Things You Must Do To Protect Your Computer At Home and At Work

Philip Siddons

By way of introduction, **spyware** installations on computers that go on the Internet have become a billion dollar expense across the country. Sooner or later, **viruses** and **spyware** will accumulate on your computer and you will likely lose Internet access; your computer will slow down to a crawl and ultimately you will have to have your hard drive reformatted. All of your data will be lost (unless you backed it up to CDs or some other backup means) and all of your software will have to be reinstalled. This is a huge time-consuming and financially costly nightmare. Here is what is happening.

Without our knowing it, merely visiting certain websites on the Internet exposes our computers to automatic installation of malicious software on our PC. The software can track what websites we visit, what products we purchase, copy our charge card information and keyed-in passwords, etc. It's called *identity theft*. It also ruins the computer. With all of the tracking and automatic information gathering software services that automatically gets installed on your computer, in time, your computer will slow down to a crawl and vital system-required software (that enables internet access and basic computer functioning) will be erased. The aggressiveness of the malicious software our computers are exposed to when on the Internet is so bad that the following list shows the minimum requirements for your computer.

1. You must have current **anti-virus** software always running on your computer and you must have it automatically check for and install updates from the vendor source of that software. *The Shield* (PC Magazine's highest recommended and most effective antivirus detecting and removal software); or Norton's Symantec antivirus or McAfee antivirus programs are a must.
2. You must have **anti-spyware** software always running on your computer and you must have it automatically check for and install updates from the vendor source of that software. *Spyware Doctor* (PC Magazine's highest recommended and most effective spyware detecting and removal software available) or a similar high-level anti-spyware product is a must. *Spyware Doctor* found and removed about 7,000 infections on the staff computers at Buffalo Urban League's Genesee Street office alone.
3. You must have a **hardware firewall** (**or router**) between your DSL or Cable modem and your computer
4. You must have your **Windows XP firewall turned on**
5. You may want to, additionally, **use a software firewall**. The *Comodo* firewall is rated by PC Magazine as the best and it is free. *Zone Alarm's* firewall is also right at the top of the list but it costs around $30.

Once you are on the Internet or in your email program, here's some **standard safety tips**:

- Don't open any email from people or organizations you don't know. Erase them. If you're fairly sure they are spam emails, right-click them (in *Outlook*), choose Junk Email and choose Add Sender to Blocked Senders List. Definitely don't open any attachments or click on any links in emails from people you don't know. You'll end up on somebody's server in Asia and they don't regulate what they can do to your computer.
- Don't respond to any email messages from PayPal unless you have an account with them. If you do, make sure the message has your name at the top. If not, Add the Sender to blocked Senders List.
- DO NOT download any "free" software like Weather Bug, free tool bars, software that claims it will fix viruses or spyware. Definitely do not install any software you didn't buy from the store or bought on line with your money. Even if your lifelong friend wants to give you a great software for free, *don't* install it on your computer for any reason. Keep your software "clean" (or legitimate). If your life-long friend becomes offended, make new friends elsewhere.
- Don't go to internet game sites. This is probably an impossible thing to ask of a teen but game sites and other popular teen websites are loaded with malicious viruses and spyware. Same thing goes with music exchange download clubs. If your computer does go to these sites, or worse, to porn sites, you computer *will* encounter malicious software and the only chance of your computer's survival is if you have all five of the above-mentioned safeguards in place but even then, it is still risky. Ask yourself, "Is this particular site really worth risking everything on my hard drive and all the expense of reformatting the hard drive and then having to load all the software back on it again?" □