windows Firewall?

It is an anti-hacker tool, so people can't get into your PC from the internet.

Is it any good?

Yes and no. Yes because the firewall is actually quite effective, no because it is a Microsoft product and installed on every machine since Windows XP Service Pack 2 and most hackers target this firewall as it is a Microsoft product.

Should I use it?

I would say yes, but I also have another program now protecting me against hackers, more about that later...

A firewall (protection from hackers) DOES NOT protect you from Viruses, Spyware or Adware.

This means there are 3 things we need to protect ourselves from:

1: Hackers (Firewall) - People scanning the internet trying to get into your computer to either steal stuff or looking to corrupt your PC.

2: Viruses - These usually destroy some part of your computer so you have to reinstall from scratch. They also can be worms in the fact that they replicate themselves by sending themselves to your email contacts or other computers you may have linked together (networked).

3: Spyware/Adware - These nasties aren't usually intended to kill your PC, but they certainly slow it down to a crawl. They are usually pop-up advertisements in the hope you click on them (Adware). Others log everything you do on your computer in the effort to try steal your details (identity theft – Spyware, also called Malware).

Out of all of them, the Spyware range is probably the worst.

Why?

Well, hackers don't usually target individuals, usually they get a better reputation amongst their clan if they manage to hack into a large well known company (but this isn't always the case), it is still very advisable to take preventative measures.

http://www.antispyware2008.net/scan

Viruses are aimed at damaging more than anything else, they have a purpose in mind to corrupt your system, they usually do not log any information but they are known to replicate themselves.

Spyware/Adware is the probably the worst. Although they are not always intended to corrupt your system they certainly slow it down? Why? Because once infected the Spyware/Adware usually calls more sites that you may click on or visit and install more spyware. Each instance of Spyware/Adware also uses system resources (Memory, CPU). The more malicious ones can also steal your identity!

In this guide I am going to focus on Spyware & Adware

Anyway, a few weeks ago I got infected by clicking on a banner. I have a pop-up blockers installed as part of my Internet Browser but these guys often know how to get around them.

But before I tell you how I got rid of these nasty programs after spending days and lots of money let me explain further what this stuff is.

Spyware/Adware:

What's the difference? (Basic Summary)

Well, usually Spyware is used to gather information from your computer. It can be used to log personal information and computer habits. It can log websites you have visited and send the information back to a central location (fraudster).

Until a few years ago the threat from Spyware wasn't much to be considered

Adware usually displays advertisements. This is very annoying but usually not as severe as Spyware in the fact that they do not 'usually' transmit any personal information.

Spyware…what is it?

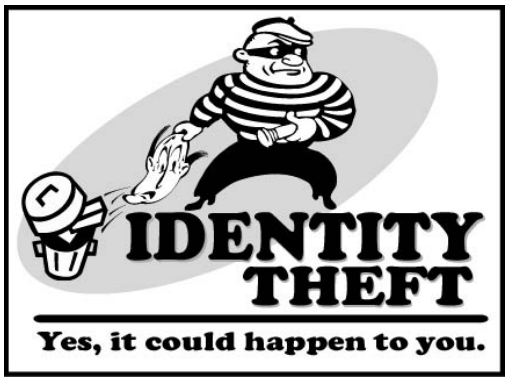
Over the years because the Spyware problem has mutated so much, we now describe Spyware as part of a much larger category of rouge software called "Malware" (malicious software programs).

Spyware (Malware) is when these nasty little software programs install themselves onto your computer without your knowledge or consent. Once in place these programs may do hundreds of undesirable things to your computer.

> They can log your keystrokes, steal your passwords, observe your browsing habits, call pop-up windows, send emails and send you rogue emails, redirect your web browser to phishing pages (pages that look real like PayPal or eBay but are actually fraudulent copies), report your personal information to distant servers (identity theft) and serve up pornography.

Spyware usually operates invisibly, and are extremely difficult to find and get rid of. They cannot be seen in 'Task Manager' and to top it off they cannot be removed via Add/Remove programs as they are hidden.

