



The epidemic of unscrupulous web pages, links, emails, and hidden downloads pose a serious threat to your computer and its data - from viruses to spyware that can transmit your account names and passwords. Most of these incidents are innocent, intended for advertising or driving traffic to a site, but they do slow down your internet connection dramatically. You can prevent a majority of this from happening by following our recommendations.

AntiVirus Software - We recommend Norton AntiVirus Corporate Edition. From our experience, this version has no known bugs in it and it appears to handle all virus infections better than any other vendors' products, including other versions of Norton Antivirus! Make sure you update your virus definitions at least once every 2 weeks.

Firewall – If you are using a broadband internet service (DSL, cable, ISDN, etc.), you should have a router installed between incoming cable and your PC or network. Most of the broadband routers on the market today also include basic firewall protection. This makes your system 'invisible' from hackers who surf the web looking for "open" ports on connections that are always on. Dial-up connections do not typically require this as they are 'on-line' for only short periods of time. This causes the PC address on the internet to change continually making it almost impossible to hack.

Software Firewall – This is software that installs on your PC and monitors incoming and outgoing network (internet) activities. They will block unwanted access, however, they do require some configuration for your particular environment. We recommend ZoneAlarm.

Spyware Checker – **LavaSofts' AdAware** is the most popular software program to quickly check for and remove most spyware.

Spyware Blocker – We use **Spybot Search & Destroy**. It is available as a download on the web, however, it is more advanced and therefore caution should be taken. We do not recommend keeping this program memory-resident all the time.

Browser – Your browser software is most likely Microsoft's Internet Explorer, as it is currently used by about 63% of all web surfers. It is also the most susceptible to intrusion. You can eliminate many of the problems by switching to Netscape Navigator or Opera browsers. They are both available free of charge on the web.

If you insist upon using Microsoft's Internet Explorer browser, you need to restrict some of its settings as the factory defaults will leave you vulnerable. Do the following;

1. In **Control Panel**, go to **Internet Options**. Click the **Advanced** tab. Uncheck **Enable install on demand**. Click **apply**. This setting will cause a dialog box asking for your permission to download something. You should read the description and/or agreement carefully and click the "Cancel" or "No" button unless you're sure that it's something that you have requested. You could be agreeing to the installation of spyware, advertising pop-up or to change your start page to something else (usually a pay-per-click page).
2. In **Control Panel**, go to **Internet Options**. Click the **Security** tab. Click the **Custom Level** button. On the item **Download signed ActiveX controls**, check the **Prompt** selection. On the item **Download unsigned ActiveX controls**, check the **Prompt** selection. On the item **Initialize and script ActiveX controls not marked as safe**, check the **Disable** selection.

If you suddenly see an additional search bar on your browser, your PC has been infiltrated or hijacked.

POP-UP Blockers – These are not required or recommended. If you visit 'normal' sites, pop-ups are typically not an issue. If you are experiencing many pop-ups, either you are frequenting undesirable sites (adult, advertising, etc.) or your PC is infected with spyware, which should be removed. Pop-up blocking software typically has a 'high overhead' and will slow down your internet throughput.

Web Surfing – If you stick to visiting only legitimate sites you are familiar with, your risk for problems is minimized. Do not signup for any online free offers from any organization you are not familiar with. These sites are notorious for silently downloading and installing spyware on your PC while you are consumed with filling-out their 'forms'.

Watch out for fake or "spoofed" sites. There are regular emails circulating for ebay, banks and other services warning you that you must login to your account to verify your personal information. These are NOT the real sites, but a temporary look-alike page designed to steal you name and password or other information.

If you are ever want to verify the true identity of a web page, enter the following java command into your browsers' address bar, then press enter.

javascript:alert("Actual URL address: " + location.protocol + "/" + location.hostname + "/");

Finally, look at your Add/Remove Programs on occasion and remove any suspicious programs.

Today's Top SpyWare

- 1) KaZaA.com – Free (copyright infringing) music downloads. In order to download the music, you must first download and install a suite of software containing a handful of devious spyware programs, one of which is item #2 below. To read the history of KaZaa, click [here](#).
- 2) Ezula – The nastiest spyware component included with the KaZaa download. Removal can permanently damage your Windows installation!
- 3) GATOR (GAIN) – A spyware program installed when you sign up for some money saving offers on the web.
- 4) NetPal – A Browser Helper Object (BHO) that infiltrates your browser and can redirect your web pages or information to other sites.
- 5) n-CASE (msbb.exe) – A spyware program that downloads and displays advertisements. It also tracks Web-browsing habits.
- 6) DoubleClick – One of the largest online marketing agencies anxious to gather web trends.

It is important to realize that these sites are currently recognized and the leading offenders of dubious internet practices. As they become widespread and therefore well known, they are eventually replaced by other names and schemes and new methods to disguise their identity and add-ons to thwart removal. You can see that this is a moving target that needs constant attention.

NOTE: This information is intended for IBM-compatible PC's and does apply to Apple computers. The Apple MAC operating system is different from Windows, and is much less susceptible to threats. Different hacker codes and procedures would be also be required. Additionally, since the Apple market currently makes up only about 9% of the total PC market, there is not as much incentive for hacking or software development.