

# Computer Security Checklist



## Ways to avoid computer viruses, vandalism and other threats to computers, networks and information

- ❑ Be especially careful with passwords. Make them at least five characters in length and avoid obvious passwords, like a name, nickname, home telephone number, date of birth, astrological sign, exact sequences on your keyboard (QWERTY or ASDFGH), any publicly available information, or any of the previous items spelled backwards. Also, use different passwords for different services or locations.
- ❑ Use and regularly update anti-virus software.
- ❑ Install a spyware-removal program on your computer or run a free online scan that cleans the spyware off your computer. The most popular spyware-removal programs are AdAware and PestPatrol. REMEMBER, be suspicious of anything that can be downloaded for free on your computer. Other harmful programs can be downloaded at the same time without your knowledge. *Spyware is software or a program that gets installed on your computer WITHOUT your knowledge or your permission. After it is on your hard drive, spyware will send personal information stored in your computer to other places on the Internet. Spyware floods your browser with all those annoying popups, steals your information, spams your email inbox, slows down your computer and your Internet connection.*
- ❑ NEVER open an attachment ending in .exe or .vbs, among other types. NEVER open an attachment from a source you don't know. NEVER open an attachment with a double extension, like .jpg.vbs or .doc.exe.
- ❑ Be on the lookout for hoax (*a trick*) virus alerts. A real or true virus alert will take you straight to more information about the specific virus threat.
- ❑ Use a firewall between the parts of a computer system that someone from the outside can access and the parts used from within. Many hackers use programs that search the Internet for computers with ports open. When they find a computer with an open port (like an open door), they can examine, use and change the files on the computer.
- ❑ For email communication with friends, set up a free email account and use a "fake" name for the account. When you do that, if you start receiving junk emails you can simply close the account and open another.
- ❑ NEVER give out information that identifies who you are, like your real name, address, city, or telephone number.
- ❑ AVOID phishing, or being tricked by someone who uses email and a fake website to "reel you in" and take your personal information for criminal use.
- ❑ If a hacker or virus deletes or damages your files, the easiest solution is to clean off your hard drive and then copy your files from a backup, or a copy of your files stored in a safe place.
- ❑ Wireless networks present another problem. Anyone with an antenna and amplifier can intercept and use a wireless network. If you are using a wireless network, enable (allow) encryption on ALL the transmissions and place the transmitters as FAR as possible from your outside wall and even farther from your windows.