These applications can seriously use up system resources and can cause your PC to crash or freeze.



Adware…what is it?

Adware is similar to Spyware; but its primary goal is to install secret advertising software. This usually generates on screen adverts (called pop-ups) and once installed often can get around any pop-up blocker you may have.

They can be a real pain and often nearly impossible to uninstall (like Spyware).

The worst forms of adware are 'hijack' links in web pages. So instead of taking you to the correct website they take you to a different site who has often paid the adware makers.

Others will open a new page every time you browse to a website. Some will open multiple web pages, this can get really annoying. Sometimes pop-up advertisements will show at random intervals on your desktop.

Spyware/Adware are generally used to cause or monitor certain behaviors:

- Collect information from your computer without your knowledge and/or consent
- Transmits a unique code to identify you (for tracking purposes) without your knowledge
- Collects/transmits information about your computer use or other habits without your knowledge
- Installs itself on your computer without your knowledge and/or consent
- Keeps reinstalling itself, no matter how many times you remove it
- Performs other unwholesome duties without your knowledge and/or consent

You could possibly have Spyware/Adware on your PC if:

- You notice other web pages opening without you going to the website
- Your web browser home page has changed without your knowledge
- There is a new toolbar in your browser that you didn't install or want
- Your computer is running slower than usual
- Internet has slowed down and not as fast as it used to be
- Your PC isn't as stable as what it used to be (crashing, irregular behavior)

http://www.antispyware2008.net/scan

As you can see, Spyware and Adware are not good for your computing experience and can be VERY dangerous by monitoring your personal information.

How do you get infected?

Software:

Peer to Peer file sharing. Many free file sharing applications install spyware. If not installed with the application the files shared often contain them.

Many software applications come embedded with 'advertising' built-in to help pay the developers.

Others will have a disclaimer deep inside the license agreement saying that information about you and your browsing habits will be sent to the company's website.

The information collected about you is often for advertising purposes, but spyware can scan files on your hard drive, listen in on other applications like chat programs, read cookies and send back this information

Be careful of free software, totally free software often contains some form of advertising and can install applications like 'GAIN' (The Gator Advertising and Information Network), often referred to as GAINware. This allows you to get free software that is supported by ads and information based on the web sites you view.

Here are SOME Spyware/Adware programs installed with software:

Brilliant Digital
Gator
Joltid
Topsearch
NavExcel Toolbar
WhenU SaveNow
WhenU Weather
PIB Toolbar
Huntbar Toolbar
NEO Toolbar
Ezula

The last research I did there are nearly 300,000 instances of different Spyware/Adware circling the net!

