21 Ways to Buff Up Your Browser

You probably spend more time working (and playing) in IE, Chrome, Firefox, or Safari than in any other application. Here are our favorite tips, tricks, and add-ons to supercharge your Web browser.
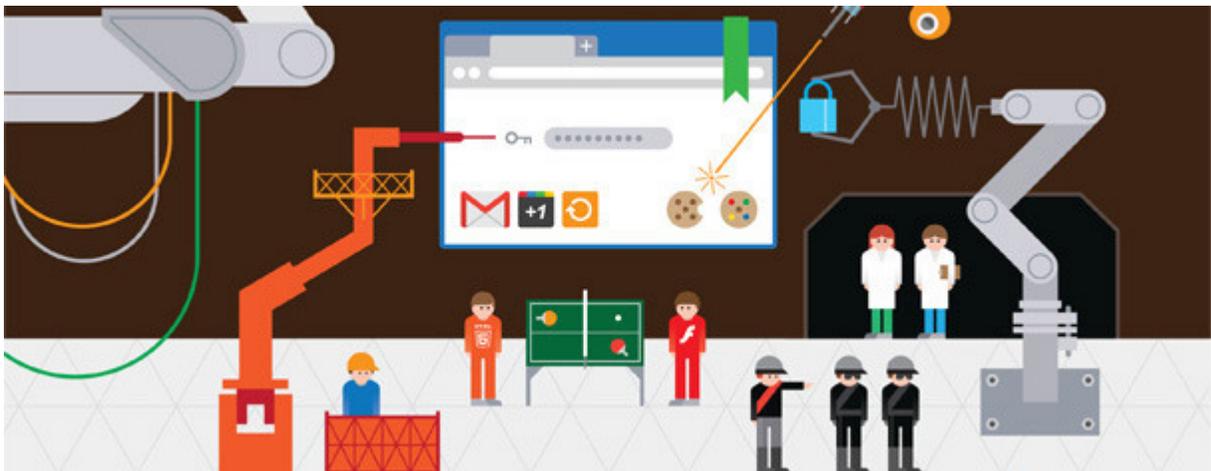
By Patrick Miller, PCWorld

Illustration by Papercut.fr

Whether you are at home, work, or school, odds are you spend a lot of time staring at your Web browser. So why does it look—and run—like everyone else's? This collection of our favorite browser secrets and extensions can make your browser safer and more efficient than ever—and help you figure out what's wrong when things don't work as you expect.

Unless stated otherwise, our tips are for all of the four major browsers: Chrome, Firefox, Internet Explorer, and Safari.

Editor's note: *For an in-depth comparison of the latest versions of six browsers for PCs--Opera and RockMelt as well as the four covered by our tips here--see* "Which Browser Should You Use?"; *for our appraisals of five popular mobile browsers for the Android operating system—Chrome for Android Beta, Dolphin Browser HD,*

Firefox for Android, Opera Mini, and Opera Mobile—see "The Best Browsers for Your Android Phone."

Use These Essential Tips and Extensions

1. Automatically update your Web browser. The easiest way to keep it stable and secure is to set it to update automatically so that you're always using the latest version. Fortunately, each major browser, by default, updates automatically. Safari receives updates from Apple Software Update (installed by default with Safari, or other Apple software), Internet Explorer gets updates from Windows' built-in Windows Update feature, and Firefox and Chrome both check for new updates whenever you launch the browser.

If you think auto-updating has been disabled, here's how to reenable it:

For Internet Explorer, go to *Control Panel, Windows Update, Change settings,* and set the drop-down menu to *Install updates automatically.* This setting will make most Windows updates install automatically, too.

In Safari, find the Apple Software Update tool on your PC, either by pressing the **Windows** key and typing in **Apple Software Update** or by going to *C:/Program Files (x86)/Apple Software Update* and opening *SoftwareUpdate.* Inside the tool, click the *Edit* menu, choose *Preferences,* and set the update frequency to either *Daily* or *Weekly.* Apple Software Update doesn't download updates without you approving each one, so you don't have to worry about accidentally updating something that you don't want to.

