FIRST STEPS LINUX BEGINNERS SERIES

Firefox Cover your tracks

ON the DISC

There are genuine security reasons for removing accidentally accessed mail-order bride sites from your PC's memory, you know. Let Andy Channelle show you the way to safer, more discreet surfing.

LAST TIME

We added a little panache to home video with a musical soundtrack crafted in *Audacity* or *MainActor*. If you missed the issue, call 0870 8374773 or +44 1858 438975 for overseas orders.

Most computer users understand that browser security is an important issue – the fear that a cracker from some organised crime syndicate could comb through personal data via a *Firefox* vulnerability is enough to put many people off the internet for life. However, there is an area of web security that, because it doesn't sell as many newspapers (probably), tends to be ignored, even though it has real implications for an individual's security and privacy. This is the personal security policy: how much data a web browser can retain, and a method for managing it in a secure manner.

The most interesting thing about this side of the security coin is that it's the one the user has the most control over; it is reliant on *your* input, *your* clickstream and *your* decisions. In this tutorial, I will outline some of the ways in which you can tread lightly when using the *Firefox* browser and, should the need arise, have all traces of your activity erased once the browser has been closed down.

Aside from security concerns, there are many valid reasons why you might want to do this. You may be using a public net terminal and not want the next customer to see what you've been doing. You may be booking a trip to Paris for your partner and not want to ruin the surprise. You may be booking a trip to Paris for 'a friend' and not want to be rumbled by your partner. Or you may just feel uncomfortable allowing others to know about your browsing habits.

We'll be using a combination of tools built into *Firefox* and, when more automated or finer control is needed, freely available browser extensions. All of the extensions used are available using the Get More Extensions option in *Firefox*'s Tools > Extensions menu, unless otherwise stated.

There are three main elements of the browser application that can be used to monitor your browsing habits – cookies, cache and history – but there are also effective tools for managing them.

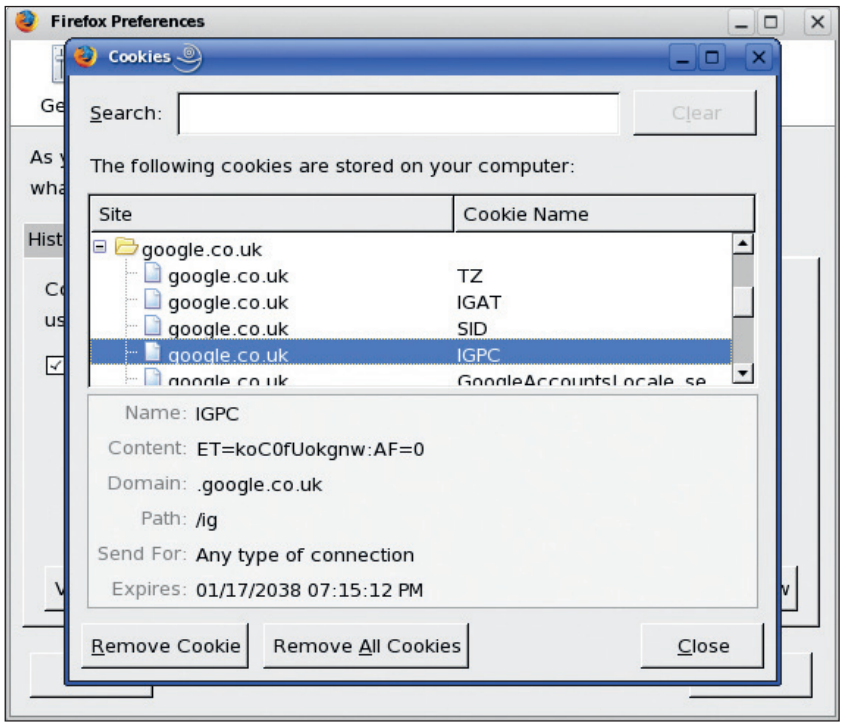
PART 1 – MANAGING COOKIES

The first part of this personal security policy deals with cookies. These are small text files that are deposited on your machine by a website and used by the server to identify you. Contrary to popular belief, the cookies themselves don't usually store any of your personal information – they simply point to a reference file on the server that contains various bits of user data such as the last time you visited a site, which adverts you clicked on and which website you came from.

