Protect Your Computer

By using safety measures and good practices to protect your home or office computer, you can protect your privacy and data. The following tips will help you lower your risk while you're online.

Install a firewall

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer. Hackers search the Internet in much the same way that some telemarketers automatically dial random phone numbers. Hackers send electronic probes, or pings, to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random pings. A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed Internet connection, such as DSL or cable.

Some operating systems have built-in firewalls that may be shipped in the "off" mode. Therefore:

- Be sure to turn your firewall on.
- Ensure your firewall is set up properly and updated regularly.
- Check your online "Help" feature for specific instructions.

Use anti-virus software

Anti-virus software protects your computer from viruses that can destroy your data, slow down or crash your computer, or allow spammers to send e-mail through your account. Anti-virus protection scans your computer and your incoming e-mail for viruses, and deletes them.

- Keep your anti-virus software updated to cope with the latest bugs circulating the Internet. Most anti-virus software includes a feature to download updates automatically when you are online.
- Make sure your anti-virus software is continually running and checking your system for viruses, especially if you are downloading files from the Web or checking your e-mail.
- Set your anti-virus software to check for viruses when you first turn on your computer.
- Give your system a thorough scan at least twice a month.

Use anti-spyware software

Spyware is software installed without your knowledge or consent. It can monitor your online activities and collect personal information while you surf the Web. Some kinds of spyware, called keyloggers, record everything you type in – including your passwords and financial information. Your computer may be infected with spyware if you receive a sudden flurry of pop-up ads, are taken to Web sites you don't want to go to, or if your computer begins to run slowly.

Spyware protection is included in some anti-virus software programs.

- Check your anti-virus software documentation for instructions on how to activate the spyware protection features. You can also buy separate anti-spyware software programs.
- Keep your anti-spyware software updated and run it regularly.
- Download software only from sites you know and trust. Piggybacking spyware can be an unseen cost of many "free" programs.
- Don't click on links in pop-up windows or in spam e-mail.

Manage your system and browser to protect your privacy

Hackers are constantly trying to find flaws or holes in operating systems and browsers.

- To protect your computer and the information on it, ensure your security settings in your system and browser are set at medium or higher. Check the Tools or Options menus for how to do this.
- Update your system and browser regularly, taking advantage of automatic updating when it's available. Windows Update is a service offered by Microsoft. It will download and install software updates to the Microsoft Windows operating system, Internet Explorer, and Outlook Express. It will also deliver security updates to you. Patching can also be run automatically for other systems, such as the Macintosh operating system.

Secure your wireless network

If you use a wireless network in your home, take precautions to secure it against hackers. Encrypting wireless communications is the first step.

- Choose a wireless router with an encryption feature and turn it on. WPA encryption is considered stronger than WEP. Your computer, router, and other equipment must use the same encryption.
- Consider disabling identifier broadcasting if your router enables it.
- Note the name assigned to your Wi-Fi network. This name – called an SSID, or Service Set IDentifier – lets you connect your computers to the network manually. The SSID is often the equipment maker's name.
- Change the SSID on your router and the pre-set administrative password. Hackers know the pre-set passwords on many wireless routers.
- Consider turning off your wireless network when you're not using it.

Remember that public hot spots may not be secure.

- Avoid accessing or sending sensitive personal information over a public wireless network.