Hide your identity

Before you venture online, keep the following facts in mind:

- Someone on the Net can make money by selling your personal data.
- Every time you go online, you give someone new information--however small a piece it may be--about your preferences.
- Some data collectors are not content to wait for you to come to them and may try to trick or steal more information from you.

We can call these the Basic Rules of Personal Information, and they hold true for everyone who uses the Internet, from your Uncle Sid to Larry Ellison. Your good name and every iota of data about you is for sale. Since you're not getting a cut of the profits (at least, most people aren't), it's best to keep your private information to yourself. After all, once it's out of your hands, you have no control over who gets it and how they use it.

Protect your IP address

Like the number and street name of your real-world address, a computer's IP address tells others where and how to find the computer online. This identifier is composed of four numbers, each between 0 and 255, separated by periods (for example, 123.123.23.2). Every Web site and electronic device connected to the Internet must possess a unique IP address; that is, no two devices can have the same IP address at the same time.

If spammers or hackers manager to get your IP address, they can assault your PC with viruses or even hack directly into it to steal your personal data. You can put up dedicated hardware or software firewalls and install antivirus programs on every node in your network, but, given enough time and resources, a determined hacker can break into almost any computer.

You should guard your IP address as carefully as you would your full name and street address. Neither your browser nor Windows itself allows you to hide your IP address from the outside world, but some third-party software takes care of this problem. For $5 per month, Freedom, from Zero-Knowledge Systems, masks your true IP address from the real world by routing all your Internet data through the Zero-Knowledge network. This program can stump even Web bugs (see below).

If you use a dial-up connection, you're less at risk because your IP address changes with every session. But if you have an always-on connection, such as DSL or cable, you probably have a static or unchanging IP address. A static IP can leave you vulnerable to repeated scans and attacks. On the other hand, if you get a different IP address each time you connect to the Internet--a *dynamic IP address*--you can present a moving target for the hackers. If you're privacy conscious, ask your ISP for a dynamic IP address. Intruders will have a much harder time finding your computer time and time again if your address isn't constant.

Cookies keep track

But Web sites also use other technologies to track you down and trace your movement online. Cookies are small data files that the Web sites you visit can store in your browser's cookie file to track your path across the Web or record your user preferences. Most cookies have useful purposes. For example, if you register to view a specific Web site (such as the New York Times on the Web), the site can plant a cookie on your computer so that, thereafter, you won't need to enter your username and password to access the site. There are two kinds of cookies: persistent cookies, which remain on your computer even if you shut it down, and per-session cookies, which are often used to store the contents of a shopping cart and won't be saved once you power off your PC.

The threat cookies present isn't from the depth of the information they can reveal; cookies don't permit hackers unfettered access to your private files, for instance. The threat is a small but long-term erosion of your privacy. Most sites record cookies every time you click a new link within the site and can later find out which pages you read and how long you lingered. Such information may be very useful to marketers who mine it for details on your

habits and likes or dislikes. Over time, these minute data fragments can help companies build a profile of you, which they could sell to yet more aggressive marketers.

Bugs do it better

If you delete the cookies regularly or configure your browser not to accept them (see Stop hostile apps for instructions), snoopy sites can't collect enough data to profile you. That's why some companies use Web bugs as a user-tracking backup if cookies don't work. Here's how Web bugs work: These tiny graphics, sometimes just a pixel high and a pixel wide, are the same color as a Web page's background. Any time you visit a site, the site must have your IP address before it can load any Web graphic file (including a Web bug), and, with your IP address in hand, the machine that hosts the Web bug can log your address for the duration of your session. Even with cookies blocked, bugs let sites track users surreptitiously. In many cases, the tracking may be benign--a site monitoring how popular a particular page is--but it isn't always just the site that uses a Web bug. Commercial sites with banner ads have discovered that ad banner companies themselves, such as DoubleClick, may use Web bugs to track the traffic on the sites that host their ads. So Web bugs can open you up to unwanted profiling, and (if the Web bug loads after a user fills in a Web order form, for example), possible junk mailing.