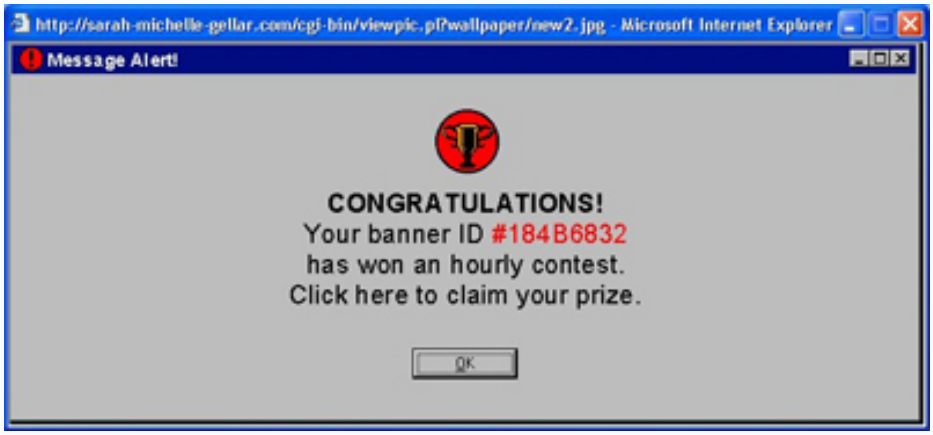
Introduction to How Spyware Works:

Spyware is a category of computer programs that attach themselves by sneaking on a computer's operating system (OS) to intercept or take partial control over the user's interaction with the OS, without the user's informed consent.

While the term spyware suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits, sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software, and redirecting Web browser activity. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet or functionality of other programs. In other words, spyware is malicious software that can hijack and cripple your computer; it can suck the life out of your computer's processing power. They're designed to track your Internet habits, nag you with unwanted sales offers or generate traffic for their host Web site. It has been known to cover-up as prize-notification pop-up window, like the example below. According to some estimates, more than 80 percent of all personal computers are infected with some kind of spyware

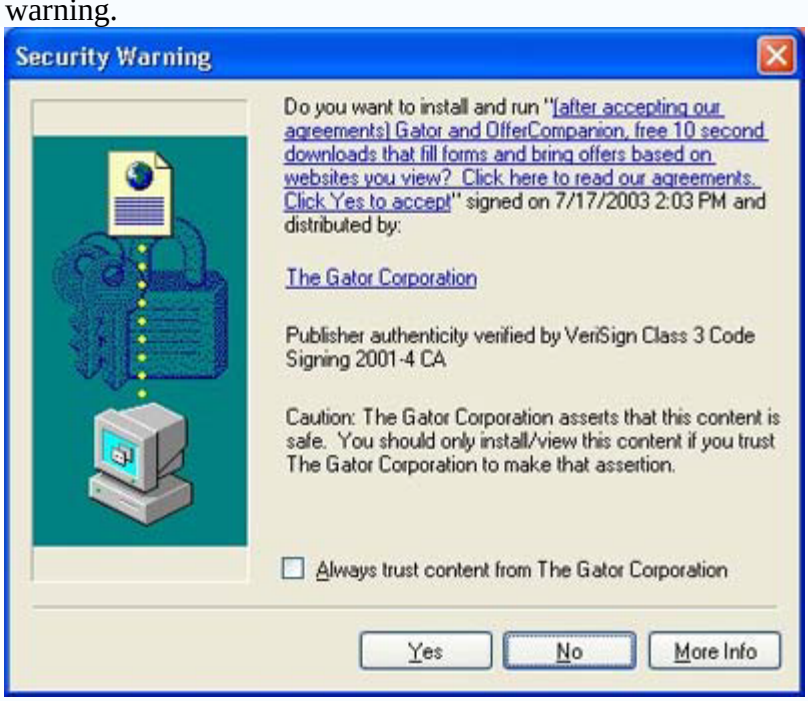


How Your Computer Gets Spyware:

Spyware usually ends up on your system through deception of the user or through exploitation of software vulnerabilities, like clicking a button on a pop-up window, installing a software package or agreeing to add functionality to your Web browser. These applications often use trickery to get you to install them, from fake system alert messages to buttons that say "cancel" when they really install spyware. Here are some of the general ways in which spyware finds its way into your computer:

