

That “bleeping” computer!

Mondays and Fridays are usually the most interesting days in my line of work. I say this because it is on these days that most phone calls coming from my clients begin with the phrase, “that bleeping computer!!!” Lately, I have noticed a rather substantial increase in the number of those calls. Most of them are the result of a computer infected by “Spyware”, “Adware” or some other malicious program. Oh yes, Spyware! Installed on your computer, but mostly without your consent, it monitors or controls your computer use. It may be used to send you pop-up ads, redirect your computer to websites, monitor your internet surfing, or record your keystrokes, which could lead to identity theft. Spyware is one of the biggest threats to your privacy and the security of your data. It's also the number one cause of system slowdowns because it uses precious system resources. So, exactly what is “spyware”? In a nutshell, it is a program that either sends information about you and your internet browsing habits to a remote location like a data warehousing company. It could also be sent to a potential thief looking to steal your data such as bank access numbers, passwords or credit card information. Spyware can also place unwanted ads on your computer, change your homepage, install new and unexpected toolbars, and place unwanted icons on the system tray or your desktop or any combination of the above tasks. A side effect of spyware is sluggish or downright slow performance of your system, usually combined with frequent system crashes or other unpredictable behavior. But how does spyware get on your computer? There are several ways for that to happen. Sometimes, it is automatically installed by the website you are surfing. This method is typically used by sites serving adult content, but not only. For example, one of my clients infected her computer while surfing web sites about wedding planning and cake recipes. Another way to get infected is to download “free” software like “Weather bar” or “Bonzi Buddy” from the web.

How can you protect yourself?

- **NEVER, never, (I did say “never” didn’t I...) operate your computer without a good antivirus program.** My favorite is TrendMicro, but there are many other programs available, like McAfee and Kaspersky Lab. Always use a hardware firewall installed between your computer (or your network) and the internet. If you don’t have hardware firewall installed, you should install it as soon as possible. A good quality firewall can be installed for around \$80 to \$90. Without a firewall, your computer can become part of giant network, accessible by anybody with a bit of computer know-how. Using a computer to access the Internet without a firewall can only be compared to parking your car with keys in the ignition, leaving the car door unlocked and then coming back hoping your vehicle is still where you left it. You wouldn’t do that, would you? Yet, I see networks and computers without installed firewall every day?
- **Keep your software, including the operating system up to date.** Make sure that the virus definitions are always up to date, as new forms of spyware and viruses are released every day. Outdated software, especially Windows itself, can be a major indirect cause of infections.
- **Download only from sites you know and trust.** It can be appealing to download “free” software like games, peer-to-peer file-sharing programs, customized toolbars, or other programs that may change or customize the functioning of your computer. A blinking banner informing you that you have won something (we all have seen those) doesn’t mean you won anything and they will tell you that after you enter your email and maybe your home address. They will also tell you that by giving them your address you have agreed to receive fifty emails per day offering products ranging from “penile enhancements” to “no prescription required medications” to “unbeatable stock tips”. “Free search bars” or “free

weather bars" or "free smiles" are just an excuse to self-install all kinds of nasty programs on your computer. Be smart, think about what you do online.

