



Digital Garbage

Dealing with and understanding **spyware, adware, malware, viruses, and bad programs**

The average non-geek consumer buys a Dell PC, follows the instructions for setup, and is happy with his or her new purchase. The machine runs smoothly and is lightning fast with everything it does. A few months pass, and over this time the user begins to notice something. His nice new machine is not as fast as it was out of the box. It takes longer to start it up and to shut down. There are weird advertisements popping up and then closing instantly. The homepage of the internet browser goes to some weird search site that doesn't even search.

All of these problems can be attributed to spyware, viruses, and other digital garbage we all accumulate over time if we are connected to the Internet. Such garbage often causes significant performance issues, not to mention the invasion of your privacy. At the very least, random pop up ads and toolbars in your browser get *very* annoying. The good news is we do not have to tolerate it. If you are here reading this guide, you are one step closer to understanding an important step in PC maintenance. Alternatively, you may also be here because you have one of the problems listed above. While preventative maintenance is the key to avoiding major problems, knowledge of what you are dealing with is just as important.

What is this stuff?

Spyware – Programs designed to collect information about your web browsing habits and anything else you use your computer for. The information is then transmitted back to its source, where the data is processed for whatever purpose. They generally come disguised inside of another program, and the user is never told. Certain peer-to-peer file sharing clients were known for having spyware. Some cookies are spyware, as they can track what you are doing.

Adware – Programs designed to shove advertising in your face. This can be as mild as AOL's Instant Messenger, to as obscene as a barrage of fifty pop-ups happening at random. Adware is common with "free" programs. Sadly, many people simply don't care about adware (just look at the amount of people still using AIM) and this shows corporations that this method of advertisement can be effective.

Malware – Short for "malicious software". This is a general term used to describe anything that is loaded on your computer, with or without your consent, and causes undesired operation. I personally use this term broadly to describe spyware, adware, viruses, and crappy programs.

Viruses – sneaky programs designed to do many things, mainly to spread to other systems. A virus can do just about anything once it has installed itself on a system. It can sit in memory and cause your computer to do strange things, or just be really slow. Some are more difficult to remove than others, so the key is to prevent yourself from ever getting one.

Bad Programs – This is more of my opinion, but I've found that poor programming can cause a lot of problems. Sloppy programming can cause system errors, or slow your machine significantly. It is important to identify bad programs and replace them with something better.

Examples

There are so many different types and variants of malware that is nearly impossible to cover it all. I will go over some of the more common ones I have come across.

GAIN/Gator

The Gator Advertising Information Network is self-described to be a helpful application. It sits in the background and will fill in forms and save you money. Not only is form-completion unnecessary now with browsers having the same feature, but this program is spyware. It tracks your browsing/buying habits for its own purposes. Anyone concerned with their privacy wants to get rid of this. It comes bundled with some software, or is a stand-alone download from a sleazy website. (<http://www.pchell.com/support/gator.shtml>)

CoolWebSearch

This is considered a Trojan horse, and can sneak into a system by exploiting a bug in Internet Explorer. This means that all you need to do is go to a sleazy website, and it will install itself. (<http://www.spywareinfo.com/~merijn/cwschronicles.html>)

WildTangent

This is designed to allow you to play 3D games over the net. It is not technically spyware, but it does gather system information and update itself, both without asking. I personally don't like programs doing things that I did not authorize it to do. (<http://www.pchell.com/support/wildtangent.shtml>)

BargainBuddy

Adware that pops up ads based on keywords, and uses a BHO to intercept 404 errors, and displays its own window. (<http://www.pchell.com/support/bargainbuddy.shtml>)

HP, Creative, etc. (Bad Programs)

This is, again, my opinion. I have found that software included with Hewlett Packard printers include a bunch of things that no one needs for their printer to function. All your computer needs is a driver - nothing more. HP installs its own program that loads and sits in the background, with an icon in the system tray (icons in the bottom-right corner next to the clock). This is not necessary, and only slows your system. Creative's software is similar, all you need is a driver, and no extra software. Yet it proceeds to install all these things that it thinks you need. I actually had to forcibly remove these programs, because they were trying to reinstall themselves upon restart (there were other problems). It would get stuck halfway into its reinstallation, and would not terminate. Removing all these extra bad programs helped the system perform *much* better. Why companies make these programs is a topic for another paper.

What about these toolbars in my browser?

