

The Academy of Plumbing 40 Privacy: part one

You'll have heard of the Digital Economy Bill, which by now might well be the Digital Economy Act, and its provisions for the use of "orphan works" that so many of us have so vociferously protested against. Its primary purpose is to crack down on Internet piracy. Illegal downloading of copyright films, music, and stuff like that. Amongst other things it contains provisions to force ISPs to retain IP addresses of illegal downloaders, to retain logs of who sent e-mails to whom, and lists of which websites you have visited.

All of this is done in the name of protecting legitimate copyright holders' rights and to combat organised crime and terrorism. It all looks hard to argue with. Indeed, all along, the Government's position has been that if you have nothing to hide, you have nothing to fear. Well, yes. On the other hand, the fact that you have nothing to hide does not mean that you should be obliged to let in anyone and everyone to see what you have - it's rather like saying that you should give these people the keys to your doors. So, we must start to think carefully about how to keep our Internet communications more private, because there appear to be as many ways of electronically invading our privacy as there are grains of sand on the beach and it's hard to put technological genies back into their bottles.

COOKIES. MMM...

Most websites that you visit download and store on your computer little text files called cookies. These files contain

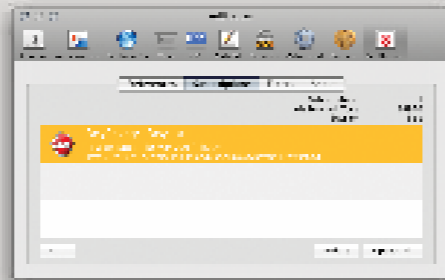
all sorts of data: your site account details and preferences; the date and time of your last visit; a tracking ID code so that the website can see if you have visited before. Some websites won't work without these cookies being enabled. For many purposes, cookies are perfectly innocuous. The real problems tend to come from Internet advertisers who also place tracking cookies onto your computer so that they can track which sites you have visited, how frequently, and how you got to them, so that they can sell this data. These are rather less pleasant.

Firefox contains built-in functions that enable you to control which cookies are stored, how they are stored, and when they are erased. Firefox, Camino, and other browsers can also block adverts and pop-up windows. Unfortunately, apart from its pop-up window filter, Safari doesn't do any of this. Fortunately, a couple of free add-ons deal with the problem very well. Safari AdBlocker blocks adverts; Safari Cookies controls cookies. I have run Safari AdBlocker or a predecessor, PithHelmet, for several years and am so accustomed to viewing a virtually ad-free Internet that on the rare occasions I am forced to turn it off, I am struck by how most commercial websites look like those full-page adverts from Comet that you see in the red top newspapers.

A further advantage of blocking ads is that the Web speeds up: there is simply less data to download. Use these utilities. Both can be set to allow ads and/or cookies on a site-by-site and even page-by-page basis.

The Digital Plumber

By Paul Ellis



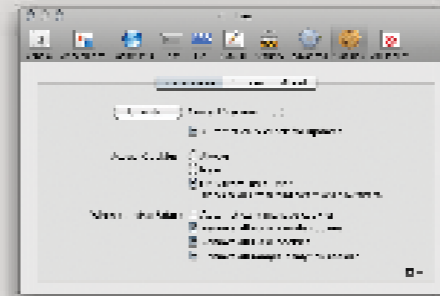
Safari AdBlocker

FLASH COOKIES

Flash is all over the Internet. Many photographers' websites are built using Flash: for years it has been the easiest and most consistent way to create a website featuring sophisticated design and interactivity. More recently Flash has become used to deliver Internet advertising. It's little-known by Web users that Flash can store its own cookies. Unlike traditional browser cookies, Flash cookies are not controlled through the cookie privacy controls in a browser, which means that even if a user thinks they have cleared their computer of tracking objects, they most likely have not.

