



Safer Browsing

1. Switch to Firefox or Safari or upgrade to IE 7
2. Use Internet Options to set security and other controls
3. Delete temporary internet files, cookies and browsing history frequently
4. Use the Pop-up Blocker and Phishing Filters and controls
5. Use care and common sense in selecting which sites you visit

Just The Basics

1. Back It Up! Use Windows Backup or a 3rd party utility or manually copy important documents, photos or music to an external disk.
2. Use the Error Checking and Defrag tools for each hard drive weekly to keep it fast and safe.
3. Keep your anti-virus and anti-spyware software up-to-date.
4. Always do the automatic Windows updates!

Browser Safety (Part 1 of 3) Dangerous Searches

You trust Google, right? AOL, Ask.com, MSN, Yahoo, they're all powerful search engines and if you want to find stuff on the web you've got to use the search tools.

Well, watch out! That link you go to after a search could be loading your computer with spyware and scams.

One study concluded that an average of 9% of sponsored links and 3% of organic links go to questionable web sites. Consider the results of the following searches on Google:

"free screensavers": 57% "dangerous" links
"screensavers": 55% "dangerous" links

"Dangerous" is defined as a site whose downloads contain spyware, adware, embedded code, is deceptive, or sends spam email, or any combination of these traits.

Current trends are even more alarming! You can protect yourself by installing a combination of anti-virus, anti-spyware, and anti-adware applications. Even the best antivirus software needs help from other specialized apps.

Keep your anti-virus definitions updated, use anti-malware tools like SpyBot S&D and AdAware. And remember, good ol' common sense is one of the most powerful tools in your arsenal. If you don't know it or if it seems questionable—just don't go there!

Next issue: Browser settings and tools

(Note: search engine statistics from Tom Spring, Net Watchdog, PC World, May 26, 2006)

Secure Wireless Networking

The allure of quick and easy wireless connectivity everywhere you go is both the boon and the bane of wireless networking. We've all heard the warnings many times, but we mostly ignore them.

Between myself, my wife, and my live-in mom-in-law, there are frequently as many 6 or 7 computers on my home network. Additionally, clients often bring their laptops in and need to connect. My business and livelihood depend on these computers being as secure as possible.

Having an unsecured wireless network is an open invitation to unimaginable trouble. Here are a few simple steps you can take to make your home or business network more secure:

1. Hide the SSID. If the SSID is hidden it is not likely that casual browsers will see the network to connect. Connect to your router's settings page, find the wireless settings and set the option to hide the SSID.
2. Set a password. Again, while connected to the router's settings page, select the option for either WEP or WPA. Doing so will require any computer or device connecting to the network to use that password. Typically a WEP ID is stamped on the label on the bottom of the router. (Write it down and keep in a secure place).
3. Use a wired connection whenever possible. Wired is ALWAYS more secure than wireless, plus it frees up bandwidth on your router.

This is important. Expect more next issue!