



Connecting to the Internet: How to Stay Safer Online

UNIVERSITY OF CALIFORNIA POLICE DEPARTMENT
601 Westwood Plaza, Los Angeles, California 90095
310.825.1491 ■ 310.206.2550 Fax
<http://www.ucpd.ucla.edu>



EMERGENCY: CALL 911

Your computer depends on you to keep it operating safely and securely.

If your computer is attacked by a virus or by a hacker, the damage is done. You could lose important personal information or software that's stored on your hard drive, as well as valuable time trying to make repairs. Your computer could be used without your knowledge to attack other computers, including those that protect our national security.

The following "do it now" tips can help you minimize and perhaps even avoid the damage that a virus or hacker can reek on your computer.

1. Use Anti-Virus Software

A virus is software that is planted in your computer to damage files and disrupt your system. Most viruses enter a computer hidden in a seemingly innocent program, often as an attachment to an email. The software code, attached to the program, copies itself, and then inserts the copied code into other programs. A virus can result in lost data or require costly repairs to your system. You can avoid these risks by installing software that scans your computer and your incoming email for viruses, and then deletes them.

You can download anti-virus software from the websites of software companies, or buy it in retail stores. Look for anti-virus software that recognizes current viruses, as well as, older ones; that effectively reverses the damage; and that updates automatically.

2. Regularly Update Anti-Virus Software

To be effective, anti-virus software must be updated routinely with definitions to the latest

"bugs" circulating through the Internet. Most commercial anti-virus software includes a feature to download updates automatically when you are on the Internet.

3. Don't Fall for Fibbing E-mails

Most viruses won't damage your computer unless you open the email attachment that includes the virus. So hackers (people who use the Internet to access computers without consent) often lie to get you to open the attachments. The email may appear to come from a friend or colleague, or it may have an appealing file name, like "Fwd: FUNNY TEXT" or "As per your request!" It could appear to link to a website or promise to clean a virus off your computer if you open it. Don't open an email attachment even if it looks like it's from a friend or coworker unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining the contents.

In addition, don't forward any email warning about a new virus. It may be a hoax and could be used to spread a virus. If you receive a chain letter or hoax virus alert, let the sender know so they can stop spreading the virus.

4. Use Strong Passwords

Hackers may try to steal your passwords to gain access to the personal information stored on your computer. To make it more difficult for them, use passwords that have at least eight characters and include numbers or symbols. Avoid common words. Some hackers use programs that can try every word in the dictionary. Don't use your personal information, your login name or adjacent keys on the keyboard as passwords.

Don't share your passwords online or over the phone. Your Internet Service Provider (ISP) should never ask for your password. You may want to change your password periodically.

5. Take Advantage of your Software's Security Features

Chances are your web browser and operating system software give you some options for increasing your online security. Check the "Tools" or "Options" menus for built-in security features. If you don't understand your choices, check them out using your "Help" function.

Similarly, your email software may give you the ability to filter certain types of messages, such as some unsolicited bulk email, also known as spam. But it's up to you to activate the filter.

6. Backup Important Files

If you follow these tips, you'll reduce the chances of falling victim to a hacker or virus. But no system is completely secure. If you have important files stored on your computer, copy them onto a removable disk, and store them in a safe place.

7. If Your Computer is Infected, Take Action Immediately

If your computer has been hacked or infected by a virus, disconnect from the Internet right away. Then scan your entire computer with fully updated anti-virus software.

Before you reconnect to the Internet, think about how your computer could have been accessed and what you could have done to avoid it. Did you open an email attachment and let loose a virus? Is your anti-virus software

out-of-date? Take steps to minimize the chances of it happening again.

8. Report Serious Incidents

If you think you've been hacked or infected by a virus, email a report of the incident to your Internet Service Provider (ISP) and the hacker's provider (if you can tell what it is). Often the ISP's email address is abuse@ISPname.com, or postmaster@ISPname.com. By doing this, you let the ISP know about the problem on their system and help them plan.

If you have particularly sensitive information stored on your computer or you're planning to upgrade to high-speed Internet access, don't forget to:

- **Install a Firewall** A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall makes it tougher for hackers to locate your computer and get into your programs and files. A firewall is different from anti-virus protection. Anti-virus software scans for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources.
- **Turn Off Software Features that You Don't Use.** You may want to turn "off" some software features such as "instant messaging," "printer-sharing," or "file-sharing," that typically are "on" when a computer is shipped. Because these programs facilitate the passing of information between computers, they are an excellent entry point for hackers.

- **Update Your Current System Software.** Install the current Windows, Mac OS or Linux patches and upgrades.
- **Consider upgrading your system software to the newest version.** Often the new version incorporates security features that make it more difficult to compromise your computer.

For more information on crime prevention, contact:

CRIME PREVENTION UNIT

UCLA Police Department

**601 Westwood Plaza
Los Angeles, CA 90095
(310) 825-6111**

www.ucpd.ucla.edu

"Working together to keep our community safe"