

Are Cookies Costing You Cash?

By Bill Hely

This is the story of how a minor design oversight is costing many online merchants a packet in lost sales, yet they will never see the problem unless a special type of visitor points it out to them. Or unless they read this article!

In March 2005 JupiterMedia Corporation (<http://www.JupiterMedia.com>) released an extensive report titled *"Measuring Unique Visitors: The Dramatic Decline in Cookie-Based Accuracy for Web Measurement"*. As the title suggests, the focus of the report was concern about the accuracy (or otherwise) of website traffic measurements, which rely heavily on the presence and persistence of cookies on the computers of website visitors. Some of the report findings were:

- During 2004, 58% of online users had deleted cookies from their PCs;
- 38% of online users believe that cookies are an invasion of their security and privacy online;
- 44% of online users believe that deleting or blocking cookies will protect them.

As uninformed as those last two beliefs are, there's nothing there that's very surprising. But there was another statistic which I found very hard to believe:

- 39% of online users may be deleting cookies from their primary computer monthly.

Hard to believe because, in my fairly extensive experience with end-users, many more than 61% of computer users wouldn't know what cookies are, where to find them or how to delete them!

I accept that a lot of people have erroneous ideas about the security/privacy aspects of cookies, and that quite a few do delete their cookie stores on a regular basis. But 39%? Nope, I'm just not convinced. 39% of **experience users** perhaps, but certainly not of computer users in general. Well ... not yet, but more on that in a moment.

Anyway, the main purpose of the Jupiter report was to provide advice to webmasters on how to cope with *"the decline in accuracy of visitor measurement"* due to not being able to rely on the persistence of cookies on visitors' computers. It is the existence of cookies that allows a web user's movements around the 'net to be tracked, within reason. If cookies are blocked or deleted then accurate tracking (measurement) is difficult if not impossible.

Like all such authoritative reports, this one has been widely disseminated, quoted, analysed and discussed. But there's a very important point about cookies that has been completely missed by a great many webmasters and online marketers.

I'm not talking about your losing business because your tracking and analysis might be inaccurate. My concern is much more direct.

**I'm talking about visitors that will go to
your website - try to buy - fail - and go away!**

You see, as JupiterMedia discovered, many people **are** concerned about cookies (often unnecessarily so) and many are turning to a type of software called a Cookie Manager. This is a small, simple background application that typically allows the user to, among other things:

- Intercepts a website's attempt to place a cookie on the visitor's computer, allowing the user to accept or reject Cookies on the fly;
- To compile "always allow" and "always deny" lists;
- To view "orphan" Cookies;
- And to generally manage the storage of cookies on their computer.

OK, so we've established that many people do not have a full complement of cookies on board at any given time, and that there is a trend towards this control becoming more widespread. Now we get to the problem!

Many websites use cookies as an integral part of their within-the-site navigation and, if the appropriate cookies are not present, navigation around the website either stops working altogether, only "sort of works" sometimes, or becomes very confused.

Often the website owner has no idea about this. Perhaps he had the site built by a programmer or web designer, or maybe he uses a 3rd party affiliate management or tracking program that employs cookies. Because the site owner is not personally blocking cookies in his browser, he never sees the problem himself. Most visitors to his site aren't blocking cookies either, so he won't be alerted by a flood of complaints.

But what happens when someone using a Cookie Manager visits the same website? The site's programming attempts to drop a cookie on the visitor's computer, the Cookie Manager asks the visitor if he wants to accept it, the visitor (out of habit) quickly clicks "Never accept", and continues browsing. He decides not to buy at the moment, but comes back later or is again referred there at a later time.

This time, on the later visit to the same site, there is no prompt to block or allow the cookie because last visit this site was added to the Cookie Manager's permanent block list when the visitor clicked "Never accept". The visitor starts following the site's navigation links to a purchase page or a trial download and ... strange things are happening. Probably it appears that many or all of the sites links are broken or misdirected.

So, Mr/Ms Online Marketer, what happens to your prospective customer now? Well, in all probability he's "outta there". You've tested his patience, lost his faith—and lost your chance to make a sale. And you haven't a clue why another visitor left without buying.

OK, so about now you are thinking to yourself: *"Yeah, well, how often is that gonna happen anyway?"*

Well, let me tell you: I use a Cookie Manager, I recommend the use of a Cookie Manager in my popular book *The Hacker's Nightmare*[™], and I know for a fact that many of my readers adopt the same practice. Further, cookie blocking is integral to a number of firewall and security-type applications. If you do a Google search for the term "[cookie](#)"

[manager](#)" you will get hundreds of thousands of hits, so obviously there's a lot of awareness of the concept.

