

NOW SpinRite 6.1 – Fast and useful for spinning *and* solid state mass storage!

Misfortune Cookies



Adjusting Internet Explorer to Block Tracking Web Cookies

Page last modified: Aug 13, 2005 at 11:12

Gibson Research Corporation

Synopsis:

None of Internet Explorer's standard cookie privacy settings are usable or useful because they are either absolutely restrictive or easily bypassed. This page explains Internet tracking using cookies, discusses the various types of cookies, and demonstrates how to configure Internet Explorer to firmly block third-party "tracking" web cookies while allowing safe first-party and session cookies.

What's in a Cookie?

Netscape corporation, early pioneers of the world-wide web (www), created web browser "cookies" as a means for allowing web sites to offer enhanced services to their users. "Cookies" allow you to roam around advanced web sites such as eBay and Amazon while remaining "known" to the web server.

"Cookie" is a software programming term referring to a unique token that isn't in itself particularly meaningful, but which can be used to uniquely identify some other entity to which it has been assigned. In the case of a web browser, once a browser has received and accepted a site's "cookie" token, that browser can be uniquely identified in the future by the cookie token it carries.

Unless it is configured not to, a web browser will always accept any cookie offered to it by a cookie-enabled web site. It happens invisibly and without the user's involvement, knowledge, or permission. And from that point on that unique cookie is typically used to uniquely identify that individual browser, user, and computer from all others on the Internet.

Therefore, ALL cookies ARE ultimately about identifying and TRACKING web browser contact. That's what cookies are for. Anyone who is adamant about NEVER being identified from one web page to the next can, and perhaps should, COMPLETELY disable all web browser cookies. This is not difficult to do with Internet Explorer:



Blocking **all** cookies is possible, but some web sites now depend upon at least a bare minimum of cookie support. The good news is that it **is** possible to make that safe and private.

Why not block all cookies?

Some web sites will refuse to function if at least a "session cookie" is not accepted by the web browser for the current web surfing "session". Such web sites use session cookies to maintain some brief history of their user's movement among their pages. They require a "session cookie" to make this possible.

A "session cookie" is a non-persistent cookie which a web browser agrees to accept and carry — but only for the current web surfing session. Unlike regular cookies which are persistent and can be retained and carried in a browser for years, session cookies are kept in memory and are not written to the system's permanent storage. They are discarded when the browser or computer system is shut down.

What are first-party cookies?

So called "first-party" cookies are those offered to your web browser by the **same** web site you are visiting. While these cookies — whether they are session-cookies or persistent-cookies — **do** allow your movement around the site to be followed by the site, they are not generally regarded as a privacy concern because they can not be seen or accessed by other sites.

First-party cookies are what allow you to be recognized by active web sites where you have accounts, like news sites or eBay or Amazon. The first-party cookie your browser carries uniquely identifies your web browser and keeps you from having to log back onto a web site every time you return.

However, even that might not be what you want, depending upon who and how many people use your computer. But remaining "known" to web sites you return to can be a handy option to have — and first-party cookies make that possible. As we will demonstrate below, you can enable "session-cookies" to allow the temporary use of a web site, while disabling "persistent-cookies" to prevent a site from remembering your browser when it later returns. But . . .

**It's "third-party" cookies
that are the real problem.**

What are third-party cookies?

So called "third-party" cookies are sneaky cookies that were never really meant to happen and they have been, and are being, exploited by advertising and marketing firms and others, to track your actions and movements as you surf the web. Here's how they work:

Modern web pages are composed of many separate pieces. Users with slower or congested Internet connections are accustomed to seeing pieces of web pages arriving at different times.

