



TenStep Supplemental Paper

8 July 2005

Spies and Saboteurs

Recent reports point to software vendors who take liberties with information about you, tracking and even selling it. In the past year, multimedia company RealNetworks was accused of collecting information about users' listening and downloading habits, and online advertising firm DoubleClick has been sued for collecting and selling demographics data on users' movements online.

No Girl Scouts Here

How do these businesses collect all this dirt? Many people are concerned about cookies, text files that Web sites write to your hard disk, saving information such as your surfing and purchasing habits. The data, generally used for sending advertisements based on your Web behavior, is often harmless. But that data can end up in the wrong hands, so you might want to consider some cookie-management utilities.

Applications such as Cookie Crusher give you control over which sites can save cookies. Your browser probably also offers some cookie-management tools. In Internet Explorer 5, for example, select Tools/ Internet Options/ Security, click the Internet icon, then choose the Custom Level button to set your cookie-management preferences. In Netscape, click Edit/ Preferences/ Advanced to check your cookie settings. You can instruct your browser to accept all cookies, to accept only cookies that return to the original Web site (rather than some other site or hacker terminal), or to disable cookies altogether.

Worse Web Spies

Web bugs are an even sneakier method of tracking your surfing and shopping habits. These little devils are invisible tools, sometimes just one dot lodged on a Web page, that assign unique ID tags to your system, then report back information about you, such as which sites you've visited and what you've purchased. The worst thing about such bugs, however, is that you can't see them, and anti-cookie filters won't fix them. In fact, there's currently no fix for these sneaky little devils, but lawsuits and complaints from privacy advocates may keep their production to a minimum. Still, their existence is a good reminder to surf carefully and use anonymizers if you really don't want to be tracked.

Code on the Loose

Finally, some Web sites may inadvertently hide rogue code, often JavaScript or VBScript, that performs tasks you haven't authorized. These sneaky bits of programming can upload files to your system that are small enough to go unnoticed on high-bandwidth connections. The file may be a virus, a Trojan horse (a file that appears normal but may hide a virus), or just a mole, which collects information on you and sends it back to whomever is interested in your data. To protect yourself against these sneaky scripts, set your browser to prompt you before it downloads any file to your system. In IE 5, for example, select Tools/ Internet Options/ Security, click the Internet icon, then click the Custom Level button and set your preferences for ActiveX and Scripting.