



**Who's  
Watching?**

# Personal Computing Tipsheet

from "Who's Watching Charlottesville?"

October 1, 2008

## Some Tips for Safer Personal Computing

### Quick Tips

- Secure personal information like your SSN and tax forms if you store them on your home computer.
- Change your Internet surfing habits—*always* think before you click. It's one of the best ways to protect yourself online.
- Get informed about wireless security. You don't want strangers mooching off your home wireless network, or criminals stealing your personal info while you surf online!

### Learn More

**Strong Passwords**  
whoswatching  
charlottesville.com/  
password.html

**Spyware & Adware**  
whoswatching  
charlottesville.com/  
adware.html

**Firewalls**  
whoswatching  
charlottesville.com/  
firewalls.html

**Mobile Security**  
whoswatching  
charlottesville.com/  
mobile.html

- **Use strong password protection.** Learn what constitutes a strong password, create ones you can remember, and never share your password with anyone. You can check your password strength using many of the password strength testing tools online.  
*Note:* If you have reason to believe someone has learned your password, *change it immediately.*
- **Use up-to-date anti-virus and anti-spyware software.** Install anti-virus software on your computer, and schedule daily updates that will recognize new virus types as they emerge. Enable the automatic protection of all incoming files, and schedule weekly scans of your hard drive. Antivirus software, however, is not enough; install anti-spyware software on your computer, too. You may want to download the Microsoft's anti-spyware software Windows Defender, which is pre-installed on Windows Vista, for Windows XP.
- **Don't open files from unknown sources.** Carefully judge the credibility and trustworthiness of the source of a file before opening it. Email attachments and downloaded files are common sources for malicious programs. Bear in mind that some viruses and worms can mimic the identity of a familiar email correspondent. If you weren't expecting an attachment, you may want to contact the email sender to verify the attachment before opening.
- **Back it up.** Create a backup of your entire system periodically, and back up critical data files, whenever you update them.
- **Keep your application software updated.** Check your software manufacturers' websites regularly for updates to their products. A hole in some software can undo all the other security measures you've taken.
- **Remember physical security.** It may sound obvious, but it's important: protect your system from theft by physically securing your computer. Purchase a lockup cable for your laptop to increase security while on the go, and a surge protector with a circuit breaker to protect against power line surges. Verify that your system is covered under a homeowner's or renter's insurance policy.
- **Turn off unneeded software features.** The more software packages there are on a computer, the more opportunity for hackers. Uninstall software and turn off features you don't use.
- **Turn on firewalls.** Firewalls can prevent hackers from making unwanted connections to your machine. The firewalls on recent Windows and Macintosh operating systems are turned on by default.
- **Encrypt your home wireless network.** Encryption of your home wireless network will prevent hackers from eavesdropping on your private communications. To encrypt your network, consult the manual that came with your wireless router, or search online for tips on securing your home wireless network.
- **Scrub and recycle your old computer.** Don't recycle or give away your old computer until you are *sure* that your personal information has been scrubbed from it.
- **Pay attention to your mobile devices.** Laptops, phones, portable music players, and thumb drives can be easily lost. Know what data you have put on them! Avoid putting sensitive data on these devices, because they're so mobile they're a security risk too.