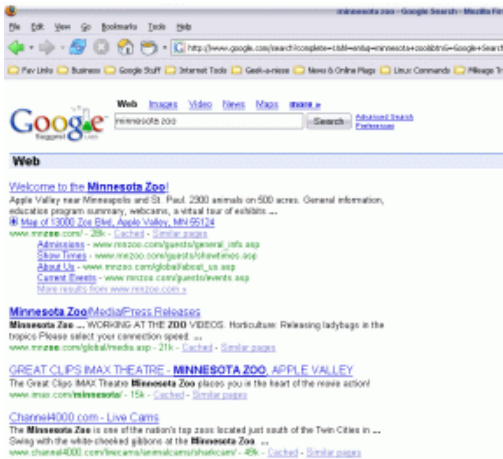
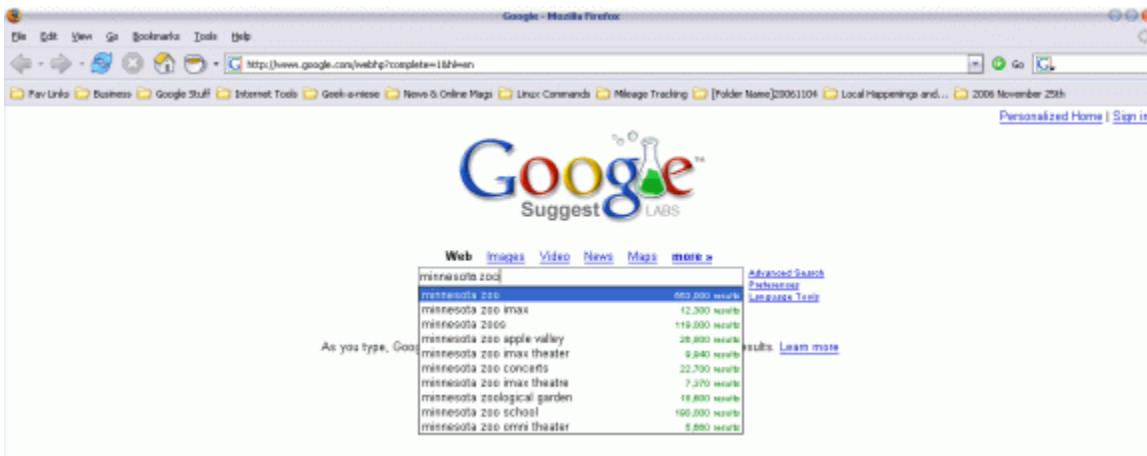


## Spyware Prevention Checklist – Tips for safe computing at work

- When searching for things, the safest way to go to a website is to type the name of the website into the search engine box rather than typing directly into the address bar at the top.

Google Suggest

<http://www.google.com/webhp?complete=1&hl=en>



The first result is website for the Minnesota Zoo.  
Google is the **BEST** search engine for accuracy, layout and speed.

### [Welcome to the Minnesota Zoo!](#)

Apple Valley near Minneapolis and St. Paul. 2300 animals on 500 acres. General information, education program summary, webcams, a virtual tour of exhibits ...

[+ Map of 13000 Zoo Blvd, Apple Valley, MN 55124](#)

[www.mnzoo.com/](http://www.mnzoo.com/) - 28k - [Cached](#) - [Similar pages](#)

[Admissions](http://www.mnzoo.com/guests/general_info.asp) - [www.mnzoo.com/guests/general\\_info.asp](http://www.mnzoo.com/guests/general_info.asp)

[Show Times](http://www.mnzoo.com/guests/showtimes.asp) - [www.mnzoo.com/guests/showtimes.asp](http://www.mnzoo.com/guests/showtimes.asp)

[About Us](http://www.mnzoo.com/global/about_us.asp) - [www.mnzoo.com/global/about\\_us.asp](http://www.mnzoo.com/global/about_us.asp)

[Current Events](http://www.mnzoo.com/guests/events.asp) - [www.mnzoo.com/guests/events.asp](http://www.mnzoo.com/guests/events.asp)

- Never download software to your workstation or desktop from the Internet, no matter how helpful or interesting it may appear. Get approval from your manager or the IT person first. Even innocuous toolbars and nifty utilities can be packed with unwanted spyware. Be especially wary of file-sharing programs, which you shouldn't be using in the office anyways.

- Stay away from any questionable sites, including pornography, gambling, hacking or other off-beat sites. But you shouldn't be, in any case, visiting these types of sites at work either. At most companies, you could be terminated for doing so.

By Adria Richards

---

- Whenever an unwanted, or unexpected, pop-window appears, shut it down by immediately by clicking on the “x” in the upper right hand corner of the window. You can also use “Alt + F4” if the window is maximized and you cannot access your toolbar. Never click on any button, even if it says “Cancel” or “Close” on the window itself. These buttons can masquerade as innocent features that inadvertently start an unwanted download of spyware.
- Be suspicious if endless pop-up windows start opening simultaneously, or if the performance of your workstation turns into a crawl. Assume that you’ve been hit by spyware and seek assistance!
- Download Firefox and use it instead of Internet Explorer: <http://www.mozilla.com/firefox/>
- If you’re using Internet Explorer as your browser, change its settings to block Active X objects. Go to Tools > Internet Options > Security > Custom Level. There is a section near the top of the dialogue box devoted to Active X controls. At the very least, disable downloading of both signed and unsigned Active X controls and those marked as unsafe. Some Active X objects are spyware. This will block them.
- If you’re workstation is running Windows XP SP2, then turn on the pop-up blocker feature in Internet Explorer and activate the firewall now bundled as part of SP2. The pop-blocker is listed under Tools in Internet Explorer’s menu bar, and the firewall can be turned on from the Windows Firewall icon in Control Panel. These actions won’t stop spyware altogether, but they can help.
- My favorite good anti-spyware application for home users and small business is Spybot Search and Destroy. After installation make sure to update to the latest definitions to help remove spyware:  
Spybot Version 1.4: <http://www.safer-networking.org/en/mirrors/index.html>