Erasing your web browsing history.

Web browsers have the habit of storing information about the sites you visit "for your own benefit". When you close the browser, quite a lot of personal information is left behind in the form of cached pages, 'cookies', history, registry entries and index.dat files (Windows), or .plist files (MAC). This is done to make it easier for you to revisit those sites with minimum effort. If you feel that you need to erase this information once you finish using the computer, you should investigate how to do it for your particular browser and operating system. Even if you know how, it will probably take you all afternoon to clean up after using the internet. Not a practical proposition for the security-minded professional (or the paranoid). There is some cleanup capability in most browsers, but information is frequently left behind. Some cleanup software vendors claim that their offering will erase the offending files from your computer, but you never know. Keep in mind that even if you delete all those files, it is possible to recover them with specialized software: I can do it, and so can the bad guys. Is it dangerous to leave stuff behind after going on the internet? It all depends on how advanced your paranoia is.

Some useful alternatives to just deleting personal information.

All major web browsers (IE, Firefox, Opera, Safari, etc.) come in "portable" versions. These are made by hackers (and, who knows, possibly by the bad guys themselves). The programmers basically use the installer for the application and expand it into a self-contained folder. The idea is that you keep the "portable" browser folder in a USB memory stick and run it from there. The claim is that this doesn't leave any personal information in the computer. Everything is saved to the memory stick (you remove it and nothing stays behind). I have two observations: there is no guarantee that the hacked software is well written (some information may find its way to the computer after all), and you don't know if it comes with a malicious payload (a Trojan that sends information to the bad guys). However, if you get hold of a portable browser with a good reputation it could solve your privacy problems. Portable Firefox is worth considering. But use them with caution: portable browsers are not the real thing.

Run the web browser in a sandbox.

The idea is similar to that of the portable browsers. You install software in your computer that allows you to run your normal browser, but keeping all the files the browser generates in a single folder. When you finish the internet session, just delete the folder and all your personal information is gone to the recycle bin. The software I use is called Sandboxie (free download from the internet). It works very well with Firefox and Internet Explorer. Another option is Kaspersky Internet Security (an antivirus program) which comes with the sandbox virtualization technology as part of the package for web browsing. For even greater security you can use a “file shredder” program to make the deleted sandboxed folders completely unrecoverable.

Run your PC from a CD or USB memory.

It is possible to run your computer from a CD or USB memory stick. The idea here is to access the internet without using the hard drive at all (you can physically remove the HD before attempting this). There are many options, for example the Ubuntu (linux) live CD and Active@ Boot Disk. Some Sony VAIO laptops come with a "quick web access" start button which does the same thing from a special chip on the motherboard. In all these cases the web browsing history disappears from RAM memory as soon as you switch off the computer. You can always save files to USB memory during one of these sessions.

Make an image of your system.

I keep a clean "image” of the system partition of one of my computers. The software I use is called Acronis, but there are others. After a few days of internet use I simply overwrite the system partition with the saved image and I have a clean computer again. You don’t even have to worry about picking up a virus: If you do, you just overwrite the partition again with the saved clean image. Any data you had in in the system partition becomes automatically unrecoverable because the whole partition gets overwritten. The down side is that it can take an hour to install the image (the bad guys have fast cars) and you lose all your new downloads and installations. Apart from safety considerations, imaging the system partition is a must if you "experiment" with your computer.

If you are interested, look up some of these software packages in the internet. And don’t forget to cover your tracks!