

Firefox content filters

CHILDPROOF

Firefox has a reputation of being the most innovative Web browser. We show you how to apply Firefox's distribution-specific tools to make browsing the web safer for your children.

BY ERIK BÄRWALDT

For the most part, the Internet can be a safe and comprehensive resource for information, but there also is a dark side. In addition to useful, factual content, the Internet can be a source for obscene, irritating, and even downright dangerous sites that are not appropriate for the general public, particularly children.

Filter Problems

Parents and school admins need systems to help filter the content. Web content filters are available for any major operating system, but they are often insufficient. Commercial solutions can be expensive and, depending on the filtering method, may have some disadvantages.

Many web content filters simply access predefined, regularly updated blacklists of blocked Internet addresses or just filter terms recommended by these sites. They do not check the page content, so

dubious pages can still be accessed despite a running content-filter system as long as they have a harmless-looking

URL. On the other hand, the filter might block harmless sites based on keyword definitions. Another problem is that many solutions are complicated to install and maintain and require in-depth network knowledge because they rely on a proxy server. If you want to avoid the hassle but still enjoy the protection of an effective and easily deployed filter, FoxFilter and Public Fox are two good options for the free Firefox web browser.

Foxy Installation

To install either of the filters, you do not need any experience with Linux administration. Simply go to the Mozilla Add-ons page, select the add-on, and then relaunch Firefox [1][2].

If you are working offline and prefer to use a CD or a USB stick for a larger scale installation on multiple machines, Firefox will let you do so via the *File | Open* menu. Firefox identifies FoxFilter and Public Fox as extensions and automatically launches the installation dia-

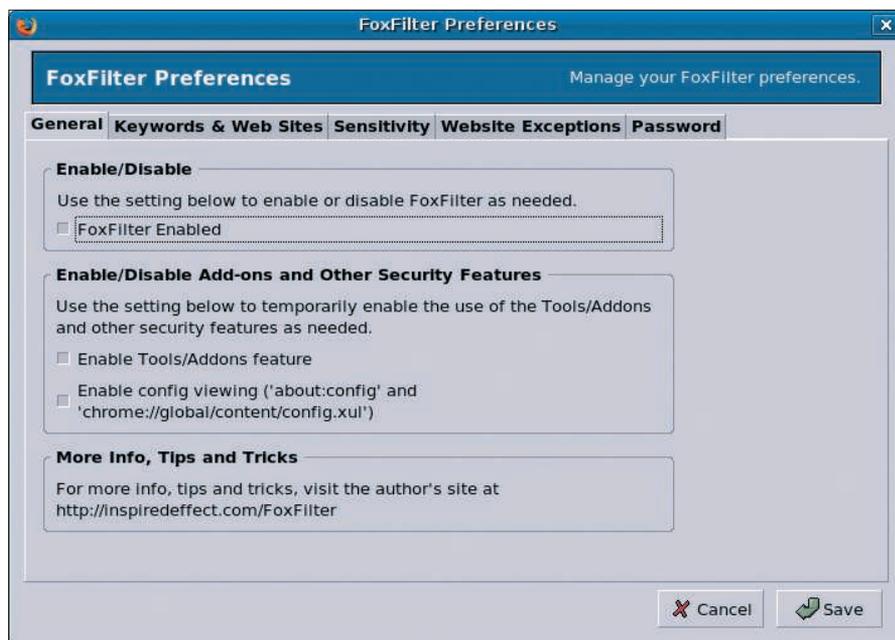


Figure 1: Enabling and disabling FoxFilter.