Most cookies are innocuous and, indeed, you may regard them as worthwhile – it's good to know what's been dropped on to your PC and who put it there – but it can be insecure for the machine to magically log on to websites, or webmail, and show other users of the same computer which sites you've visited.

Firefox has a number of built-in options for cookie management, and these, along with many other things we'll be looking at, are hidden away in the main Preferences dialog box. The settings we need are accessible via the Edit > Preferences menu under the Security tab. In versions prior to *Firefox 1.5*, the main tabs will be ranged down the left-hand side of the dialog box with options presented as a list in the main pane, often with further options accessible with the small disclosure icon, which is a small cross. From version 1.5, things have been cleaned up and now follow the tabbed model that is used in the main browser with tabs situated along the top of the window.

If you're using an older version of *Firefox*, update it now (it's on the coverdisc). We are talking about security after all, and the most up-to-date software is usually the best option.



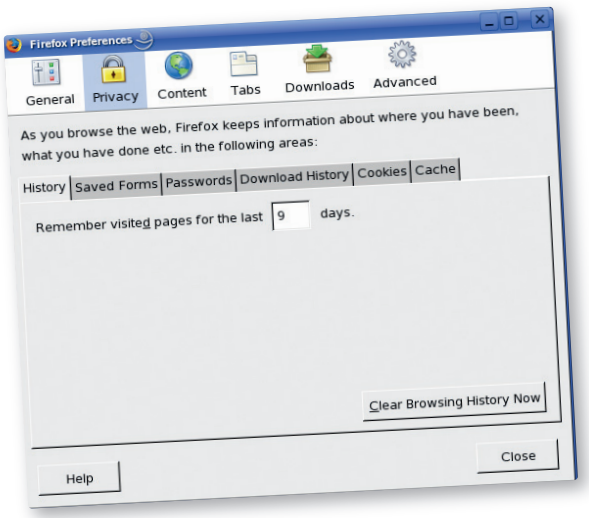
Google's cookies can tie a machine to its search history, which is not always a good thing.

Best before...

By examining the Cookies option, you'll notice that *Firefox* has a number of tools available for cookie management. By default, the browser will allow a website to set a cookie on your machine and let it expire when it is designed to do so. We can change all of this behaviour.

It's possible to prevent any website from depositing a cookie by deselecting the first option: Allow Sites To Set Cookies. This is a sledgehammer approach, however, and will result in many websites being unworkable. This is especially true of online banking sites where cookies are a part of the security model.

The Exceptions button offers a more nuanced approach. With the Allow Sites... option selected, the Exceptions option provides tools for blocking certain sites from setting cookies. When it is not selected, Exceptions will allow you to define sites that can use them. The process of defining a site is very simple:



This newly tabbed interface is where you configure personal security settings for *Firefox*.

just add the URL of the site you wish to configure options for in the Address Of Website text area and then choose Block (to stop a site from dropping a cookie), Allow (which is a blanket invitation) or Allow For Session (which will discard a site's cookie once you close down *Firefox*). If the last option sounds appealing, it's possible to set the browser to remove all cookies on closure. Just select the Until I Close Firefox option in the Keep Cookies drop-down list. Now every website visited will see you as a first-time browser.

To browse cookies, use the View Cookies option at the base of the dialog box. This will present you with a long list of cookies that have been set on the machine you're using. They are organised by originating site, so, for example, cookies set by **www.google.co.uk** will be under a different heading from those set by **www.google.com**. Hitting the small disclosure icon beside the site name will give you more information about the number of cookies that the site uses, and selecting one of the cookies will tell you about the host, the originating domain (sometimes) and the expiry date *(see the image, left)*. Sometimes this last will simply say 'at end of session', which means the cookie will be discarded when *Firefox* is shut down. As well as being able to search for individual cookies, you can delete individual ones or remove every cookie on the machine.

The all-seeing option

There are a couple of good cookie management extensions for *Firefox*. If you're simply concerned with knowing what a site is dropping on to your PC and being able to delete cookies after the fact, *View Cookies* is a useful download. It adds an extra tab to the Tools > Page Info dialog box (called, appropriately, Cookies), which allows you to view and delete any cookies deposited on your machine by the currently viewed page.