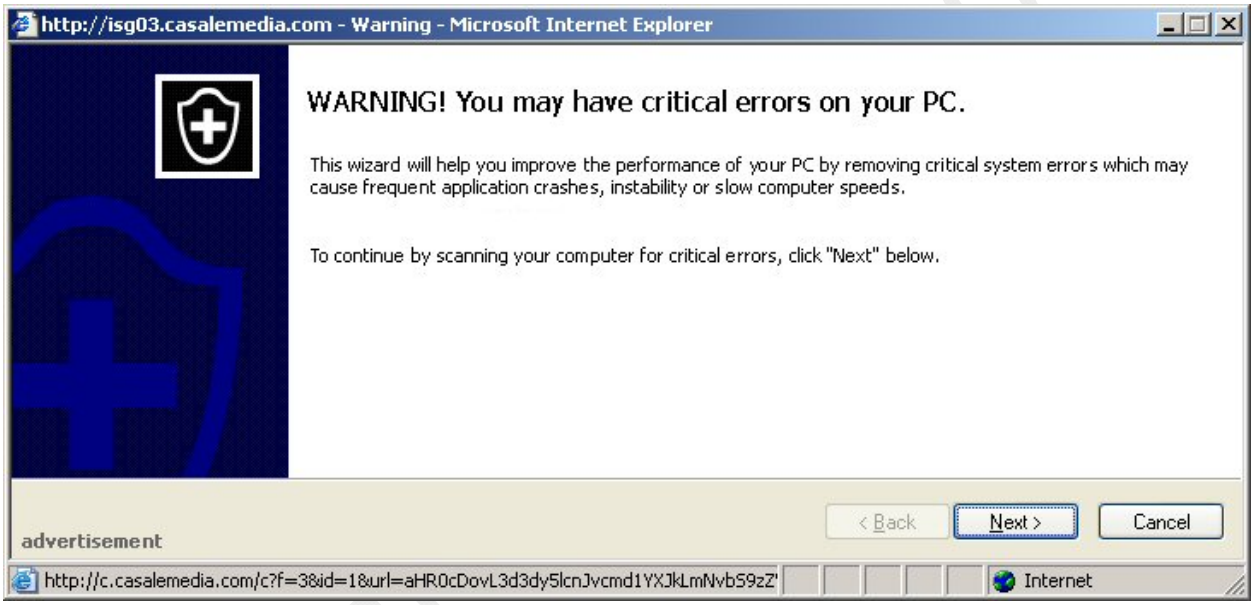
http://www.antispyware2008.net/scan

Oh, be careful. Some sites advertise that their 'Free' software is Spyware/Adware free but it is NOT always the case.

Because Spyware is often included with freeware and shareware it doesn't hurt to do some research on programs BEFORE you download them. Doing a simple search in Google or a major search engine should tell you a little more whether or not the software is legitimate. Usually people post in forums or a review about the software and will let you know if it installs anything malicious.

Web browsing:

Proper reputable websites are usually safe, but there are lots of websites that try to influence you to click on a hover ad or intelligent pop-up (a pop-up that can get around your browser's pop-up blocker or other pop-up blockers).

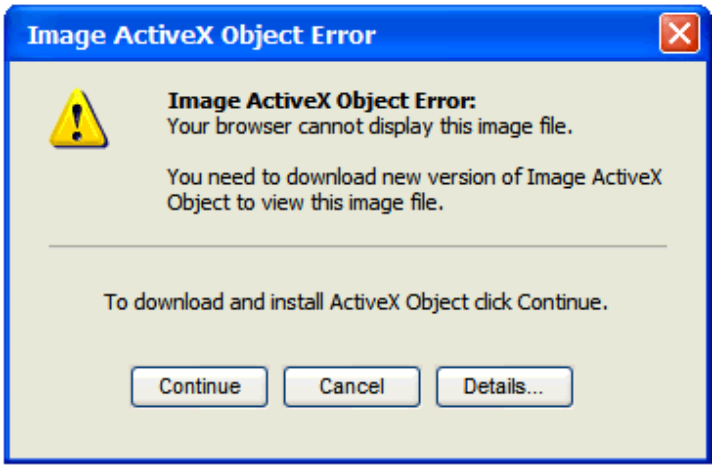


ActiveX controls:

Some websites advise you to install an 'ActiveX' control that installs itself into your web-browser. If you do not know what it is do not accept the installation. Once installed it will have free reign to gather and display whatever it wants.

But it can sometimes be tricky to prevent, as some free game sites will require you to install an Activex control to play a game, well, this may also contain adware/spyware.

Screen savers, weather monitors and emoticon packages also often contain a variety of adware/spyware.



How do I know if my computer is infected with Spyware?

The ONLY way to make sure you are safe is to run a full system scan using good, reputable software.

CAUTION: Only use Anti-Spyware software you trust! I Only recommend tested products.

See 'Why' below (extract from SC Magazine):

A complex plot involving fake anti-spyware products has scammed thousands of victims out of money and personal information, according to Secureworks.
Anti-spyware solution scam steal personal financial information.

Hackers in Russia and other Eastern European countries are using the Russian Business Network (RBN) internet service provider (ISP) and other hosting outlets to lure victims into clicking on malicious ads on high-traffic websites, the Atlanta-based company reported this week.