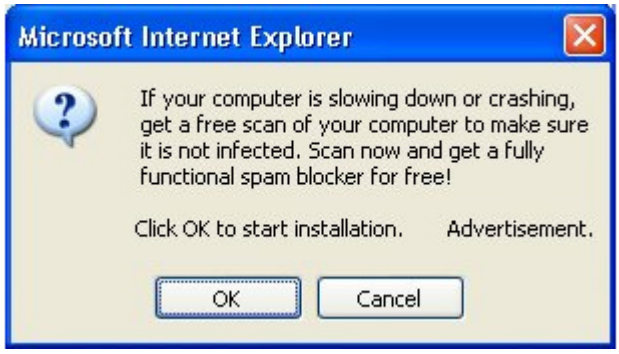
- **Piggybacked software installation** - Some applications (particularly peer-to-peer file-sharing clients) will install spyware as a part of their standard installation procedure. If you don't read the installation list closely, you might not notice that you're getting more than the file-sharing application you want. This is especially true of the "free" versions that are advertised as alternatives to software you have to buy.

- **Drive-by download** - This is when a Web site or pop-up window automatically tries to download and install spyware on your machine. The only warning you might get would be your browser's standard message telling you the name of the software and asking if it's okay to install it. If your security settings are set low enough, you won't even get the warning.



- **Browser add-ons** - These are pieces of software that add enhancements to your Web browser, like a toolbar, animated pal or additional search box. Sometimes, these really do what they say they'll do but also include elements of spyware as part of the deal. Or sometimes they are nothing more than thinly veiled spyware themselves. Particularly nasty add-ons are considered **browser hijackers** (these embed themselves deeply in your machine and take quite a bit of work to get rid of).

- **Masquerading as anti-spyware** - This is one of the cruelest tricks in the book. This type of software convinces you that it's a tool to detect and remove spyware.



When you run the tool, it tells you your computer is clean while it installs additional spyware of its own. Also some applications will tell you, you have spyware and will lead you to a website to download a program to help uninstall the software, and sometimes it

will tell you that you have to buy the program. But really what it is doing is just installing more spyware on your computer and then once you buy those programs (which you will have to purchase via online) you are hit with Crimeware**.**

Programs distributed with spyware:

These common spyware programs illustrate the diversity of behaviors found in these attacks. Note that as with computer viruses, researchers give names to spyware programs which may not be used by their creators. Programs may be grouped into "families" based not on shared program code, but on common behaviors, or by "following the money" of apparent financial or business connections.

- Bonzi Buddy
- CoolWebSearch
- Dope Wars
- EDonkey2000
- Grokster
- HuntBar
- Internet Optimizer
- Kazaa
- Morpheus
- Movieland
- RadLight
- Extended Copy Protection
- WeatherBug
- WildTangent The antispyware program Counterspy used to say that it's okay to keep WildTangent, but it now says that the spyware Winpipe is "possibly distributed with the adware bundler WildTangent or from a threat included in that bundler".
- Zango
- Zlob trojan

Programs formerly distributed with spyware:

- AOL Instant Messenger (AOL Instant Messenger still packages Viewpoint Media Player, and WildTangent)
- DivX (except for the paid version, and the "standard" version without the encoder). DivX announced removal of GAIN software from version 5.2.
- FlashGet (trial version prior to program being made freeware)
- magicJack

Partial list of rogue software:

There are a large number of fake anti-spyware programs active on the Internet. Typically, widely-distributed Web banner ads falsely warn users that their computers have been infected with spyware, enticing them to download the rogue software. Once installed, the software uses human engineering and false positives to manipulate the user into purchasing the software. These programs do not actually remove spyware - or worse, may add more. The following is a partial list of known rogue software. Often the same software is distributed under several names.

