If the computer you're using now is not protected, identity thieves and other fraudsters may be able to get access and steal your personal information.

Tips from the California Office of Privacy Protection

By using safety measures and good practices to protect your home computer, you can protect your privacy and your family. The following tips are offered to 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 the way some telemarketers automatically dial random phone numbers. They send out pings (calls) to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random calls. A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed Internet connection, like DSL or cable.

Some operating systems have built-in firewalls that may be shipped in the "off" mode. Be sure to turn your firewall on. To be effective, your firewall must be 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 then deletes them. You must 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. In addition, make sure that the 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. You should also give your system a thorough scan at least twice a month.

◘ Use anti-spyware software.

Spyware is software installed without your knowledge or consent that can monitor your online activities and collect personal information while you surf the Web. Some kinds of spyware, called keyloggers, record everything you key in – including your passwords and financial information. Signs that your computer may be infected with spyware include a sudden flurry of pop-up ads, being taken to Web sites you don't want to go to, and generally slowed performance.

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 buy separate anti-spyware software programs. Keep your anti-spyware software updated and run it regularly.

To avoid spyware in the first place, 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, put the security settings in your system and browser 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, Outlook Express, and will also deliver security updates to you. Patching can also be run automatically for other systems, such as Macintosh Operating System.

◘ Secure your wireless network.

If you use a wireless network in your home, be sure to 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. If your router enables identifier broadcasting, disable it. Note the SSID name so you can connect your computers to the network manually. Hackers know the pre-set passwords of this kind of equipment. Be sure to change the default identifier on your router and the pre-set administrative password. Turn off your wireless network when you're not using it.

Remember that public "hot spots" may not be secure. It's safest to avoid accessing or sending sensitive personal information over a public wireless network.

For More Information

- **California Office of Privacy Protection (www.privacy.ca.gov)**

The California Office of Privacy Protection provides information for consumers on protecting your computer, identity theft, and other privacy topics. The tips above are taken from “CIS 12: Protect Your Computer from Viruses, Hackers, and Spies.”

- **OnGuardOnline (www.onguardonline.gov)**

OnGuardOnline provides practical tips from the federal government and the technology industry to help you defend yourself against Internet fraud, secure your computer, and protect your personal information.

- **Consumer Reports (www.consumerreports.org)**

The independent nonprofit Consumers Union provides product reviews and strategies in a September 2006 article in ConsumerReports.org, “Stay Safe Online: Best Software Tools and Strategies,” available for free online. Product ratings are available to subscribers.

- **PC Magazine (www.pcmag.com)**

The magazine provides product reviews in December 2006 articles, ”Suitest Security Software,” available for free online at http://www.pcmag.com/article2/0,1759,2076246,00.asp.