Clicking on a malicious advertisement opens a pop-ip warning about a suspicious problem on the victim's computer, initiating a "sales process" for a bogus anti-spyware solution that costs $39.95 to $79.95. The rogue websites collect credit card numbers, names and other personal information in the process, according to Secureworks.
Finally, the "anti-spyware solution" downloads a Trojan, such as Zlob, which retrieves other personal information from the victim's PC over time, or a rootkit, which gives the attacker remote control of the victim's computer.

The names of the bogus anti-spyware found in this offer include Spy-shredder, AntiVirGear, MalwareAlarm, and about 40 others.

The scammers make money not only from the sale of the "solution", but also from the sale of credit card numbers and access to the Trojan and rootkit-infected computers….

http://www.antispyware2008.net/scan

Symptoms of Spyware and Other Pests

Depending on the type of infection, it can be quite easy to see you have a problem. These are actually better as you know that there is something wrong. The bad news is that the most dangerous Spyware can actually be very difficult to detect and you will probably never notice them.

That's why most checking and removing of these nasties are done with software designed to do just that.

Here are some symptoms:

- **Do you see pop-up advertisements?**

When you are online do ads keep-popping up displaying things you never asked for?
When you aren't browsing the internet does the occasional ad still pop-up?
Did you visit a website or open a web page? Most pop-ups launch when you open a new web page.

Obviously not all websites have bad pop-ups, if you are visiting a reputable website that you know and trust they may include pop-ups for latest news or products. Your web browser should notify you if a pop-up has been blocked and you can usually allow that site to display pop-ups if you wish.

Be careful of sites you don't trust or is your first time visit.

In fact if you see any ad that was not called for by you then you are probably infected with Adware/Spyware.

- **Is your computer is doing weird things?**

Some of these nasties can alter the way your computer behaves.

Sometimes making your CD drive open and close by itself, or applications opening or closing by themselves.
Is your hard drive spinning away while you aren't doing anything?
Is there an unusual icon in the system try (bottom right by the time)?
Do you notice unusual internet activity on your modem or broadband router? Eg. Lights flashing without actually browsing the internet?

If so, you'd better check for Spyware…

http://www.antispyware2008.net/scan

- **Slow Computer?**

There can be a number of reasons why your computer is running slow, but if it is used on a regular basis then you are probably familiar with the usual speed of your machine. Computers are machines, they do not have a 'good day' or a 'bad day'. If a sudden change in how your computer is running happens it could be a sign of Spyware or Adware.

Spyware/Adware and other nasties are each a program of their own, therefore using system resources (CPU, Memory, and Internet Speed).

- **Toolbars…**

There are many companies that now ask if you would like to install their toolbar.

Some more reputable ones are Google, Yahoo, eBay. The Google toolbar has been accused of being spyware because it includes a Page Rank feature that tells Google where people are surfing on the Web. However this feature can actually be disabled.

Be careful of many toolbars, these are often found within free applications and usually incorporate their own advertising systems. Remember, not a lot is free nowadays, and always ask yourself: 'What's the catch?'

- **Instant Messaging Pest-Ware**

EXAMPLE: There was/is an application called 'Buddylinks' which requires the user to download, install, and agree to an end-user license agreement (EULA). It is known to spread marketing messages via AOL's Instant Messenger (AIM). It appears to be a recommendation from an AIM user that encourages contacts to visit a web page to download a video game, such as the 'Osama Found' game.

Deep in the EULA is a statement that AIM users who download it give their permission to send marketing messages to their Buddy List contacts. This way the program can spread itself by sending links to the web page, and it seems to come from a known contact.

- **E-Mail**

This can be a total annoyance. If you are getting a lot of bounced back mail and see signs of emails being sent without your knowledge, then it is possible that 'trojan spamware' has found it's way onto your computer.