A lot of people use the Google toolbar because it is decent at blocking pop-up windows. The Yahoo toolbar will do this also. There are others that load seemingly without a decision from you, and are impossible to get rid of. These are called BHOs (Browser Helper Objects), and usually do more harm than good. MySearch is an example.

These days both Internet Explorer and Mozilla both include built-in popup blocking. Mozilla even has a Google search box built-in. Toolbars are unnecessary anymore. Uninstall them and update to the latest browser versions.

But advertisements aren't bad, are they?

If you ask me, it's the scum of the earth. Have you noticed that TV advertising has taken precedence over the program you are trying to watch? Turn on SpikeTV or any cable channel and watch it for an hour (if you can stand it).

Even while you are watching the show, advertisements are crawling at the bottom, or are taking up the bottom right-hand quarter of the screen. Not only that, but every four or five minutes the show you are trying to watch is interrupted for five or six minutes of *more* advertisement. Their goal is to get inside your mind and make you want to watch/buy whatever they are advertising.

The Internet allows advertisement to go a step further. What they want more than anything is for you click on their advertisement. If you do, that earns them a fraction of a cent that, when combined with all the other misguided people clicking on the same advertisement, earns them enough money to continue doing it. This also will continue to perpetuate the theory that these sleazy advertisements are more effective than they really are. If nobody ever clicks on any advertisements, they will become worthless and hopefully will die out.

Where does it come from?

The primary sources for digital garbage are sleazy websites, “free” programs or services, and peer-to-peer programs. If it all possible, one should avoid all three.

Sleazy websites

Porn sites fall under this category, but pretty much any website that asks you to install something is a sleazy site. Any site worth your time will NOT ask you download a “plugin” or any other “special” software. These sites describe these programs very vaguely, betting on the ignorance of its visitors. If the software gets downloaded, they get their money.

“Free” programs and services

Any program that asks you or, better yet, requires you to install “extra” programs is not worth your time. AOL’s Instant Messenger a free service but the client software is ad-driven (or should I say ad-ridden?). It also asks you to install WildTangent, which we mentioned above. The AWS WeatherBug is also garbage that will slow down your computer (and is also ad-ridden). Be aware that there are plenty of truly free programs. These are made by freelance programmers writing software for the greater good. Some of these I even list as great tools for removing spyware. All they ask is a small donation if you like what they make.

Free screensavers, online games, emoticon packs, flash animations, and similar things are all potential delivery methods for spyware. When you go to install anything, read the End User License Agreement (EULA). Check for any mention of company names that aren’t affiliated with what you want to install. Then, use the ‘Custom Install’ option in the setup program. If there is not one, or it doesn’t give an option to not install the spyware, then you do not need the program. Delete it and move on. (<http://www.pcpitstop.com/spycheck/kids.asp>)

Let’s look at one in particular; AOL Instant Messenger. Bundled along with it is WildTangent (described above). They also want you to install the AWS WeatherBug. I’ve done some research on this, and as near as I can tell, it is not spyware. It has advertisements though, and that’s why they want you to install it. If you click on just one single ad, it has done its job. Because of this sleazy practice of bundling adware, I don’t use AIM.

If you’re like me and do not want to support companies that try to cram spyware down users’ throats, than I suggest you try the Basic version of Trillian. This is an instant messaging client that is compatible with AIM, Yahoo Messenger, MSN Messenger, ICQ, and IRC. It is a superior product, and is free. The full version offers more functionality for a cost, but it is well worth it. (<http://www.trillian.cc>)

In general, if a program is free, read the EULA. Check for anything mentioning 3rd party software (software from a company other than the one the main program came from. GAIN is an example). Get the name of the program or company of this 3rd party software, and Google it. Look for any mention of people having trouble with it, or any mention of spyware. If you find any, don’t install that software. Also, usually any program under the GPL license agreements are from the good guys, and is probably safe. The GPL is a General Public License used by UNIX programs and many free software packages.

Also, when going through the install process, DO NOT just click 'Next' and 'OK'. Read what you are saying okay to. Uncheck anything that doesn't sound like what you are wanting to install.

P2P File sharing

It started out as an interesting idea, but has become a breeding ground for viruses. Not only that, but you've got the All Seeing Eye of the RIAA cracking down on small-time users (don't even get me started on that). Stop using Kazaa, WinMX, etc. There is not even a positive side to getting music and movies from P2P networks, because generally the people ripping and encoding the files are amateurs. The resulting product they make available is either of an unacceptable bitrate, and/or is full of pops and skips. Take some time to learn how to use IRC, and you'll be much better off. You won't be safe from viruses, and there are still some amateur encoders, but the overall experience is much better if you are patient. Instant gratification will get you into trouble. (Or you could buy tons of CDs from eBay for dirt cheap).

