



Internet Safety Tips and Terminology

Knowledge is power, especially when it comes to using the Internet. Optimize your Internet experience by practicing the safety tips provided here and by familiarizing yourself with common Internet-related terminology.

[Internet Safety Tips - Tips for Safe, Secure Internet Usage](#)

[Internet Terminology – Let's Talk Internet](#)

Tips for Safe, Secure Internet Usage

Internet usage opens the doors to a whole world of information, resources and conveniences like online bill paying and shopping. Unfortunately, media reports about identity theft, file-destroying computer viruses and Web site hacker attacks have some people apprehensive. For peace of mind when you're online, follow these tips:

- Use your Web browser to bookmark trusted Web sites. For example, in Internet Explorer simply click on "Favorites" in the top navigation bar and then select "Add to Favorites."

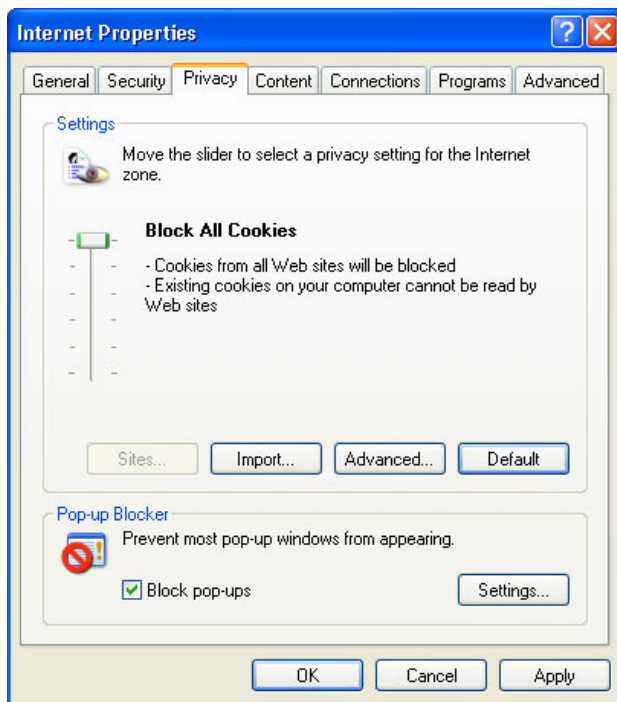
A screenshot of the top navigation bar of an Internet Explorer browser window. The menu items are: File, Edit, View, Favorites, Tools, and Help. The "Favorites" menu item is highlighted in a light blue color.

- Be wary of an information-collecting Web page that is an "orphan" page. You typically won't be able to locate a home page for the company, or you'll find the home page has an "under construction" message on it.
- Look for an "@" symbol anywhere in the page URL. This usually indicates a fraudulent Web site.
- Do business only with Internet companies that use a secure form to capture private information. To verify that your session is secure, look for "https:" instead of "http:" in the URL address line, as well as the padlock icon on your browser's status bar.
- Viruses spread rapidly and can damage or destroy your computer. New ones appear almost daily. It's critical that you install and update anti-virus software regularly. Make sure your computer also has up-to-date anti-spyware software. (Both are available at office supply and computer retailers and over the Internet directly from the software companies.) These programs will alert you when someone is trying to install "spyware" on your computer when you're using the Internet and when a virus is trying to infect your system.
- Be wary of e-mail attachments. Viruses can hide in an attachment. Don't open an attachment from anyone you don't know. Even if you do know the sender, an infected attachment may have been sent from an infected machine. The safest thing to do is to scan the attachment with anti-virus software before you open it.
- If you're required to register for an online account or for access to a Web site, you'll need a user name and password. Choose ones that would be difficult for others to guess. Your birth date may be easy to remember but it's also one of the first combinations of numbers a hacker would try. Try to combine letters and numbers in your passwords.

- Never send your Social Security number, credit card number or bank account information by e-mail. Always confirm the validity of e-mails or Web sites requesting personal or financial information.
- Cookies are small text files, stored on your computer, that allow a Web site to quickly identify you and store small bits of information about you, such as user names, passwords and preferences. If you do not want a Web site to retain and recall information about you, you can choose to block cookies, or delete one or all cookies using your Web browser.

To block cookies:

- Go to your computer's control panel and select "Internet Options."
- Choose the Privacy tab where you can choose your cookie settings, and whether to allow pop-up windows.