The second extension I'd recommend is more invasive (you'll be reminded of it at each new site) but also more useful if you're concerned about the security of your browsing habits. By installing Permit Cookies and setting *Firefox* to stop any site from »

THINK PUBLIC

This tutorial looks at ways you can hide your browsing habits from someone else with local access to your machine. It has not covered more extensive private browsing through anonymiser services or proxy servers, which can almost completely mask a user's IP address. This is an important distinction, because the police, customs and a wide range of other public bodies can apply for a warrant to see web logs (not blogs) kept by your ISP if they suspect that you're involved in criminal activities, and these can be tied to individual IP addresses over time. Unless you're willing to put in an enormous amount of effort, you should always assume that your browsing habits have more in common with postcards than letters and that someone somewhere is keeping records. Proxy servers are usually spirited away in places where the UK/US/Whatever authorities have no jurisdiction. But, of course, they also keep records. Big Brother *is* watching you.

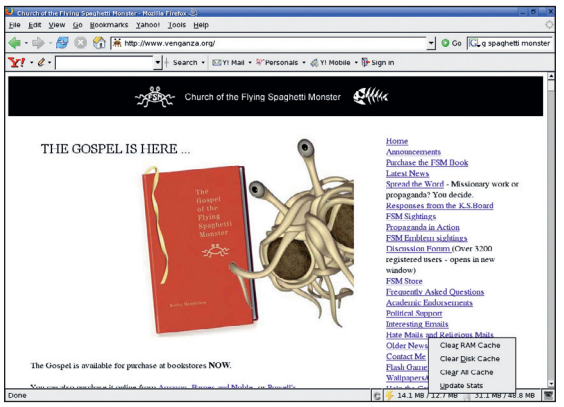
setting cookies – as discussed earlier – you will be prompted on a page-by-page basis to allow or forbid a cookie to be dropped on to your computer. Moreover, it's possible to change the settings as you browse. You might, for example, allow a cookie to be set and then change your mind. With Permit Cookies installed, it's possible to hit the small 'C' icon at the bottom right of the browser window to see which cookie is active and change its permissions.

As ever, there is a trade-off between security and convenience; you can have all your Amazon preferences and passwords remembered, but anyone who uses the computer (or who gains access to it by some nefarious means) can use it to buy books on your credit card. If you opt for convenience, I would recommend having a regular (weekly or, at the very least, monthly) cookie clearout. You may need to re-input some passwords as you browse, but that's a price worth paying.

Extensions such as *Permit Cookies* hand more control back to web users – which is *Firefox*'s guiding philosophy.

PART 2 – CLEARING YOUR CACHE

The next important area of investigation is the browser cache. This is simply a backup of pages that you've visited, built with the intention of speeding up browsing. As an example, imagine that you visit the *Linux Format* website ten times a day to check up on forum postings. By using the cache, the browser won't have to download persistent data such as the images used on the site and, if nothing has changed since the last visit, will use the cached page. This is brilliant in terms of saving bandwidth and speeding up browsing, but a disaster from a security perspective if you're attempting to cover your tracks. As with cookies, *Firefox* has a built-in method for clearing the cache, but it's basically an all or nothing proposition.



The *Cache Status* extension shows how much cache space is being used and gives you a quick way to clear it.

The cache settings are in Edit > Preferences > Security under the Cache tab. This is a very sparse box containing a space for defining how much disk space is set aside for the web cache, and a button labelled Clear Cache. Hitting the latter will, as expected, clear out any cached data. At the very least, this should be done every week or so.

There are more pressing concerns with cached content than the problem of another user of your computer knowing what sites you've visited. Other websites may gain access to this data using non-cooperative cache scanning. According to Collin Jackson and colleagues at Stanford University, this type of cache scanning may allow website owners to discover, in some detail, your browsing habits. A cache attack could be used like this: **siteone.com** takes an image from **sitetwo.com** and embeds it in a page where you can't see it. You visit **sitetwo.com** and the image is cached, alongside some metadata such as when the site was visited etc. When you visit **siteone.com** it checks the cache and realises you've been to **sitetwo.com** and can extract information about your browsing.