CHEEKY BLIGHTERS

Web advertisers love this functionality and spray Flash cookies all over the place. Several services even use this surreptitious data storage to reinstate traditional cookies that a user has deleted. So even if a user gets rid of a website's tracking cookie, that cookie's unique ID will be assigned back to a new cookie again using the Flash data as the "backup". Sly, eh? Safari Cookies can be set to delete Flash cookies when Safari quits. The add-on BetterPrivacy does a similar job for Firefox.



Safari Cookies

CLICKTOFLASH



ClickToFlash blocking Flash advert

Do you really need to see your webpage distractedly flashing ('scuse the pun) with animated gewgaws? ClickToFlash stops Flash loading in the first place, replacing Flash movies with placeholders. This speeds things up no end and prevents multiple instances of the Flash plugin from leeching your CPU power. One click on the placeholder and Flash loads. Essential.

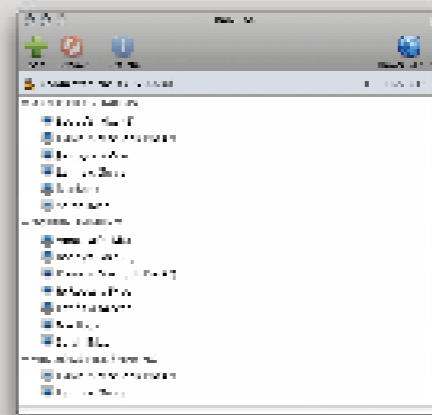
That's Flash and cookies taken care of, but what do we do about people spying on our communications while in transit? If we are at home or in our studios and we have a properly-secured wireless network using WPA2 security, we can be reasonably confident that no one on our little network is spying on us. This is not the case elsewhere. Internet cafes, public wireless hotspots, hotels and similar are all likely to have lots of users on their network, some of whom can easily be script-kiddies sniffing the data packets that travel over the local network for juicy tidbits. How do we keep them out?

TUNNELLING

Corporates invariably use VPNs (virtual private networks) to create a secure encrypted link or tunnel directly from offsite computers to their company network. VPNs are very useful because they scramble your datalink in a way that is very difficult to decipher and send all of your communications down this link, which keeps out prying eyes and enables you to go to places such as banking websites and view content that it might be unsafe to from your current location.

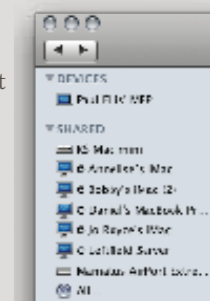
THE EASY WAY

Unfortunately, VPNs can be a pig to set up. Macintosh users have access to a couple of shareware programs that aim to provide the functionality of VPNs without their headaches. I've written about ShareTool before. I use it myself and have found it to be quite reliable. It allows you to share files, share screens, remotely print, and share other network resources as if you were at home or in your studio. Crucially, it also works as a web proxy for Firefox which means that if you use Firefox as your browser, you appear to the Internet to be browsing the web from your home IP address, not from the IP address of your current location. There can be lots of advantages to this, if you think about it. Sadly, Safari is less easy to automatically set up in this way.



ShareTool, connected

A new application called Slink does very much the same thing as ShareTool but with some advantages. ShareTool needs to know the current IP address of your home network and has a rather ugly way of storing that as a favourite for later recall. Slink uses a DNS-like system to keep an up-to-date record of your home network's IP address in much the same way that MobileMe's Back To My Mac does. This method is secure and Slink has a rather nicer user interface than ShareTool. Use one of them, and keep those prying eyes out when travelling. Next time: e-mail privacy.



ShareTool's remote network computers



Slink, connected

LINKS

Safari AdBlocker: <http://bit.ly/37rdIw>
Safari Cookies: <http://bit.ly/FoKti>
BetterPrivacy: <http://bit.ly/BZRQx>
ShareTool: <http://bit.ly/brQIW2>
Slink: <http://slinkware.com/>

PDFs of this and all my other IMAGE articles are available to download at www.thedigitalplumber.co.uk, each with live weblinks for your browsing pleasure. Go and get 'em.

© Paul David Ellis, 2010. All Rights Reserved.