

W I S C O N S I N

# Office of Privacy Protection

*Safeguarding Information for Your Future*

## Protecting Your Computer from Hackers

- **Back up important files.** Familiarize yourself with your computer's built-in recovery tools. This will be beneficial if your system is compromised by a virus or a computer hacker.
- **Use strong passwords.** Select passwords that are at least 8 characters in length and contain upper and lower case letters, numbers, and punctuation. This is especially true for passwords that are used to access your email and bank accounts.
- **Use virus protection software and set it to update daily.** Most virus protection software has a feature that will scan downloaded files automatically and some will even scan incoming emails by default. There are both free and retail versions of virus protection software available.
- **Update your operating system regularly.** Be sure to apply all security patches released by the software manufacturer. Some operating systems allow you to enable automatic updates.
- **Avoid installing unnecessary, unfamiliar, or untested software.** This could include games or toolbars that could leave your computer open to attacks. Spyware and viruses are commonly acquired by installing unfamiliar programs.
- **Do not send sensitive or private information via email.** Email is not usually encrypted, or in other words not in a "secret code," and can be intercepted and read by hackers. However, there are encryption software packages available.
- **Install at least one spyware or adware detection and removal application.** Make sure to update and run it periodically. As usual, there are both free and retail versions available.
- **Use a personal firewall.** Firewalls help to protect your computer from hacker attacks by preventing unauthorized Internet connections to your computer. There are free and retail versions available and firewalls can come in the form of both software and hardware.
- **Secure your home wireless network.** Change your wireless router's default password. Enable WPA encryption and use a long password or passphrase. If WPA encryption is not available, WEP encryption is better than nothing.

If you believe your identity has been stolen, contact the Wisconsin Office of Privacy Protection at 1-800-422-7128 or email us at [DATCPWisconsinPrivacy@Wisconsin.gov](mailto:DATCPWisconsinPrivacy@Wisconsin.gov). Visit our website at [www.privacy.wi.gov](http://www.privacy.wi.gov) for more information.