In Firefox, click the *Firefox* menu; choose *Options,* click the *Advanced* tab at the top, click the *Update* tab, and make sure the boxes under 'Automatically check for updates to:' are checked.

With Chrome, you can't disable auto-update without monkeying around with command-line options or your Windows Registry. However, if Chrome finds a new update during a browsing session, it will show a little arrow next to the wrench icon at the top-right of the window. Just click the wrench and choose *Update Google Chrome* to install.
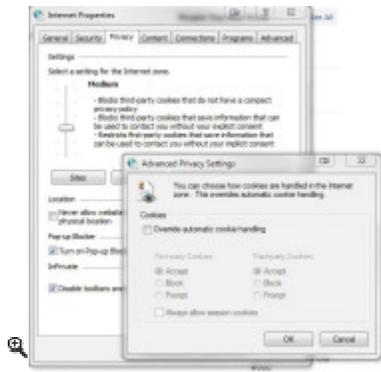
Block third-party cookies that track your browsing.

2. Disable tracking cookies. Cookies are great, especially if you don't want to type in a password every 30 seconds. Few people, however, like the kind of cookie that follows you from one website to another to report to advertisers on what you're looking at. But you can block those "third-party" cookies without getting rid of the useful kind.

For Internet Explorer, go to *Control Panel, Internet Options,* click the *Privacy* tab, and either choose a preset on the slider that blocks third-party cookies, or click *Advanced,* check *Override automatic cookie handling,* and check *Block* under 'Third-party cookies'.

In Safari, go to *Edit, Preferences, Privacy,* and set 'Block cookies' to *From third parties and advertisers.*

In Firefox, go to *Firefox, Options, Privacy,* and select Use custom settings for history from the drop-down menu. Uncheck Accept third-party cookies.

With Chrome, go to *Options, Under the Hood, Content Settings,* and check *Block third-party cookies from being set.*

Crash prone? Lazarus saves data you enter into Web forms.

3. Save your form data with Lazarus. *(Browsers: Safari, Chrome, Firefox)* Did your browser crash just when you were about to send a lengthy, painstakingly composed message? Never again. Grab Lazarus, and it will automatically save whatever you had been typing before the crash.
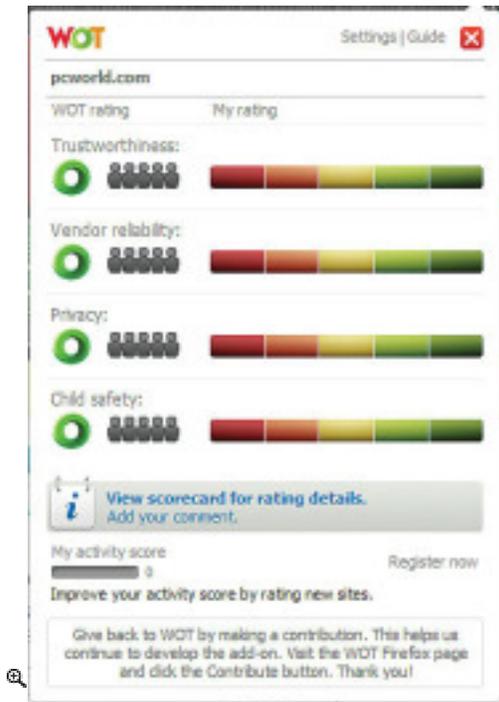
 Use Web of Trust's safety ratings for links.

4. Stay safe with Web of Trust. Not sure whether a link is safe? Web of Trust can help. Just install the WOT extension into your browser of choice, and you'll see a little circle pop up next to every link on the page you're viewing. The circle's color—a traffic-light red, orange, or green—represents an aggregated safety rating from millions of other Web of Trust users for trustworthiness, vendor reliability, privacy, and child safety.

