Protect Your Computer

from Viruses, Hackers, & Spies

Tips for Consumers

Consumer Information Sheet 12 • January 2015

Today we use our computers to do so many things. We go online to search for information, shop, bank, do homework, play games, and stay in touch with family and friends. As a result, our computers contain a wealth of personal information about us. This may include banking and other financial records, and medical information – information that we want to protect. If your computer is not protected, identity thieves and other fraudsters may be able to get access and steal your personal information. Spammers could use your computer as a "zombie drone" to send spam that looks like it came from you. Malicious viruses or spyware could be deposited on your computer, slowing it down or destroying files.

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 email through your account. Anti-virus protection scans your computer and your incoming email 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 email. 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.

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

☑ 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 email.

☑ 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 "Tool" 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.

☑ Use a Strong Password – and Keep it to Yourself

Protect your computer from intruders by choosing passwords that are hard to guess. Use strong passwords with at least eight characters, a combination of letters, numbers and special characters. Don't use a word that can easily be found in a dictionary. Some hackers use programs that can try every word in the dictionary. Try using a phrase to help you remember your password, using the first letter of each word in the phrase. For example, HmWc@wC2 – How much wood could a woodchuck chuck. Protect your password the same way you would the key to your home. After all, it is a "key" to your personal information.

☑ 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.[1] 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.[2] 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. You may also consider buying a mobile broadband card that will allow you to connect to the Internet without relying on Wi-Fi hot spots. A mobile broadband card is a device that plugs into your computer, laptop, PDA, or cell phone and uses a cell phone signal to provide high-speed Internet access. They are sold by cell phone companies and require a monthly service plan.

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

☑ Be Careful if You Share Files

Many consumers enjoy sharing digital files, such as music, movies, photos, and software. File-sharing software that connects your computer to a network of computers is often available for free. File-sharing can pose several risks. When connected to a file-sharing network, you may allow others to copy files you didn't intend to share. You might download a virus or bit of spyware that makes your computer vulnerable to hackers. You might also break the law by downloading material that is copyright protected.

☑ Shop Safely Online

When shopping online, check out the Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! Shop elsewhere.) Learn how to tell when a Web site is secure. Look for "https" in the address bar or an unbroken padlock icon at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers as it moves across the Internet.

☑ Parents, Take Control

Don't let your children risk your family's privacy. Make sure they know how to use the Internet safely. For younger children, install parental control software that limits the Web sites kids can visit. But remember – no software can substitute for parental supervision.

☑ Additional Information

Consumer Information Sheet 6: How to Read a Privacy Policy

Consumer Information Sheet 9: Protecting Your Child's Privacy Online

Consumer information from the California Department of Justice, available at *www.oag.ca.gov/privacy.*

OnGuard Online

Practical tips from the federal government and the technology industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information, at *www.onguardonline.gov*.

Online Guide to Practical Privacy Tools

Computer security resources from the nonprofit Electronic Privacy Information Center, available at *www.epic.org/privacy/tools.html*.

Product Reviews

The independent nonprofit Consumers Union provides product reviews and strategies in a September 2008 article in *ConsumerReports.org*, "Get the Most from Security Software," available for free online at *www.consumerreports.org*. Product ratings are available to subscribers.

PC Magazine provides product reviews in an October 2008 article, "The Best Security Suites for 2009," available for free online at *www.pcmag.com/article2/0,2817,2333448,00.asp*.

PC Magazine provides reviews of free software in a May 2008 article, "Free Security Software," available for free online at *www.pcmag.com/article2/0,1759,2304349,00.asp*.

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy

NOTES

[i] WEP is Wired Equivalent Privacy, a security protocol that encrypts data sent to and from wireless devices in a network. WPA is Wi-Fi Protected Access: a security protocol developed to fix flaws in WEP.

[ii] SSID is Service Set Identifier, the name a manufacturer assigns to a wireless network router. The same SSID may be assigned to all hardware of the same type.

Kamala D. Harris
Attorney General
State of California

California Department of Justice
Privacy Enforcement and Protection Unit
www.oag.ca.gov/privacy