- **Don't install or open any file without knowing exactly what it is.** A video or image file you are about to open or download, may actually be disguised spyware or virus.
- **Minimize "drive-by" downloads.** Make sure your browser security setting is high enough to prevent unauthorized downloads.
- **Think before you click.** This sounds trivial, but the best defense is still an informed user. Don't click on popups promising to increase your computer performance. Don't open suspicious emails. Don't click on banners offering free icons, or weather bars, etc. There is no such thing as free lunch; this stuff is almost always infected with spyware or worse.
- **Don't click on links in unsolicited emails that claim to offer anti-spyware software.** Some software offered in spam actually installs spyware.
- **Prevent access to your computer by unauthorized persons.** Some people have very funny browsing habits, you should ask them to practice them on their own machine. Protect your computer with a password and set it to activate automatically.
- **Do not use any of the file sharing programs.** Downloading a pirated movie, music or software can end up costing you much more than the money you think you will save by not buying it.
- **Do not open any email attachments unless you know and trust the sender.** Although note should be made that some unscrupulous companies have created a software able to "spoof" an email address. Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into executing a file or releasing sensitive information (such as passwords).
- **Don't use Internet Explorer unless you absolutely have to.** Internet Explorer is the most popular browser, meaning that most people who program spyware target Internet Explorer and its many security holes. Avoid a lot of problems by switching to a different browser whenever you can. Alternate browser like Firefox and Opera are easy to use and offer advanced browsing features which Internet Explorer lacks.
- **Run spyware scanning programs on a regular basis.** Install a good anti-spyware program and run it at least twice a week. Update the program's definition files frequently and always before running it.
- **Last, but not least, always backup your data.** There are many inexpensive ways to do that, including backup to a different drive, computer, CD or DVD. The best way to protect your data, in my opinion anyway, is to backup your files to a remote location, away from your office. This way, your data is protected in case of fire or burglary. Most importantly, remote backup can be setup up to start automatically, without any user interaction. It is very inexpensive, reliable and there are no worries about tracking, labeling and storing the disks, tapes or other devices.

How to remove spyware from your computer?

Depending on which form of spyware your computer has been infected with, it can be very easy or almost impossible to remove it. Here are the first steps you should take before attempting to remove spyware.

- Usually, programs used for spyware removal are rather safe, but back up your data, even if you do regular backups already. Also, some forms of spyware can embed themselves within critical system files, removing them can damage your operating system installation.
- Turn off system restore within Windows. It can be very disappointing to spend all the time and effort to remove spyware, only to have your operating system put it back from a previous restore point. (Instructions on how to turn off system restore can be found in the Windows help file.)
- Download, install and run one of the many available spyware removal programs. AdAware by Lavasoft is a good one, and can be downloaded for non-commercial use free of charge from

<http://www.lavasoftusa.com/software/adaware/>. Another one is Spybot or Microsoft AntiSpyware, available from many sources, also at no charge. Those programs should be able to remove most of the unwanted spyware.

- In some instances, especially where the system's registry has to be modified, you will have to call an experienced and knowledgeable computer technician for help. I stress the words "experienced" and "knowledgeable" – sometimes, the so called "computer geek" or "nerd-on-wheels" can create irreversible damage to your computer system, including loss of data. Being thrifty at this point is not likely to pay off.

According to "Business Week" magazine, consumers have strong opinions about spyware. "If I ever meet anyone from your company, I will kill you," a person who identified himself as James Chang said in an e-mail to Direct Revenue last summer. (Direct Revenue is \$100,000,000 a year company, responsible for a large portion of spyware related problems) "You people are evil personified," Kevin Horton wrote around the same time. "I would like the four hours of my life back I have wasted trying to get your stupid uninvited software off my now crippled system."

By the time you combine the existence of spyware with the never ending flow of spam (unsolicited commercial e-mail), one question begs to be answered. Why do they do it? The answer is actually very simple. Money. A lot of money. A company controlling access to 10 million computers can make about \$100,000 a day. How does it work? How do they make money on spyware or spam? Imagine this, after your computer gets infected, you will be forced to click on a "pop up" window, an advertising banner or your Web searches will be redirected, controlling the results you see and making your search engine basically ineffective. Each mouse click on the controlled banner, website or search is counted and stored by a web based database system such as Clickbank or Doubleclick. Based on that data, a payout is made to the person or company that planted the spyware on your computer. The amount varies from \$0.01 to more than \$1.50 per click, multiply that by the number of infected computers, and the revenue generated is quite substantial. Simply because of the amount of money involved, it is safe to assume that spyware and spam are here to stay, but you can prevent it from infecting your computer with the right knowledge.