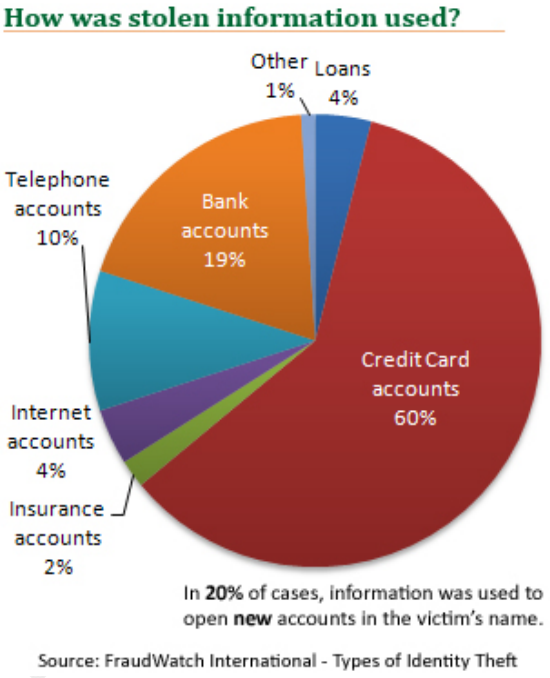
Spamware is a Trojan that can turn your computer into a Spam launching pad and create headaches for unknowing computer users, especially if it sends itself to your contacts (not good).
They can also 'steal' a copy of your address book and send it back to a spammer.

- **Keyboard Loggers/Identity theft**

Some of these worst Spyware are Keyboard loggers. These can capture passwords and user names, so if the bank, brokerage or credit card accounts you access appear to be tampered with, your computer maybe the source of the trouble and infected with this malicious software.

User names, passwords, credit card details, banking details, in fact any personal details as well as Web-based applications are also vulnerable.

The only way to know if you have any of these nastie pests is to run a system scan using good and reputable software.



Helping YOU avoid them!

First things first, run a full system scan of your PC and make certain your PC is clean.

CLICK HERE TO RUN A FREE SCAN NOW

Once clean I would advise you abide by the following to help prevent infection in the future.

- **Always make sure you have your anti-spyware software is running BEFORE you start browsing the internet.**

- **Don't use peer to peer networks**

Even if you find a file-sharing application that is actually free of spyware the files that you download could be infected.

You see, it is easy to embed a bit of spyware into a program, I've even had a go myself and succeed in making a pretty nasty program that could cause a lot of damage to Windows (malware). It was for testing only.

I would recommend using quality pay download sites, be weary of Eastern Europe (Russia etc).

- **Quality web-browsing**

Don't click onto any website you see. Usually the search results in Google, Yahoo, MSN will give you a brief description of the site and the URL (the link name). If it doesn't look up to much don't visit it.

As a rule of thumb most of the first page results are decent quality, when you start going to the 3rd or later pages the quality of the results tends to whither and the sites often begin to get a little more dubious. However this depends on what you are actually looking for.

You should have a pop-up blocker installed, latest version of Internet Explorer or Mozilla Firefox come with built-in pop-up blockers, however some websites use dialogue boxes and can sometimes get around the pop-up blockers.
If you are on a website that you don't 100% trust close the window, but be careful, sometimes they make a close button in to actual advertisement, this will still take you to their site or infect you.
I suggest you use the ALT + F4 keys to close the window or your web-browser. This terminates the window without having to click on the 'close' button.

Be careful if a website asks you to install ActiveX controls, or anything for that matter. If you don't trust it, do not install it. Obviously if the site is something like Microsoft or Apple then you know they are okay. But if it is a MP3 site in Russia then I would probably close the window and go somewhere else.

ALWAYS stay away from websites that offer you serials, cracks and free software. These sites are ALWAYS riddled with Spyware/Adware and you will get stung badly!

- **Pirated/Copied Software**

This is a grey area, but I know the 'hackers/crackers' sometimes hide adware/spyware in their keygens or the application installer itself. We all know it is illegal to install pirated software but if ever come across it run a scan on it with your anti-spyware software before doing anything.

- **I would recommend you always keep your Anti-Spyware/Adware application up to date a run/schedule a full system scan once a week.**

If you are 'clean' you should stay that way, if you follow safe web-surfing hbbits, stay away from scrupulous looking websites and free software that sounds too good to be true.