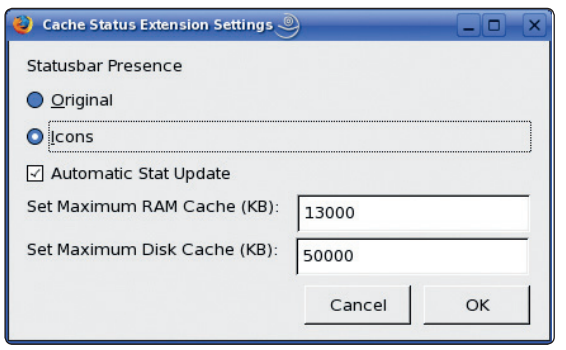
At the website **www.safecache.com**, Jackson *et al* go into some detail about the other ways in which cached content can be used to invade a user's privacy. They have also come up with a solution: a *Firefox* extension they've coded that segments cached content according to the domain of the originating page and prevents cache-based privacy attacks. Basically this means that cached content can be used only by the originating site, and not 'reused' by a different site so that no information is leaked about the user's browsing. The drawback is that some cache 'hits' are returned as 'misses', which will have a slight impact on efficiency, and according to some reports, SafeCache can adversely affect any customised toolbars you may have. In three installations, however, I didn't encounter any serious issues.

Speed boost

More prosaic cache management can be achieved with the Cache Status extension. The latest version, 0.6.2 at the time of writing, gives easy access (on the bottom status bar of the browser) to information about the browser's use of RAM and disk space and users can clear either cache with one click. The same data is also available by typing 'about:cache' in *Firefox's* address bar, but this extension puts it right there in real time.

The Cache Status extension has an added benefit. *Firefox* tends to cache a lot of information in RAM in the name of providing quick access to previously visited sites; the problem is that in a long browsing session this can affect the performance of the browser and other applications, so it's quite a good idea to clear the cache occasionally. To do this, right-click on the area displaying the cache information and select Clear RAM Cache (or Disk Cache if necessary). The figures in the status bar show how much available space is being used, so a display of '1MB/13MB' would tell us that the browser is using 1MB of the 13MB that has been set aside for cache RAM.

Helpfully, you can also adjust the size of both RAM and disk caches in the extension's preferences. Go to Tools > Extensions, select Cache Status and hit the Preferences option. If you're pushed for space on the browser's status bar, it's possible to display icons only for the extension (also in the Preferences dialog), with the rest of the information shown as a tooltip when the mouse is hovered over the icons.



***Cache Status* has tools for configuring options in *Firefox*. Dialup users might want larger figures in these boxes, but 13MB of RAM and 50MB for disk cache seems adequate.**

PART 3 – THE END OF HISTORY

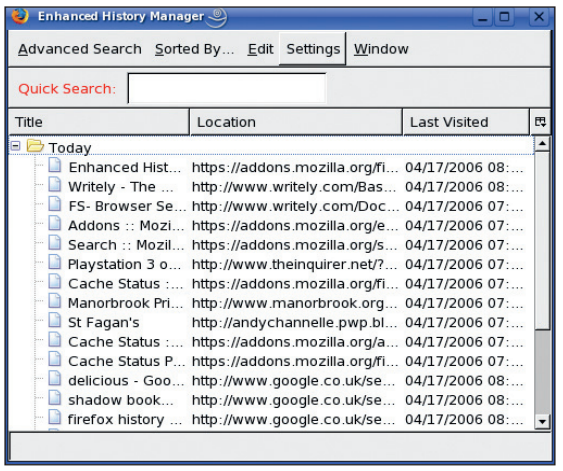
For anyone attempting to hide their browsing from other users of the same computer, the History feature is the biggest threat. To see it in action, hit Ctrl+H or select View > Sidebar > History. Here for the world to see are the last nine (by default) days of websites that the browser has served up. What's more, this History can be sorted into alphabetical, chronological or 'most visited' order, and thus provides other users of the same computer with an enormous amount of information about the sites (and each page within a site) you've visited.