To delete a single cookie (using Internet Explorer)

- Open Internet Explorer and click the "Tools" button, and then click "Internet Options."
- On the "General" tab, under Browsing History, click on "Settings."
- Click the "View files" button.
- Click the "Name" column heading to sort all the files alphabetically, and then scroll down until you see files that begin with the prefix Cookie:. All cookies will have that prefix, and they usually contain the name of the Web site that created the cookie.
- Right-click the cookie you want to delete. Click "Delete", and then click on "Yes."
- Close the window that contains the list of files, and then click "OK" twice to return to Internet Explorer.



To delete all cookies (using Internet Explorer):

- Open Internet Explorer and click the "Tools" button, and then click on "Internet Options."
- On the "General" tab, under "Browsing history" click on "Delete."
- Click "Delete cookies."
- When you are prompted to confirm that you want to delete cookies, click "Yes."
- Click "Close" and then click "OK."

Note: Some Web sites store your member name, password, or other information about you in a cookie. If you delete that cookie, you might need to enter your personal information again the next time you visit the site.

- Make your computer has "pop-up" blocking software that is activated to block unwanted ads. Keep in mind, however, that some Web sites present information in new windows. Pop-up blocking software may confuse these with "pop-ups" and prevent them from opening. When you're browsing on a trusted Web site, you can set your pop-up blocking software to allow windows open only from that specific site.
- Always sign-off or log-off from any online accounts. Remember that you are most vulnerable when connected to the Internet. If there isn't a good reason to remain online, disconnect from the network.
- Install a firewall on your computer. A firewall is a software program that blocks unauthorized access to your computer. This is particularly important if you have a broadband connection, such as DSL or a cable modem.
- Update security patches for your operating system and Web browser. Security "holes" can turn up periodically. Once they are discovered, you can download fixes. For Windows users, an easy way to update your system is click on the Windows Update option under the Start menu or by pointing your Web browser to this link: <http://windowsupdate.microsoft.com/>.
- Back up your data. Make copies of your files in case they become corrupted or your system fails. Get in the habit of doing this on a regularly, at least once a week.



Let's Talk Internet

When you use the Internet, you often encounter what may seem like an entirely different language. Whether you're a new user or a veteran, make sure you understand the following Internet-related terms. They'll help you with navigating your way through the World Wide Web as well as understanding about Internet and computer security.

Adware – is software which displays advertising banners while the program is running. If your computer has pop-up blocking software, you can use it to prevent these ads from appearing.

Attachment – is a file included along with an e-mail message. It can be virtually any kind of file, such as a photo, music or video. You can open the attachment and view it on your computer screen or save it on your computer. Attachments can be misused, as in the case of someone sending you an offensive image or a harmful [macro](#).

Bandwidth – the rate at which information can travel through the wire into your computer. It is typically measures in bits per second. A full page of English text is about 16,000 bits. A 28.8 modem can move 28,000 bits per second.

Baud rate – refers to how many bits can be sent or received per second. Bits per second (Bps) is a measurement of how fast data is moved from one place to another.

BBS – stands for Bulletin Board System and is an online system for discussion, information sharing and announcements.

Blog (short for web log) – is usually defined as a personal or noncommercial Web site that uses a dated log format (usually with the most recent at the top of the page). It typically contains links to other Web sites along with commentary about those sites. A Web log is updated frequently and sometimes groups links by specific subjects, such as politics, news, pop culture, or computers.

Bookmark – is a [URL](#) saved in your browser. Bookmarking is the process of saving a URL in your browser that allows it to be recalled instantly in the future.

Browser (or Web browser) – is computer software that allows you to read and navigate pages on the [World Wide Web](#).

Cache – is a device used to temporarily store data. It is a time-saving feature that can be especially helpful on the [World Wide Web](#), allowing the cache file in your computer to store sites that you have recently visited so you can get to them quickly.

Chat room – is a place on the Internet where users can communicate in real time through text voice. Many chat rooms are found on Web pages, but there is another common form of chat on the [Internet](#) called IRC, which requires a special kind of program to access.

Cookie – It's a dessert. It's a snack. It's also be a small file stored on your computer by a Web site to keep track on information about you, such as what page you are on, what options you have selected, or what items you are going to purchase.



Cyberspace – a term used to describe the online world, coined by William Gibson in his novel *Neuromancer*.

Download – to transfer data from one computer to another.

