How To...

Maximise your browser security

Wayne Williams shows you how to customise your browser's settings to make it more secure

Part 2 | Firefox

Part Two

Mozilla's browser has a good reputation when it comes to security, partly helped by the fact that it's open source. Because anyone can examine the source code (the non-compiled program), vulnerabilities tend to be identified and fixed before hackers get the chance to exploit them. The browser can be made even safer with a bit of light tweaking, and there are plenty of add-ons available that can tighten things up further still.

Get the latest updates

Mozilla releases bug fixes and security patches on a regular basis, so you'll need to check that the automatic updates feature is turned on. Go to Tools, Options, click the Advanced button and select the Update tab. Make sure it's set to watch for new versions of Firefox as well as any installed add-ons. 'Automatically download and install the update' should be selected, as should 'Warn me if this will disable any of my add-ons'.

Protect your passwords

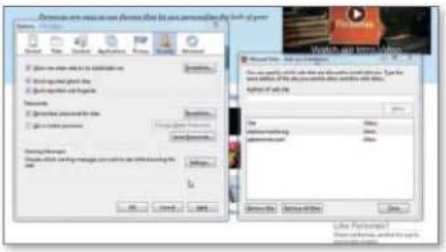
When you log into a website for the first time, Firefox will offer to store the new username and password for you. This is obviously a handy feature and will save you having to remember a whole bunch of different login details. However, it's not particularly secure.

Go to Tools, Options and click the Security tab. Click the Show Passwords button to display the usernames for all the sites it's remembering. Click Saved Passwords to show the passwords. To prevent anyone from accessing these details, you'll need to create a master password. Click the Security tab and tick the option to 'Use a master password'. As you enter your secret word or phrase (preferably made up of a mixture of letters and numbers) the 'Password quality meter' will show you how strong it is.

Firefox can store the login and password details for all your favourite sites. Keep them secure by setting a master password

Missed Part 1 of our browser security How To? Download it at www.webuser.co.uk/244

Control add-ons



You can manage a list of sites that are allowed to automatically install add-ons

By default, Firefox will warn you if a site you are on tries to install an add-on. This is a useful security feature and obviously not one you'll want to disable. However, you can add exceptions – sites that are allowed to install add-ons without your express permission.

To add or manage exceptions, go to Tools, Options, click the Security tab and then click the Exceptions button. You'll see that Mozilla's add-on site (http://addons.mozilla.org), and its Personas themes gallery (www.getpersonas.com) are both already included. Add any other sites you want given the same privilege.

While you're in the Security section, make sure 'Block reported attack sites' and 'Block reported web forgeries' are both ticked.

Control permissions

You can specify which actions a site you are currently on is and isn't allowed to perform. Go to Tools, Page Info and click the Permissions tab. Use the tick boxes to prevent that site from loading images,

Prevent the site you are on from performing certain actions, such as opening pop-ups

opening pop-ups, setting cookies, installing extensions and themes, and/or sharing your location.

Clear your browsing history

When you browse the web normally (not using the built-in Private Browsing mode) Firefox will keep a record of all the sites you have visited. You can clear some or all of this information at any time by pressing Ctrl+Shift+Del and choosing a specific time range – sites visited in the last hour, the last two or four hours, today or everything.

Click the down arrow next to Details to choose what you want to delete, then click Clear Now.

Firefox remembers the sites you visit, but you can clear this record completely

3 GREAT ADD-ONS

HTTPS EVERYWHERE

http://bit.ly/howto1245

■ Automatically encrypts connections to various popular sites including Facebook, Wikipedia, Twitter and PayPal.

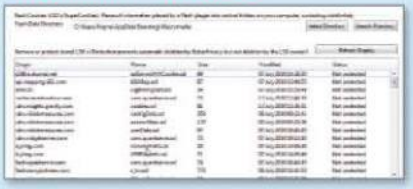
NOSCRIPT

http://bit.ly/howto2245

■ Disables any potentially dangerous executable content, including Java and JavaScript. You can allow or block scripts on a per-site basis.

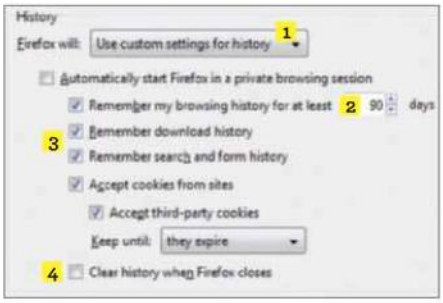
BETTERPRIVACY

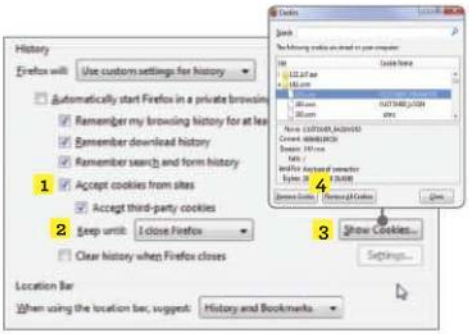
http://bit.ly/howto3245



■ Alerts you to the existence of long-term, non-expiring tracking cookies on your system and removes them for you.

MINI WORKSHOP | Manage your Firefox browsing history





1 As we mentioned earlier, Firefox automatically remembers all the sites that you visit and stores them in its history. To stop it from doing this, you can either use the Private Browsing mode or go to Tools, Options and click the Privacy button. 1 Click the drop-down menu and change the setting to 'Never remember history'. 2

2 Alternatively, you can select 'Use custom settings for history'. 1 This will let you specify how long Firefox should store your browsing history for (the default is 90 days), 2 and whether it should also keep a record of download, search and form information. 3 It's worth ticking the option to clear your history every time you close the browser. 4

3 You can choose whether or not to accept cookies, 1 reject those originating from third-party sources (such as advertisers), add exceptions and specify how long to allow cookies to stay on your system. 'Keep until: I close Firefox' is a good option to use. 2 You can view all currently stored cookies 3 and delete unwanted ones. 4

NEXT ISSUE **How To...** Make Opera, Chrome and Safari secure

On sale 12 Aug