5. Sync your bookmarks. It's 2012—and you shouldn't have to manually wrangle your collection of bookmarks on each PC you work on. Fortunately, several different bookmark-syncing tools are available, depending on which browsers you use. For Chrome, you can just log in with your Google account in *Options, Personal Stuff* and sync your bookmarks, history, extensions, and more from PC to PC. Safari can likewise sync through iCloud to Safari for Mac or PC, as well as whatever iOS devices you use with your iCloud account.

If you're not 100 percent committed to your Apple/Google/Microsoft services, however, you'll be better served by Xmarks, a free cross-platform browser add-on that will sync your bookmarks with a simple browser extension. If you're willing to shell out $12 a year, you can sign up for the Premium service to sync to iOS, Android, and BlackBerry browsers as well. Xmarks has versions for Firefox, Internet Explorer, and Safari.
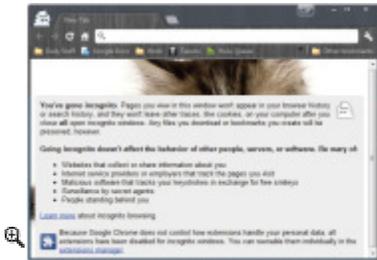
As a privacy measure, go incognito in Chrome.

6. Stay incognito and clear your history. Web browsers generally make note of pretty much every page you visit, which usually is really useful. But each major browser has a private browsing mode that won't log whatever you're doing. Internet Explorer 9 calls its mode InPrivate Browsing (**Ctrl-Shift-P**), while Chrome's name is Incognito Mode (**Ctrl-Shift-N**). Firefox has a Private Browsing mode (**Ctrl-Shift-P**), and Safari does, too (go to the *Edit* menu and choose *Private Browsing...*).

If you forget to use the private browsing mode when you meant to, you will have to clear your browser's history (and possibly your URL autocomplete or form autofill logs, as well). You can do that with **Ctrl-Shift-Delete** in Internet Explorer and Firefox, but for Chrome you must go to *Options, Under the Hood, Privacy, Clear browsing data;* and for Safari, click the *History* menu and choose *Clear history*.

7. Easily zoom in and out. Web pages aren't always as easy to read as they should be. But you can zoom in or out of any Web page by holding down **Ctrl** and rolling the scrollwheel up or down to zoom in and out as you like. Alternatively, keyboard warriors can use the **Ctrl+** and **Ctrl**- keys to zoom in and out incrementally.

Lock Down Your Browser

8. Quarantine your at-risk apps with Sandboxie. You can add an extra layer of defense to your PC by setting up a sandboxing application, which lets programs and processes run in an isolated virtual environment. Programs running within the sandbox have limited access to your files and system, and they can make no permanent changes, thus protecting you from malware that your antivirus utilities miss when you're shopping online or browsing unsecured websites. Sandboxie ($40 shareware) is a utility that allows you to open your Web browser, email client, and any other program inside customizable sandboxes. Detailed setup instructions are at the link.

LastPass can generate secure passwords for you.

9. Get a password-management app. Adding "1" to the end of a password that happens to be your spouse's first name isn't fooling anyone. Even if you're using really complicated (and hard-to-remember) passwords for important sites, odds are good that you have them written down in an unencrypted text document somewhere on your PC, or saved in your browser—which anyone who gets access to your PC can view in plain text just by going to your browser's privacy settings. You need a password management app like LastPass; Basic is free, Premium is $12 per year) or 1Password.

Various password managers offer different features, but the basic function is the same: Remember one secure password for your password manager, and the tool can generate assorted hack-resistant passwords for all your oft-used websites and services. That way, you don't risk using the same password for all your email, social networking, and online banking accounts, but you don't have to remember two

dozen different passwords that are each 20 characters long. What's more, most password managers include portable apps that you can keep on a USB drive, and mobile apps to ensure that you can access all your important sites from your tablet or smartphone (although this may cost extra). Read "Password Management: Idiot-Proof Tips" for the specifics.

NoScript disables active elements of a Web page.