Jaimie D. Travis, Fotolia

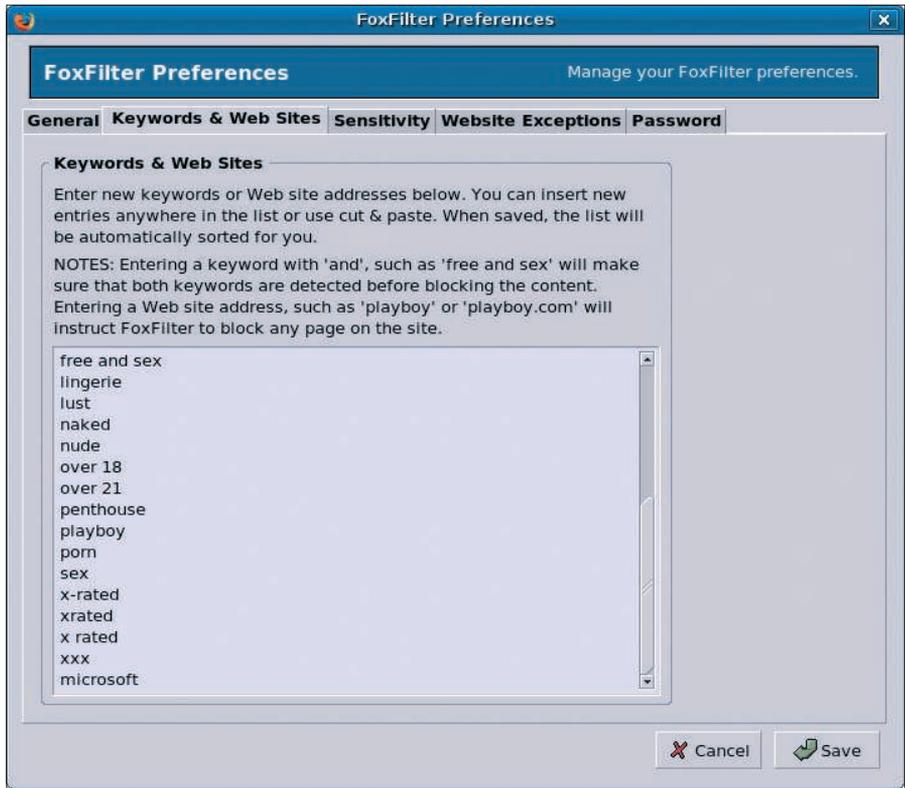


Figure 2: Unlimited options for entering restricted keywords.

log. After you restart the browser, you will have a choice of filters with the default settings already in place.

Foxy Filter

After setting up FoxFilter (version 5.1 reviewed), find the *Foxfilter Preferences* entry in your *Tools* menu. Selecting the entry opens the Preferences window with five tabs at the top.

The first tab, *General*, is for enabling and disabling the filter and for enabling or blocking Firefox plugins and add-ons (Figure 1).

Also, you can disable the configuration view – the view that appears when you type *about:config* in the address box – for the browser here. If you choose this setting, there is no way to modify browser and filter settings via the browser window workaround.

The *Keywords and Web Sites* tab gives you a neat list of blocked keywords (Figure 2).

Logical AND operators are supported here; for example, *free and adult* would only block pages that contain both words. You can add to the default list at any time.

Note that the list is not just for keywords but also will let you block complete domains.

When you restart Firefox, the browser sorts the list alphabetically, making it easy to find individual addresses even if the list grows.

The *Sensitivity* tab is for granular search depth settings. After all, what use is a long list of blocked keywords if un-

desirable, unfiltered content lurks in the depths, hiding behind harmless-sounding URLs? To avoid this danger, FoxFilter offers both an address selection option and an automatic search of the titles and metadata on the page, including the source code.

A complete check of all the content on a website ensures that the filter really will block any undesirable pages (see Figure 3).

The *Website Exceptions* tab gives you the option of listing special pages to which the filter restrictions will not apply. These pages include search engines, for example, because a listing with the search results from a “harmless” search key could retrieve undesirable content, thereby preventing the browser from displaying the whole page. As a rule of thumb, the more restrictive your *Sensitivity* settings are, the longer your list of exceptions will need to be.

The final tab, *Password*, lets you specify a password for the FoxFilter administrator. Make sure you add a password hint, just in case you forget your password. If you do not specify a password, any user can configure FoxFilter. Clicking the *Save* button at the bottom of the page stores your FoxFilter settings and immediately applies them.