E-mail (electronic mail) – is any message sent via an electronic system, although today, almost all e-mail is sent via the [Internet](#).

Emoticon – is a little face or other picture made up of text. For example, the original emoticon, the smiley, is made with a colon, a hyphen, and a closed parenthesis, like so :-)

Firewall – is a system that creates a special "wall" used by network servers to separate their [Intranet](#) from the [Internet](#). It keeps out unwanted information like [spam](#) and viruses and unwanted people like hackers.

Flash – refers to Macromedia Flash, a program that allows you to create animated content for your Web page. To be able to see Flash content you must have this program on your computer.

Hacker – a person who exploits security holes in technology for any purpose.

Homepage – the Web page that your [browser](#) is set to use when it starts up, or the main page of any Web site.

Identity theft – can happen when someone gathers enough information about you to successfully impersonate you online, by mail, over the telephone, or in person. That's why it's important to keep personal information secure, including Social Security numbers, driver's license numbers and bank account information.

Intranet - a private network inside a company or an organization.

Internet – is the international, mostly public network of computers attached together through a combination of public, government, commercial, and educational connections. Despite Al Gore's claim to founding the Internet, it was actually begun in the 1960s as a collaboration between the U.S. government and U.S. educational institutions.

Internet Explorer™ – is one of the most common Web [browsers](#). You can get the latest version of Internet Explorer™ on Microsoft's [Web site](#).

Internet fraud (or online fraud) – is any kind of crime involving fraudulent business practices that is carried out on the [Internet](#).

ISP (Internet Service Provider) – are companies that sell access to the [Internet](#) to individuals and companies.

Link (hypertext link) – is word or phrase that you can click on that will take you to another resource on the [World Wide Web](#).



Macro – is a saved set of instructions for a word processing or other software. They were originally intended to allow a computer user to save time by programming time-consuming tasks into reusable sets of instructions. However, some people embed harmful macros into documents that they send by e-mail that perform unwanted tasks such as deleting your files or sending messages to everyone in your address book. Many software programs give you the option of disabling macros to prevent these harmful tasks from being carried out.

Navigate – is the act of moving from page to page and Web site to Web site online. It is also called browsing or surfing.

Netiquette – is simply etiquette on the [Internet](#). (In other words, manners count online as well as offline.)

Password – is the secret word you use when signing onto the [Internet](#) or an online service that helps to confirm your identity.

Podcast – is an audio show that is broadcast over the Web. Users can listen to these shows on a digital music player or a computer. Podcasts can include talk shows, music, or other types of audio.

Privacy policy – Most reputable Web sites that collect personal information have a prominently displayed privacy policy. This policy should outline how the company uses your personal information, including whether or not they intend to resell it or use it for other marketing purposes.

Query - A request for information about a certain topic. A query is what you put in the box when you type something into a search engine.

Search Engine – is a program that searches information on the [World Wide Web](#) by looking for specific keywords and returns a list of information found on that topic.

Server – is a special software package that connects to a network and provides data. The computer that this software runs on is also often called the server.

Spam – refers to unsolicited commercial e-mail. (It's also a Hormel meat product and has its own museum in Austin, Minnesota.)

Spyware – like [Adware](#), Spyware is software which displays advertising banners while the program is running BUT sends data back to a third party without the user's permission (or sometimes knowledge) WITHOUT ASKING the user is Spyware.

Streaming (Media) – is the exchange of video clips, sound, or other types of media over the Internet. It is a way for the user to quickly download these files.

Temporary Internet Files –Every time you open a Web page, your computer saves a copy of that site's files and graphics in your "temporary Internet files" folder. The amount of files can build up and make your computer run slow. You may want to periodically review this folder and delete the files.

Trojan – is a program that appears legitimate but actually contains something damaging.



URL (universal resource locator) – is the string of text used by a [Web browser](#) to identify the precise location of a Web resource, including the server that hosts it, the directory in which it resides the name of the file itself.

Virus – a software program capable of reproducing itself and spreading from location to location, typically via e-mail without the computer user’s knowledge or permission.

World Wide Web (Web or WWW) – refers collectively to all of the linked pages available for browsing on the Internet.

Zip File – refers to large files that have been compressed to make them easier to send over the Internet. The receiver must download the file with a program that will unzip it, breaking it up into the individual files that were compressed together in order to view the files. For example, if you want to send a member of your family some photographs, you can zip them all together into one file to make it easier to send.