



Web Surfing: How Anonymous Are You?

WHAT INFORMATION IS COLLECTED?

When you visit a Web site, a certain amount of information is automatically sent to the site. This information may include:

- **IP address** – Every computer on the Internet is assigned a specific, unique Internet protocol (IP) address. Your computer may have a static or a dynamic IP address. If you have a static IP address, it never changes. However, some Internet service providers (ISP) own a block of addresses and assign a different, open one each time you connect to the Internet—this is a dynamic IP address. You can determine your computer's IP address at any given time by visiting www.showmyip.com.
- **Domain name** – The Internet is divided into domains, and every user's account is associated with one of those domains. Look at the end of the URL to identify the domain; for example, *.edu* indicates an educational institution, *.gov* indicates a U.S. government agency, *.org* refers to an organization, and *.com* is reserved for commercial use. Many countries also have specific domain names. The list of active domain names is available at www.iana.org/domain-names.htm and www.norid.no/domenenavnbasert/domreg.html.
- **Software details** – An organization may be able to determine which browser, including the version that you used to access its site. The organization may also be able to determine which operating system your computer is running.
- **Page visits** – Information about which pages you visited, how long you stayed on a given page, and whether you came to the site from a search engine is often available to the organization operating the Web site.

If a Web site uses cookies, the organization may be able to collect even more information, such as your browsing patterns, which include other sites you've visited. If the site you're visiting is malicious, files on your computer, as well as passwords stored in temporary memory, may be at risk.

HOW IS THIS INFORMATION USED?

Generally, organizations use the information gathered automatically for legitimate purposes, such as generating statistics about their sites. By analyzing the statistics, organizations can better understand the popularity of the site and which areas of content are being accessed the most. They may be able to use this information to modify the site to better support the behavior of the people visiting it.

Another way to apply information gathered about users is marketing. If the site uses cookies to determine other sites or pages you have visited, it may use this information to advertise certain products. The products may be listed on the same site or offered by partner sites.

However, some sites may collect your information for malicious purposes. If attackers can access files, passwords, or personal information on your computer, they may be able to use this data to their advantage. The attackers may be able to steal your identity, using and abusing your personal information for financial gain. A common practice is for attackers to use this type of information once or twice and then sell or trade it to other people. The attackers profit from the sale or trade, and increasing the number of transactions makes tracing activity back to them more difficult. The attackers may also alter the security settings on your computer so they can access and use your computer for other malicious activity.

ARE YOU EXPOSING ANY OTHER PERSONAL INFORMATION?

Using cookies is not the only method for gathering information. The easiest way for attackers to gain access to personal information is to ask for it. By portraying a malicious site as legitimate, attackers may be able to convince you to give them your address, credit card information, Social Security number, or other personal data (See [Avoiding Social Engineering and Phishing Attacks](#)).

HOW CAN YOU LIMIT THE AMOUNT OF INFORMATION COLLECTED ABOUT YOU?

- **Be careful about supplying personal information** – Unless you trust a site, don't give your address, password, or credit card information. Look for indications that the site uses secure sockets layer (SSL) to encrypt your information (See [Protecting Your Privacy](#)). Although some sites require you to supply your Social Security number (e.g., sites associated with financial transactions, such as loans or credit cards), be especially wary of providing this information online.
- **Limit cookies** – If an attacker can access your computer, he may be able to find personal data stored in cookies. You may not realize the extent of the information stored on your computer until it is too late. However, you can limit the use of cookies (See [Browsing Safely: Understanding Active Content and Cookies](#)).
- **Browse safely** – Be careful which Web sites you visit; if it seems suspicious, leave the site. Also, take precautions by increasing your security settings (See [Evaluating Your Web Browser's Security Settings](#)), keeping your virus definitions up to date (See [Understanding Anti-Virus Software](#)), and scanning your computer for spyware (See [Recognizing and Avoiding Spyware](#)).

For more information on Internet security, please visit the [SecureTexas](#) Web site, the online security resource for Texas citizens. SecureTexas provides up-to-date technology security information as well as tips to help you strengthen your part of Texas' technology infrastructure. In case of an emergency, please notify the DIR IT Security Division at 512-350-3282. Information security incidents of a serious nature should be reported as quickly as possible to your agency's information security officer and the DIR IT Security Division.

| | | |
|--|---|---|
| Brought to you by: | Powered by: | Distributed by: |
|  MS-ISAC www.msisac.org |  US-CERT UNITED STATES COMPUTER EMERGENCY READINESS TEAM www.us-cert.gov/ |  DIR  www.dir.state.tx.us/securetexas |
| Copyright Carnegie Mellon University Produced by US-CERT | | |