10. Just say no to Web scripting. *(Browsers: Firefox, Chrome)* JavaScript, Flash, Silverlight, ActiveX—these Web scripting languages can make your Internet experience a joy (streaming video) or a pain (malware and ads). To make your browser as secure as possible, grab NoScript for Firefox or NotScripts for Chrome, and your browser will default to disabling all "active" elements of any Web page you visit before they load. Then, you can selectively load the scripts that do things you want (stream video, say) and ignore the ones that do what you don't want (report back to Internet advertisers). That will help prevent "clickjacking" scripts (when you think you're clicking on an image, you're actually activating a script that will post spam to your Facebook or Twitter account), as well as "cross-site scripting" attacks where hackers can hide data-stealing code in your favorite Web app's security holes without setting off any malware alarms.

Stay on Top of Your Social Networks

Yoono helps you track your social networking accounts.

11. Use Yoono to bring your social networks together. *(Browsers: Firefox, Chrome)* Yoono is a social network aggregator that lets you easily view your feeds and post to Facebook, Flickr, LinkedIn, Twitter, and a few other chat and social networking services, so you can confine all your distractions to one tab. While you can use the Yoono website from any modern browser, you can also use a Yoono extension for Firefox and for Chrome that provides the same functionality from a humble button in your browser window. Now you can procrastinate even more efficiently!

12. Block all sharing buttons. *(Browsers: Firefox, Chrome)* On the other hand, if you lead the pack in considering social networking a nuisance, you might like Antisocial (Chrome) and ShareMeNot (Firefox). (For download locations, see the next item.) Both extensions interfere with the sharing buttons that saturate the Web these days—Facebook's "Like" or Google's "+1", for example. Antisocial keeps these buttons from loading, while ShareMeNot prevents them from automatically reporting back to their parent service with tracking information on the sites you're visiting.
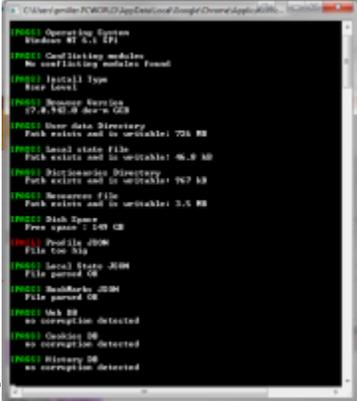
13. Search for your social networks of choice. Every browser has site-specific extensions for people who regularly use popular social networking or news aggregation sites. Search the Chrome Extensions listings for Facebook, and you'll find extensions that ditch the News Feed, let you download entire photo albums, and even notify you when people unfriend you. Find listings of vetted extensions for Internet Explorer at the Internet Explorer Gallery, for Firefox at Mozilla's Add-ons for Firefox page, and for Safari at Apple's Safari Extensions Gallery.

Troubleshoot Browser Issues

14. Tweak (or toss) your PDF plug-in. PDFs can throw a wrench into your browser's works. Not only is keeping Acrobat Reader updated a pain, but slower PCs will often choke for 30 seconds or so when you click a link to a PDF. Try using Foxit Reader instead of Adobe Acrobat Reader; it's a bit leaner and meaner than Acrobat (just be careful not to install any of the toolbars it tries to foist on you). Once Foxit is installed, go to *Tools, Preferences, File Associations* and uncheck *Display PDF in Browser.* The next time you click a link to a PDF, your browser should download it and open it in Foxit, which should keep your browser's other tabs accessible.

15. Keep multiple browsers handy, especially for Flash. Flash can be finicky, especially when dealing with
processor-pounding applications like streaming video. If your Flash applications consistently crash with certain websites or services, try accessing the same site in a different browser and see if that helps. On my home PC, for example, Hulu crashes my graphics card driver repeatedly in Chrome, but works rock-solid in Firefox.

16. Know your diagnostic modes. Most browser extensions and add-ons are fairly lightweight, but if you binge on them, they might not all play nicely together. Luckily, most browsers have a few diagnostic tricks up their sleeves.

Chrome has a built-in mode for running self-diagnostics.

