

FTC FACTS for Consumers

Safe at Any Speed:

How to Stay Safe Online if
You Use High-Speed
Internet Access



If you listen to the news, you've probably heard about hackers and viruses. But unless your computer has been targeted by one, you may not know how they could affect you. If your computer is attacked by a hacker or virus, you could lose important personal information or software stored on your hard drive. You also could lose valuable time while you try to repair the damage. Without your knowledge, your computer could even be used to attack other computers, including those that protect our national security.

The best protection against hackers and viruses is your personal commitment to online safety. If you use a high-speed connection to access the Internet, you can take precautions to better protect your time, the information on your computer and the security of our nation's computer networks.

What is high-speed Internet access?

Most Americans who use the Internet from home connect to it through a "dial-up connection" using a modem to call into a server over a regular telephone line. Many Internet Service Providers offer high-speed Internet access — also known as broadband access — usually through a DSL connection (a digital subscriber line) or a cable modem.

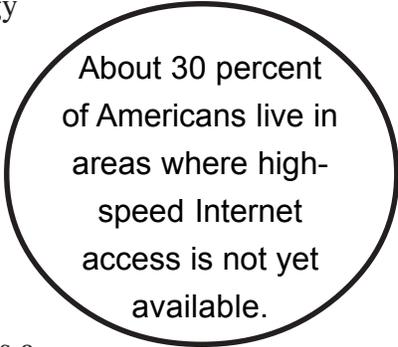
High-speed Internet access can cost more than a dial-up connection, but an increasing number of consumers choose it because:

- it is faster than a dial-up connection, which reduces the time you spend waiting for web pages to load and lets your computer work faster.
- it can connect your computer to the Internet with no dialing and no busy signals.

An estimated 24 million Americans use a high-speed connection to access the Internet.

Facts for Consumers

- it lets you make and receive voice calls over your phone line while you're connected to the Internet. That's because DSL technology can handle data and voice on a single phone line at the same time and cable technology uses a separate wire from the telephone.



About 30 percent of Americans live in areas where high-speed Internet access is not yet available.

What are the risks?

Along with their benefits, high-speed Internet connections can be an inviting target for hackers and computer viruses. A hacker is a person who uses the Internet to access computers without permission. A virus is software that is planted in your computer to damage files and disrupt your system.

When you connect to the Internet, you are identified by an Internet Protocol (IP) address — a string of numbers that identifies your machine. If you use a dial-up connection, your IP address changes every time you log on. Some high-speed connection users' IP addresses may remain fixed, making it easier for a hacker to access their computers repeatedly.

One reason a hacker might want to access your computer is to steal the personal information stored on it. A hacker could use that information to commit identity theft. Hackers who discover your credit card numbers, Social Security number or bank account numbers may use the information to run up charges in your name. Or they may sell the information to other identity thieves.

Your DSL or cable modem stays connected to the Internet unless you turn off the computer or disconnect your Internet service. These “always

on” connections can make a computer vulnerable to attack any time. Unless you take a few precautions, hackers can leave a virus or other software code on your computer that could be released later.

This technique has been behind distributed denial-of-service attacks. That's when hackers spread a virus that tells many individual computers to send messages simultaneously to the same server. The flood of messages can overload the system at, say, a bank, a government agency or another website. The systems then become swamped processing useless information or crash altogether.

If you use a high-speed connection to access the Internet, here are 10 tips that can enhance your protection against hackers and viruses, and help you stay safe online:

1. Use anti-virus software.

Most viruses enter a computer hidden in a seemingly innocent program, often as an attachment to an email. Then the virus software code attached to the program produces copies of itself and 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 and using 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 can effectively reverse the damage; and that updates automatically.

2. Regularly update anti-virus software.

To be effective, anti-virus software must be updated routinely with antidotes 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. Install a firewall.

A firewall is software or hardware designed to block hackers from accessing your computer. A properly configured firewall masks your IP address, making it tougher for hackers to locate your computer. Firewalls are designed to prevent hackers from getting into your programs and files.

A firewall is different from anti-virus protection: Anti-virus software scans your incoming communications and files for troublesome files; a firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources.

Some recently-released operating system software and some hardware devices come with a built-in firewall. It may be shipped in the “off” mode. Make sure you turn it on and set it up properly. Check your on-line “Help” feature for specifics. If your operating system doesn’t include a firewall, buy a separate software firewall that runs in the background while you work, or install a hardware firewall — an external device that includes firewall software. Like anti-virus software, a firewall needs to be updated regularly to be effective.

Some firewalls block outgoing information as well as incoming files. That stops hackers from planting programs — called spyware — that cause your computer to send out your personal information without your approval.

4. Don’t fall for a fibbing email.

Most viruses won’t damage your computer unless you open the email attachment that includes the virus. So hackers 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 appears to be from a friend or co-worker — unless you are expecting it or know what it contains. If you send an email with an attached file, include a text message explaining what it is.

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.

5. If your computer is infected, take action immediately.

If your computer has been hacked or infected by a virus, immediately unplug the phone or cable line from your machine. Then scan your entire computer with fully updated anti-virus software and update your firewall.

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? Did a hacker bypass your outdated firewall? Take steps to minimize the chances of it happening again.

6. Use strong passwords.

Hackers may try to steal your passwords to gain access to the personal information stored on your computer. To make it tougher for them, use passwords that have at least eight characters and include numerals 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.

7. 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. You probably have several choices for what types of files you want to accept from other computers. 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, or spam. But it's up to you to activate the filter.

8. Turn off software features that you don't use.

You may want to turn "off" some software features — instant messaging, printer-sharing or file-sharing — that typically are "on" when a computer is shipped. File-sharing allows several computers (connected through a network) to use the same file at the same time. Because it facilitates the passing of information between computers, this feature is an excellent point of entry for hackers. A firewall won't block files sent to you this way. If you're not on a network, turn the file-sharing feature "off." Your operating system's "Help" feature will show you how.

Another software feature that could leave you exposed to a virus is an email preview pane that lets you view attachments automatically. The preview pane could allow a virus to be launched even if you never click on the attachment.

And if you're not using your computer for an extended period, you can turn it off or unplug it from the phone or cable line. When it's off,

the computer doesn't send or receive information from the Internet and isn't vulnerable to hackers.

9. Back up 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 disc, and store them in a safe place.

10. Report serious incidents.

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

You also can report incidents to the FBI at www.ifccfbi.gov. For them to fight computer criminals, you need to report incidents.

The FTC works for the consumer to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or to get free information on consumer issues, visit www.ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.