Hark back to Jupiter Media's research discussed earlier. It tells us that a lot of other people are blocking—or want to block—cookies in various ways.

The test

So you still don't see how all this can affect your sales, eh? Well, like so many things related to online marketing, the only way to find out is to test. Here's how:

Go to <http://HackersNightmare.com?res=KburraHome> and download **Cookie Pal** for a free 15-day trial. Cookie Pal only works with Internet Explorer. There are plenty of cookie managers for Firefox, but since everyone has Internet Explorer I'll use it for this example. Install Cookie Pal (very simple) and proceed as follows.

First let me prove to you that cookies can affect navigation.

- Open Cookie Pal from the System Tray, select the Cookies Tab, then click the column header so the sort order is by name. Look for any cookies for yahoo.com and delete them. Don't forget to look for them with and without the "www" in front.
- Open the Filters tab and ensure there is no entry for yahoo.com in either of the two columns.
- Now open Internet Explorer to <http://groups.yahoo.com>. When a Cookie Pal dialog asks if you want to accept a cookie from Yahoo, click "Never".

Now go ahead and join a group, or login to one of which you may already be a member.

Sooner or later you are going to be faced with one of these messages or something very similar:

The browser you're using refuses to sign in. (cookies rejected)

OR

Your browser is not accepting our cookies. To view this page, please set your browser preferences to accept cookies.

The reason you are seeing these message is because **Yahoo has done it right !!!**

Yahoo **NEEDS** cookies for navigation, so their web developers have tested for your ability to accept cookies and responded with a useful message when it was discovered you aren't accepting them.

The alternative—don't test and do nothing—would have resulted in navigational errors and chaos at best, and that's exactly what many online shoppers encounter, because

webmasters aren't TRAPPING for the ability to accept cookies and responding with a useful message.

I thought about showing you some ways to check whether a browser is accepting cookies or not, but decided against it. There are quite a few ways you can do it and any number of different web programming scripts/languages you can use, so I'll leave it up to your own initiative.

You'll find all the examples you want by doing a Google search for something like "[test for cookies](#)" (try with the quotes first to narrow the results). If you prefer the test code to be in a particular script/language, add that to the Google search box also. For example, ASP programmers might search for: "[test for cookies](#)" ASP

But remember this: the language you use must ALSO be supported by the visitor's browser! This raises a common mistake that many web developers make—assuming that JavaScript will be OK. It is quite possible that the browser may have JavaScript disabled also, so there'd be no point using a cookies testing routine in JavaScript if the browser can't interpret the testing code. It's always possible that any **client-side** code you use (JavaScript is by far the most popular choice) may not be supported.

Using a **server-side** language such as PHP or ASP eliminates this problem.

If you insist on using JavaScript then you'll have to test for that also. A Google search for "[test for JavaScript support](#)" should give you plenty to work with to solve that problem and allow you to show a warning something like:

This website uses JavaScript to facilitate site navigation, but your browser has JavaScript disabled. Unless you enable JavaScript in your browser you will not derive full benefit from this website.

In which case it would probably also be a good idea to point to a page that describes how to enable JavaScript in the various web browsers. You can use this one of you like:

<http://www.HackersNightmare.com/enablejavascript.asp>

Still not convinced?

I'm a fairly persistent person and when I set out to do something online I'll usually press on until I find a solution.

Recently, after some research, I decided I wanted to buy a particular utility software product. I knew who the developer was and found his home page OK. However, all attempts to reach the order page for the product led me to the wrong place.

Now I wanted this thing, and I'm no beginner at finding different ways to skin the cat, so I eventually did manage to place an order. But you have to wonder how many sales had been lost in the past to potential buyers who had cookies disabled. Almost certainly any impulse buyers would not have persevered.

I've seen this sort of thing many times, so don't YOU make the same mistake with your websites.

The bottom line is:

- (a) If your web pages use JavaScript, test for it. Don't assume!
- (b) Test your own site with cookies blocked and, at the very least, advise your visitor that cookies are needed.

-oOOo-

Bill Hely is a technologist, consultant and author living in Brisbane, Australia. For most of the last two decades his professional focus has been on advising and supporting small business operators in Information Technology and Office Productivity issues—and rescuing them when they didn't heed his advice the first time around. He is the author of several books and numerous articles on technology for the business operator, including the Bible of Internet and computer security *The Hacker's Nightmare*™. For more information on this must-read tutorial and reference visit:

<http://www.HackersNightmare.com>