

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.

Often the page's text will appear first, followed by the appearance of various visual enhancements such as icons, buttons, images and photos.

These secondary components of web pages appear later, because the initial pieces of the page instruct your web browser to fetch them separately. The heart of any web page is text, but that text contains separate instructions with the name and location of the page's non-textual components which must then be fetched to finish assembling the complete page.

Part of the amazing power of the web is that a page can instruct your web browser to fetch any other pieces of the web page from any other servers located anywhere on the Internet. This is a powerful capability. But it comes at some cost of privacy and security because you, the trusting web user, are unable to exercise any control over which other "third-party" Internet servers your own web browser will be connecting to and requesting data from.

Here's the real problem:

Unless you take the steps explained and detailed below to deliberately prevent it, any of those unknown and unseen third-party Internet servers are able to plant their own persistent web browser cookies onto your computer!

In other words, not only can the site you are visiting ask your web browser to accept and carry a cookie so that it can keep track of you as you move about the site, but ANY of the other Internet servers that supply component parts of that web page are also able to give your web browser their own cookie which refers to their own server.

How does Internet tracking work?

While you might not like the idea of third-party Internet servers, for sites you never even visited, planting their cookies onto your computer, it still might not seem like a real problem.

Third-party cookies are a problem because they allow centralized Internet advertisers to track your movements around the Internet to develop a profile of you and your web surfing history and habits.

Here's how that is done:

As you wander around the Internet, surfing from site to site, your web browser is accumulating cookies from all the cookie-using sites you visit. And as we now know, although you can't see it, your browser is also accumulating cookies from sites and servers you have never directly visited — but from which the web pages you did visit have requested some sort of additional content — for example, advertising images. If many of the sites you visit are "advertiser supported" or display ads, your web browser will probably be retrieving visual advertisements from centralized advertising servers.

The third-party cookies your browser is carrying from global advertisers uniquely identifies **you** to that advertiser no matter where you roam. Every time your web browser asks the advertiser for an advertisement, it also tells the advertiser which site and web page "referred" it to the advertisement. (This is how advertisers pay the sites which host their ads.) So the advertiser also knows **where** you are, and what page you are looking at on the Internet.

In this fashion, thanks entirely to third-party cookie tracking, profiles of your Internet surfing history and habits are built up over time in central databases over which you have no control.

Why aren't any of IE's privacy settings useful?

Users of Microsoft's leading Internet Explorer web browser wanted useful privacy control over cookie handling to prevent third-party tracking. Since such features were being offered by competing web browsers, Microsoft was feeling the pressure to make them available in IE. But those third-party advertisers have a "business model" which is, after all, all about tracking us. So they put a great deal of pressure on Microsoft to keep tracking active and muddy the waters

enough so that most users would be so confused by the meaning of the settings that they would leave them alone and wouldn't change them.

All of the standard settings other than "Block All Cookies" (which we saw above) are trivial for third-party sites to bypass, and as we've already seen, blocking all cookies is overkill which isn't useful or practical. Here is the highest privacy setting at the first notch below "Block All Cookies":



As you can see from the description, this "High" setting blocks cookies that do not have something called a "compact privacy policy" or that use "personally identifiable information".

A "Compact Privacy Policy" is nothing more than a string of acronyms any server can include when it supplies a piece of a web page. Here's a typical example:

```
P3P: CP="NOI ADM DEV PSAi COM NAV OUR OTR STP IND DEM"
```

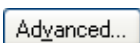
So **all** any web server needs to do, to completely bypass Microsoft's HIGHEST strength cookie privacy setting, is to add a P3P tag to their reply and IE will allow their use of cookies — period. It's like the site saying "Oh, don't you worry, **we** would never do anything you wouldn't want." Yeah, right. And it all happens without your knowledge.

Microsoft doesn't explain what they mean by "personally identifiable information" in cookies, but since cookies operate as "opaque tokens" and don't need to contain any personal information anyway — just a unique "tag" for you — this assurance means nothing.

And as Internet Explorer's "privacy" slider is moved further down from its "High" setting, things only get worse. But even at the "High" setting, any third-party server can easily plant and track long-living persistent cookies onto the user's computer.

Let's simply disable third-party cookies!

Microsoft hides the simple settings everyone really wants — and which all other browsers now offer — under the somewhat intimidating "Advanced..." button which discourages casual users from going there.



To access and change these "Advanced" settings, open any web browser window, then choose "Tool" and "Internet Options..." from the main menu. Next select the "Privacy" tab to see the dialog box we have been showing above.

Pressing the "Advanced..." button displays a simple dialog with exactly the settings every user wants. Now that you understand these terms, the settings you want to choose should be obvious to you:

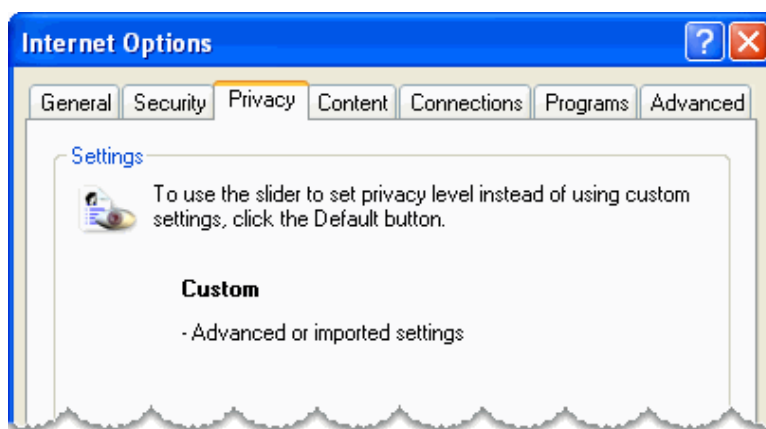


- 1 Enable the "**Override automatic cookie handling**" option to enable the rest of the dialog's controls.
- 2 For **First-party Cookies**: Select "Accept" First-party Cookies if you want web sites to be able to remember you when you return. If you prefer to remain unknown and unidentified at the start of a return visit, you can choose to "Block" persistent first-party cookies while still allowing session-cookies.
- 3 For **Third-party Cookies**: You will always want to select "Block" Third-party Cookies to flatly deny any attempts by third-party Internet servers to use cookies to track your movements around the Internet. There's just no good reason to ever allow sites and servers you don't intentionally visit to plant cookies onto your computer.
- 4 For **Always allow session cookies**: This should always be disabled (not checked). Accepting first-party cookies includes accepting first-party session cookies, so web sites that require your browser to carry a temporary session cookie will operate without trouble.

But since "Always allowing session cookies" **includes** third-party session cookies — which is NOT what we want — leaving this option disabled is the only way to completely block both persistent and non-persistent third-party cookies.

The only time you might want to always allow session cookies would be if you were not always accepting all first-party cookies.

Once you have Internet Explorer's "Advanced" cookie settings configured as you want, click the "OK" button to accept them and IE's Privacy settings will show that you are using "Custom - Advanced or imported settings".



After clicking "OK" to accept and close this Internet Options dialog, you can surf the Internet without unseen third-party web servers having the opportunity to track your movements. With these settings, Internet Explorer will ignore and discard any cookies they attempt to supply.



Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2024 Gibson Research Corporation. SpinRite, ShieldsUP, NanoProbe, and any other indicated trademarks are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer [privacy_policy](#).

Jump
To Top

Last Edit: Aug 13, 2005 at 11:12 (6,974.07 days ago)

Viewed 12 times per day