- Advanced Cleaner
- AlfaCleaner
- AntiSpyCheck 2.1
- AntiSpyStorm
- AntiSpywareExpert
- AntiSpywareMaster
- AntiSpywareSuite
- AntiSpyware Shield
- Antivermins
- Antivirgear
- Antivirus 2008
- Antivirus 2009
- Antivirus 2010
- Antivirus 360
- AntivirusPro2009
- AntiVirus Gold
- Antivirus Master
- Antivirus XP 2008
- Avatod Antispyware 8.0
- Awola
- Brave Sentry
- BestsellerAntivirus
- Cleanator
- ContraVirus
- Doctor Antivirus
- DriveCleaner
- Disk Knight
- EasySpywareCleaner
- Errorsafe
- free-viruscan.com
- FinallyFast.com
- GreenAV2009
- Graboid
- IE Antivirus
- IEDefender
- InfeStop
- Internet Antivirus
- KVMSecure
- MacSweeper
- MalCrush 3.7
- MalwareCore
- MalwareAlarm
- Malware Bell 3.2
- MS Antivirus
- MS AntiSpyware 2009
- MaxAntiSpyware
- Netcom3 Cleaner
- PCSecureSystem
- PC Antispy
- PC Clean Pro
- PC Privacy Cleaner
- PC SpeedScan Pro
- PestTrap
- Perfect Cleaner
- Perfect Defender 2009
- PersonalAntiSpy Free
- PAL Spyware Remover
- PCPrivacytool
- PC-Antispyware
- Plus4scan.com
- Premium-Antivirus-Defence
- PSGuard
- Rapid AntiVirus
- Real AntiVirus
- Registry Great
- Saliar
- SecurePCCleaner
- Security toolbar 7.1
- Smart Antivirus 2008
- Smart Antivirus 2009
- SpyAxe
- Spy Away
- SpyCrush
- Spydawn
- SpyGuarder
- SpyHeal
- SpyMarshal
- Spylocked
- SpySheriff
- SpySpotter
- Spyware Cleaner
- SpywareGuard 2008
- Spyware Protect 2009
- Spyware Quake
- Spyware Stormer
- Spy-Protect 2009
- SpywareStrike
- Spy-Rid
- SpyWiper
- System anti virus 2008
- System Live Protect
- SystemDoctor
- System Security
- Total Secure 2009
- TrustedAntivirus
- TheSpyBot
- UltimateCleaner
- VirusHeat
- Virus Isolator
- VirusProtectPro
- VirusRemover2008
- VirusRemover2009
- VirusMelt
- VirusRanger
- Virus Respone Lab 2009
- Virus Trigger
- Vista Antivirus 2008
- Watchnet Protection
- WinAntiVirus Pro 2006
- WinDefender
- WinFixer
- WinSpywareProtect
- WinWeb Security 2008
- WorldAntiSpy
- XP Antivirus
- XP AntiSpyware 2009
- Zinaps AntiSpyware 2008

What Can Spyware Do?

Spyware can do any number of things once it's installed on your computer.

At a minimum, most spyware runs as an application in the background as soon as you start your computer up, hogging RAM and processor power. It can generate endless pop-up ads that make

your Web browser so slow it becomes unusable. It can reset your browser's home page to display an ad every time you open it. Some spyware redirects your Web searches, controlling the results you see and making your search engine practically useless. It can also modify the dynamically linked libraries (DLLs) your computer uses to connect to the Internet, causing connectivity failures that are hard to diagnose. At its very worst, spyware can record the words you type, your Web browsing history, passwords and other private information.

Certain types of spyware can modify your Internet settings so that if you connect through dial-up service, your modem dials out to expensive, pay telephone numbers. Like a bad guest, some spyware changes your firewall settings, inviting in more unwanted pieces of software. There are even some forms that are smart enough to know when you try to remove them in the Windows registry and intercept your attempts to do so.

The point of all this from the spyware makers' perspective isn't always clear. One reason it's used is to pad advertisers' Web traffic statistics. If they can force your computer to show you tons of pop-up ads and fake search results, they can claim credit for displaying that ad to you over and over again. And each time you click the ad by accident, they can count that as someone expressing interest in the advertised product.

Another use of spyware is to steal affiliate credits. Major shopping sites like Amazon and eBay offer credit to a Web site that successfully directs traffic to their item pages. Certain spyware applications capture your requests to view sites like Amazon and eBay and then take the credit for sending you there

Other forms of Spyware:
Other forms of spyware include adware (which comes from the words **Ad**vertising Soft**ware**) and malware (which comes from the words **Mal**icious Soft**ware**)

Adware are software applications that are supported by advertisements. It automatically displays advertisement when the software is running. Some types of adware are also spyware and can be classified as privacy-invasive software.

Some well-know adware programs/programs distributed with adware are:

- 123 Messenger
- 180SearchAssistant
- 888bar
- Adssite Toolbar
- Antivirus 200 Family
- Bearshare
- Bonzi Buddy
- BlockChecker
- Burn4Free
- ClipGenie
- Comet Cursor
- Cydoor
- Daemon Tools
- Direct Revenue
- DivX
- DollarRevenue
- ErrorSafe
- Evernote
- Ezula
- FlashGet
- Gamespy
- Gator
- Kazaa
- Micro Antivirus
- Mirar Toolbar
- PornDigger!
- Smiley Central
- TagASaurus
- TopMoxie
- Tribal Fusion
- XXX Shop online
- XXX Toy
- Zango

Not all forms of adware are harmful but there are many examples of adware software that are also spyware or malware. As you saw from the above list some of the programs were repeated from the spyware list.