First, know how to put your browser in its safe mode, where it won't load any outside extensions: Open up the *Run* prompt from the Start menu *(Start, All Programs,*

Accessories, Run); then, for Chrome, type **chrome.exe --incognito**; for Internet Explorer, type **iexplore -extoff**; in Firefox, click the *Help* menu, and choose *Restart with Add-Ons Disabled.* Once in its safe mode, see whether your browser still crashes. If it's stable, selectively reenable extensions until you've isolated the culprit.

Besides the safe-mode approach, Chrome also offers a built-in diagnostic check. To access it, just open the *Run* prompt and type **chrome.exe --diagnostics**.

Finally, Safari doesn't have any fancy tricks for loading into a safe mode; simply go to *Edit, Preferences, Extensions,* and set the switch that appears at the top to *Off*.

17. Speed up your Net connection by changing your domain name server. Your Internet service provider's Domain Name System server translates the URLs you type (www.pcworld.com, for example) into numeric IP addresses so you can get from point A to point B without a hitch. But your ISP's DNS server may not be the speediest in your area. Download DNS Benchmark (aka DNSBench) to see which server is fastest for you; then follow the detailed instructions in "Speed Up Your Internet Connection by Changing Your Domain Name System Server."

18. Keep your toolkit handy. *(Browsers: Chrome)* Troubleshooting browser problems can be tricky because of the many elements to keep track of. Depending on the issues you're having, you must diagnose the browser itself, the PC running the browser, the local network, the Internet connection, and even the website you're attempting to access. Grab IP Address and Domain Information for Chrome, and you'll have one-click access to several different reports on any given IP or domain name, including its location, hosting information, whether it's on spam lists, and more.

Add the Network and Internet Tools extensions, and you'll have another menu that lets you easily use Whois, Traceroute, Ping, DNS Lookup, and other common network troubleshooting tools. Finally, pick up User-Agent Switcher for Chrome, and you can mask your browser to appear to the websites that you're visiting as any browser you like—perfect for sites that insist on specific browsers or versions.

Boost Browser Productivity

Evernote Web Clipper can save a Web page to your Evernote notebooks.

19. Start reading on your PC's browser, finish on your smartphone's. Want an easy way to start reading a Web page on your PC and finish reading it on your smartphone? Depending on your preferred browser, OS, and Web services, you have a few ways to do this. Read It Later is a good browser-agnostic Web service that can save sites for later perusal. If you use Google Chrome and an Android browser, you might prefer the Chrome to Phone extension, which lets you push maps, Web pages, phone numbers, and raw text from Chrome to the appropriate Android app. Evernote fans will opt for Evernote Web Clipper, an extension for Chrome, Internet Explorer, and Firefox that saves a Web page to your Evernote notebooks for easy future reference.

Add new features to your Gmail via its Labs section.

20. Take your Gmail to the next level. Plenty of folks still shy away from Gmail's Web interface. But step into the features offered by Gmail Labs (in the Gmail client, click on the gear icon in the upper right, then on *Settings* or *Themes,* and then *Labs*), and you might find the tweaks you need to switch.

My personal favorites are Multiple Inboxes, which allows you to view your Drafts, Inbox, Starred, and whatever other labels you like from the main Gmail page; Undo Send, which lets you retract a message within a few seconds after sending it; and Preview Pane, which adds an Outlook-esque email preview window so you don't have to click a message to read it. You can also turn on keyboard shortcuts in Gmail by clicking the gear icon, choosing *Settings,* and then checking the *Keyboard shortcuts on* radio button. Master the list of shortcuts, and you'll be whizzing through menus mouse-free in no time.

21. Use TinEye to find an image's origin. No matter how strong your Google-fu is, it's hard to find out where an image on the Web originally came from—and that much harder to give proper credit. Dump your image into TinEye.com, however, and the site will tell you where it came from, whether it's been Photoshopped, and where higher-resolution versions can be found. The first 50 searches a day are free, and an extension for each major browser is available if you find yourself using TinEye a lot.

Remember these tips and grab these extensions, and you'll never want to leave your Web browser again!

Few other tips:
http://www.pcworld.com/businesscenter/article/241219/speed_up_your_internet_connection_by_changing_your_domain_name_system_server.html