Preventing the trash

There is no such thing as a free lunch. If it is too good to be true, it probably is. These are both clichés, but they need to be kept in mind. If it is a free program or service, somebody is paying for it. Somebody is paying for the server to host it, paying for having it programmed, paying for testing, and paying for their time in general. Some charge a licensing fee and/or cripple the program until you pay. Others load spyware to earn their money, and then pose as a company providing a free service for the greater good. And then there are the good guys; the freelance programmer's and companies providing programs for the greater good, with no strings attached. All they ask is that it be used for personal use only, and that you donate some money to them if you find the program useful.

Your lines of defense

Anti-Virus Programs

You need a virus scanner. That's all there is to it. If you don't have a good one, you are asking for problems. I personally use Norton Antivirus 2005, and it works great. It can be bought at the store for \$40 and you get free updates for one year. Don't bother buying Systemworks, just get Norton Antivirus 2005 (or the latest version).

There are free options that I am currently experimenting with. Grisoft offers a free version of its AVG anti-virus program. As long as you keep any anti-virus package up to date with the latest definitions (the files that tell the virus scanner what to look for), then you should be in good shape. Turning on Automatic Updates (if you have the option) is a good practice if you are forgetful.

Anti-Spyware Programs

A recent development is the release of Microsoft's Anti-Spyware package. It is still in beta, but shows great promise. It sits in the background and monitors for spyware activity. It will run a scheduled scan whenever you specify. It is very similar to an anti-virus program; run it in the background and let it work for you.

Having an arsenal of other antispyware programs already downloaded can be helpful if you are badly infected and can barely connect to sites to find these tools. A list is given later in the article, and is available on wannafork.com, under spyware tools.

Firewall

There are two types: hardware and software. A hardware firewall would be a router. This is a box that sits between your computer and its connection to the Internet. It could be characterized by a bouncer at a nightclub. If you haven't been invited, you're not getting in. Any unsolicited sources that try to get into your computer are usually stopped by a router. A router will help stop worms from getting into your system, and well as any other scum looking for an "open door".

A software firewall is a cheap alternative to a hardware firewall. It is a piece of software that sits in the background and monitors all incoming and outgoing network traffic. If it sees something it doesn't like, it will block it, or ask you what you want to do. One of the problems here is the human element; you may click okay to something that is not. The other problem is that any malicious code is already half-way in the front door of your computer, and could slip by. Windows Service Patch 2 turns on the Windows Firewall by default, and this is adequate for most users. I personally use a Linksys router and have Norton's Worm Protection turned on (built into its anti-virus package). I have no problems. It sits in the background and never bothers me.

Windows Updates

New security exploits are discovered all the time, and subsequently new patches are developed. It is important to stay current with these patches. Turning on Automatic Updates should keep you current.

Since we are talking about security holes and exploits, there is a definition I would like to clear up. Many people (mostly the Media) do not understand the difference between hackers and criminals. Hackers find ways around security and generally explore the inner workings of many types of systems. Their goals are purely educational, or for the greater good of more secure systems. A criminal will use similar probing techniques to gain access to systems for personal gain. To spread a virus (and subsequent fame), or for espionage, or to just cause general destruction. It is the goal of the true hacker to find exploits and holes before a criminal. Many sources portray hackers in a bad light, when in fact they are the reasons we have new security patches and version of software. Innovation is spurred on by the hacker community.

Browser Choice

This is minor, but it is important to consider. Since most people use Internet Explorer, spyware, malware, etc. is targeted to the vulnerabilities of that certain browser. Using a different browser can help you avoid certain annoyances than only IE users have to face. I personally use Mozilla Firefox. In switching to this browser, I immediately noticed a lack of extreme popups, and less spyware was getting through. It also has a smarter interface, and is definitely worth a try by everyone. You can transfer your bookmarks from IE to Mozilla automatically, after it is installed.

Taking out the trash

Removing spyware is usually an easy process. The problems come in the form of stubborn hijackers, or viruses that take some work to destroy.

The Basic Tools

Ad-Aware SE – (lavasoftusa.com) This is the free version of Lavasoft's fantastic utility. This will find and remove the majority of spyware.