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware (a class of malware designed specifically to automate financial crime) and other malicious and unwanted software. Sometimes, annoying pop up will appear out of nowhere to direct you to some sales sites. Sometimes email spams will automatically be sent from your system. Adware and spyware progress to a malicious state if it starts to affect the use of your system actively instead of just showing you passive advertisement.

The best-known types of malware, *viruses* and *worms*, are known for the manner in which they spread, rather than any other particular behavior. The term *computer virus* is used for a program which has infected some executable software and which causes that software, *when run*, to spread the virus to other executable software. Viruses may also contain a payload which performs other actions, often malicious. A *worm* (a self-replicating computer program), on the other hand, is a program which actively transmits itself over a network to infect other computers. It too may carry a payload.

These definitions lead to the observation that a virus requires user intervention to spread, whereas a worm spreads automatically. Using this distinction, infections transmitted by email or Microsoft Word documents, which rely on the recipient opening a file or email to infect the system, would be classified as viruses rather than worms.

Malware includes a wide array of nasty batches of code that can wreak havoc to your computer, your network and even the Internet itself. Some common forms of malware that might turn your computer into a zombie include:

- Computer viruses - programs that disable the victim's computer, either by corrupting necessary files or hogging the computer's resources
- Worms - programs that spread from one machine to another, rapidly infecting hundreds of computers in a short time
- Trojan horse - a program that claims to do one thing, but actually either damages the computer or opens a back door to your system
- Rootkits - a collection of programs that permits administrator-level control of a computer; not necessarily malware on its own, crackers use rootkits to control computers and evade detection
- Backdoors - methods of circumventing the normal operating-system procedures, allowing a cracker to access information on another computer
- Key loggers - programs that record keystrokes made by a user, allowing crackers to discover passwords and login codes

Examples of Malware:

- GAIN (more info found here as well)
- webHancer (need to scroll towards the bottom of page)

- ISTBar (need to scroll towards the bottom of page)
- searchWWW
- HuntBar (more info found here towards center of page as well)
- AccessPlugin (scroll towards the bottom of the page)

More information on Adware, Spyware and other unwanted malware can be found by click here.

Prevention, Protection, and Removal:

There are many programs out there that will help with the prevention, protection and removal of spyware. But sometimes spyware gets so deep into your system that even these programs cannot fully get the spyware removed, as they have just removed the spyware that is visible, some spywares like to hide deep in the computer making it extremely difficult to find and remove. Other programs have the ability to get deep into your computer to help remove the spyware, but they are some complicated that even the most savvy computer person still has problems using the program.

At NalTech our experienced team of IT professionals are fully trained to the depth of spyware prevention, protection and removal. Our IT professionals not only use those complicated programs to remove the spyware but they also go deep into your system to remove every last trace of the spyware manually.

Another step we take at NalTech is we try to insure that your computer remains spyware free. We will setup programs to automatically run and scan for spyware on your system. We will also insure that if traces of spyware are found that they will also be automatically removed, without you even having to touch a button. We believe no spyware is too difficult for us to remove. Contact us today to let us help you with your spyware problem(s).

Sources:

- http://arstechnica.com/security/news/2004/11/malware.ars
- http://computer.howstuffworks.com/spyware.htm
- http://computer.howstuffworks.com/virus.htm
- http://en.wikipedia.org/wiki/Crimeware
- http://en.wikipedia.org/wiki/Malware
- http://en.wikipedia.org/wiki/Spyware
- http://news.zdnet.com/2100-1009_22-5535478.html
- http://www.bradenton.com/mld/bradenton/business/10650790.htm
- http://www.cexx.org/adware.htm
- http://www.forbes.com/technology/enterprisetech/2005/01/17/cx_ah_0117spysales.html
- http://www.mercurynews.com/mld/mercurynews/business/10664196.htm?1c
- http://www.pcworld.com/reviews/article/0,aid,119300,00.asp
- http://www.spywareguide.com/
- http://www.winnetmag.net/SQLServer/Article/ArticleID/45091/45091.html