As with the other issues we've covered, *Firefox* makes it possible to erase the browser's history through the normal Edit > Preferences > Security dialog – look under History – and this again should be done regularly. The downside of clearing the History is that website addresses will not be predicted in the address bar when you begin typing and, obviously, the information won't be available if you can't quite remember where you saw that rare Smiths single advertised. (Tip: use a bookmarking site such as Shadows, **www.shadows.com**, or Delicious, **http://del.icio.us**, if you need to keep your bookmarks and Favourites out of the browser.)

The sneaky geek

More control over your History is available through the Enhanced History Manager extension, accessible with Ctrl+Shift+H. EHM provides a wealth of search and edit options including the ability to delete individual entries and, more usefully, everything from a particular domain. As an example, let's imagine that I have purchased a T-shirt from **www.thinkgeek.com** for my geeky partner. When she's next online it's quite possible that she will visit the same site and, by beginning to type the address in *Firefox's* address bar (or just anything beginning with 'www.thi...'), may happen upon the very present I don't want her to see. The 'address bar stumble' is how one woman discovered that her boyfriend was regularly visiting dating websites. Yikes.

With EHM installed, I can make my purchase then open the management window (it's best to do Go > History Manager from the menu bar rather than open the sidebar) and search through the History using 'thinkgeek' as the search string. Now



A person's browser history can say a lot about them and their habits. Fortunately, this one has been heavily edited!

I'd select any entry and from the resulting list do Edit > Delete All From **www.thinkgeek.com** or – to be even more comprehensive – Delete All from Entire Domain. This will remove all of the browser's history relating to that site. Of course, you can also use EHM to kill the browser's entire history.

There is give and take in this process, and you must work out a personal security policy that best combines ease of use and privacy. You might need to give up a bit of the latter to improve the former. For the really dedicated, I would recommend the Distrust extension. This can be switched on with a single click and will monitor cookies, the cache and History for a single session. When you click on the icon again, or invoke the Distrust menu entry (secreted in the Tools menu), it will remove the browsing trail for that session only.

So, for example, if I were buying a birthday present for my partner, I would launch *Firefox* and click on the Distrust icon before visiting the Ferarri website and placing my order. When finished, I would hit the icon for a second time to clear out my cookies, cache and history so that no one can accidentally stumble across my data. *Facile, no?* LXF

GLOSSARY

■ **Cache** When a user visits a page, its data is added to a browser cache, which can be checked against the page on subsequent visits so that the browser only has to download new content. It is possible for a snooper to look through cached pages (and all the data associated with them, such as time and frequency of access, etc) on a machine.

■ **Clickstream** Your clickstream is basically everything you do on the internet. It is, understandably, a very valuable commodity and it is access to it that makes free services from such companies as Google, Yahoo and, increasingly, Microsoft viable from a business perspective. For more information about clickstream ownership, visit **www.attentiontrust.org**.

■ **Cookies** Contrary to popular opinion, cookies are not programs that collect information on your browsing habits. They are, instead, small text files that can be paired with a more extensive profile on a web server. The data on the server may record when and how often you visit a particular site, and which address you can from and went to.

■ **History** Every web browser keeps a record of a user's surfing. This means, for instance, that when you begin to type an address, the browser can automagically suggest matches based on what has previously been typed. Incidentally, if you use Google's Personal Homepage (**www.google.co.uk/ig**) and its personalised search option, your entire search history from the moment you signed up for the service will be available through the page – and is searchable. It is possible to switch off and abandon this option through the settings page, but I have found it's a decent, password-protected alternative to the *Firefox* History option.

■ **IP address** Your IP address is the series of four numbers (eg 192.168.0.1) that uniquely identify every PC connected to a network or the internet. Most ISPs provide a dynamic IP address, which means it changes every time you log on to the internet. However, records are kept of which user has a particular IP address for up to seven years and police or other statutory bodies are allowed to request this information if a person is suspected of criminal activity.

■ **Proxy server** A proxy server can be used to (almost) anonymously browse the internet or circumvent blocking software that might be installed by an employer, university or government. *Firefox* has a number of proxy server extensions, but they are quite complicated to use.

NEXT MONTH

Try various methods for opening documents, associating file types with apps and automatically launching programs at boot-up.