Spybot S&D – (safer-networking.org/en/index.html) I use this before Ad-Aware. It will find some things Ad-Aware won't, and both are great to have

AVG Anti-Virus – (grisoft.com) They offer a free anti-virus program. If you don't want to spend any money on anti-virus programs, this would be an option to consider.

Norton Anti-Virus – (Symantec.com) This is, in my opinion, the best anti-virus software for your money. It costs around \$40, and is second to none in finding viruses. It also finds some malicious adware. Upon switching to Norton from McAfee, I have had **no** problems. Buy this today. (This would replace AVG; you need either one or the other.)

Things to Consider

There are some "anti-spyware" utilities out there that **are** spyware themselves. Don't trust those pop-up windows saying "Click here for a free spyware scan!".

Have a backup of anything you would want to keep. Ask yourself “If my hard drive crashed, and I lost all the data, what would I be really upset about?” Make a list of the things that matter to you and **make a backup**. CD-Rs are dirt cheap, and just about everyone has a CD-R/W drive these days. Use your favorite burning program (Nero works fine, and Windows XP even has built in burning support) and make backup CDs. You do not need to back up system files; those are reloaded for you from your Windows XP Setup CD. The same goes for Office, and any other programs. If you have installation executables for your favorite programs, back those up too. Don’t forget to check the My Documents folder for anything that may have been saved there (I personally do not use that folder, but some programs like to put stuff there.)

The minimalist approach works well when you are trying to run a tight ship with your computer. Run as little as possible and only what you need. I personally have three icons in my system tray (more are actually running, but this is a good measure). The more you have running in the background, the more potential for slowdowns and/or crashes. When you install a new program, there is no reason for it to run on startup and sit in memory. An example of this would be Quicktime. There is absolutely no reason for it to be running a “manager” when I need to play a video, **I’ll** open and run it. Consider running as little as possible in the background.

Scan For Viruses

The first thing to do is to check yourself for viruses. These are far worse than any spyware program, and need to be dealt with first. Make sure you download the latest update before doing a scan.

Running a scan is as easy as clicking the button that says ‘scan’. If you have multiple hard drives, click something akin to ‘Scan my computer’ or at least make sure that it is set to scan both a C: drive and a D: or E: drive. Scanning optical drives is not necessary, unless you have reason to believe it to be a suspect.

Scan for Spyware

Also, this is very easy. Just install any one of the above mentioned tools. If you were to start with Spybot S&D, for example, you would install the program, and then follow the directions. Let it make a restore point, and also allow it to find all of its updates. Then run a scan, and walk away. It will take awhile, depending on your system. Review what it finds if you like, then make sure all the items have a check mark next to them, and click ‘Remove selected’. Follow the instructions, and restart if it asks you too. It may run on startup also. For more stubborn spyware, you may have to use additional tools.

This is generally how all antispyware programs operate; install first, then update, then scan, then remove items. Repeat weekly.

Dealing with Stubborn Spyware

Sometimes, antispyware programs can simply not remove some things. This is where things get tricky and you have to do some work. I first thing I would do is check the ‘Add/Remove Programs’ applet in Control Panel. While this rarely works, it can give you an idea of all the crap that is installed on your system. It helps if you know what software you have installed, and what manufacturer it is from. Unfortunately, not all legit software is labeled correctly, and so it can be mistaken for unwanted software.

Once you have tried to remove the suspected spyware (and it probably didn’t work, but made you think it did) it is best to go into the Program Files folder and check to see what is still there. Even though you have uninstalled a program, it tends to leave remnants (also in the registry, but that’s another issue). Just deleting the whole folder proves effective.

It helps to know as much about the spyware in question as possible. Your best bet is to put the name of whatever Spybot S&D, Ad-Aware, etc. found into Google and do a search. Eventually you will likely come across some helpful forums with people trying to remove the same thing as you. For more infamous spyware, you may find whole pages dedicated to the removal of such scum.

Conclusion

As you can see from looking at this document, the key to dealing with malware is prevention. Keep it from loading itself, and avoid spyware-laden applications. Be aware of anything you are installing, as you may be inviting it in. Keep yourself updated with the latest security patches, the latest virus definitions, and run a spyware scanner regularly. Plenty of things out there are free and good, but many (sadly, the popular ones) applications are out to make a quick buck by way of spyware and adware.