Different Variants Of Malicious Software

Adware

Adware is a generally harmless application that displays unexpected or unwanted advertising on your computer. It usually enters your system through freeware bundles or as additional/required content with shareware. You may choose to remove adware in order to stop unwanted advertising, but some programs are required in order to use a host application. Adware that may have tracking features/capabilities are in a more descriptive category (like Trackware or Data Miner) in order to give you more detailed information.

Annoyware

Annoyware is a type of adware that is frequently intrusive and disruptive. It causes an excessive number of popups/popunders, even when you are not connected to the Internet. Annoyware can also cause noticeable system and/or bandwidth slowdowns.

Data miner

Data miners are designed to actively collect information about you. Data miners can transmit your information to a remote server owned by the application's producer (This may be disclosed to you through a privacy policy/licensing).

Dialer

Dialers are designed to change your DUN (Dial Up Networking) settings in order to connect to your phone line in stealth mode, and/or dial expensive connections without your authorization.

Exploit

Exploit threats employ the use of software or a system exploit to install/operate.

Hijacker

Hijackers are designed to hijack your home page, Hosts file, browser favorites, default search engine, and/or system settings.

Keylogger

Keyloggers are designed to record and/or transmit keystroke information.

Malware

Malware is malicious software that is designed to harm your system.

Misc

This category is for noteworthy threats that do not fall under a specific detection category.

Monitoring Tool

Monitoring tools include Remote Access Trojans (RATs), Root Kits, etc.

MRU

These harmless records of the Most Recently Used (MRU) lists (like recent documents) are stored in your registry, but are included as a category by customer request. Some anti-spyware applications list MRU as being potentially harmful, so it appears their scan detected more content.

Spyware

Spyware is software designed to secretively collect information. It may install in stealth mode to gather information and transmit it to second and third parties without your knowledge and consent.

Trackware

Trackware is similar to Data Miners, but is passive in nature. It includes tracking cookies as well as applications that collect anonymous (not personally identifiable) information, like GUID's or sites visited.

Virus

A virus is a self-replicating program that injects itself into other programs. It can harm your system by damaging files, folders, directory structures, and erasing your hard drive. The best protection for your computer is a 3-tiered approach: anti-spyware software, anti-virus software, and a firewall.

Vulnerability

These threats use system and/or security vulnerabilities to install and operate on your system.

Worm

A worm is a self-replicating virus and/or Trojan, designed to spread across many systems and networks. The best protection for your computer is a 3-tiered approach: anti-spyware software, anti-virus software, and a firewall

Spyware Statistics

As the spyware industry becomes more sophisticated, the statistics become more staggering. Have a look at just a few of the facts and figures that show how widespread these 'cyber crimes' are in today's technological world.

IC3's Internet Crime Report, 2007

- The Internet Crime Complaint Center (IC3) received 206,884 complaints of web-based crimes during 2007.
- Internet crime is at a record high with nearly $240 million U.S. in reported losses during 2007, a $40 million increase from 2006.

FTC's Consumer Fraud and Identity Theft Complaint Data, Feb. 2008

- Identity theft continues to top the U.S. Federal Trade Commission's annual report on consumer fraud complaints, accounting for 32% of the 813,899 complaints received between January 1 and December 31, 2007.

Consumer Reports, State of the Net 2007

- In the first half of 2007, spyware infections prompted 850,000 U.S. households to replace their computers.
- 1 out of every 11 surveyed had a major, often costly problem due to spyware.
- The economic fallout per incident was $100, with damage totalling $1.7 billion.

Consumer Spyware Initiative

- Although as many as 90% of U.S. home computers have been infected with spyware at some time, a majority of PC owners don't know how to solve the problem.

Javelin Strategy and Research, Jan. 2007

- Americans lost about $49.3 billion US in 2006 to criminals who stole their identities.

Infonetics Research's Costs of Network Security Attacks: North America 2007

- Small and medium-sized organisations have "major problems" with spyware - representing 40% of all security downtime costs.
- Large U.S. organisations lose an average of 2.2% of their annual income - more than $30 million - to security attacks.