Whenever FoxFilter finds undesirable and indexed content or keywords when

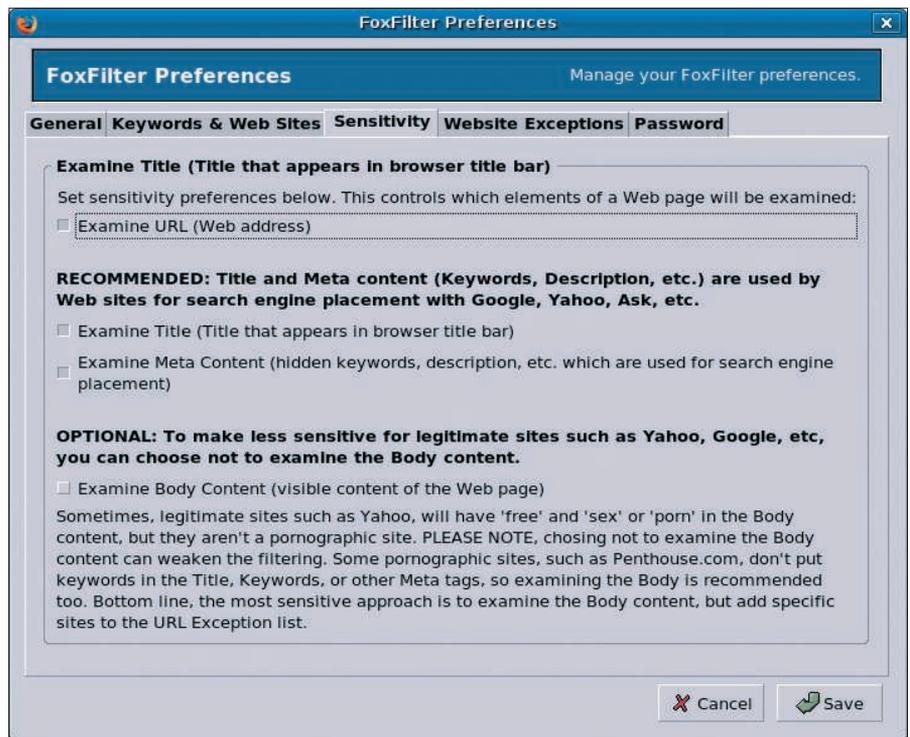


Figure 3: Setting the search depth in the Sensitivity tab.

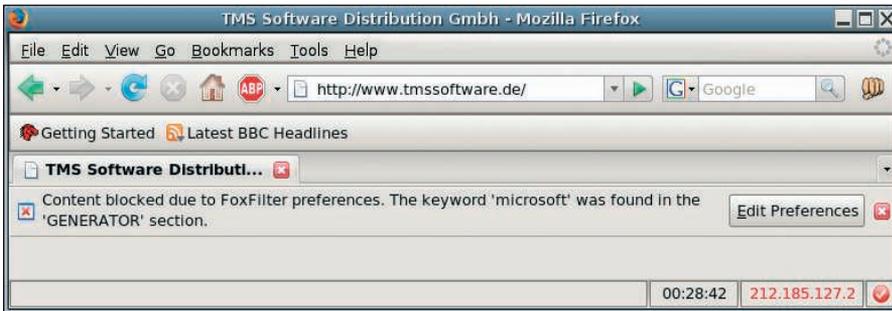


Figure 4: FoxFilter shows no mercy when it finds undesirable content.

surfing the Internet, Firefox now will refuse to load the page in question. Instead, you will see a FoxFilter warning in the browser (Figure 4).

In case of “false positives,” the FoxFilter admin can enter the password and individually unblock the page and modify the FoxFilter configuration at the same time, if needed.

Public Fox

The second web content filter, Public Fox (current version 1.04), does not immediately appear in the *Tools* menu after the install. Pressing *Add-ons* and then clicking *Preferences* opens a simple dialogue box and lets you change this (see Figure 5).

You may notice that the settings are much the same as FoxFilter. If you have already installed and configured FoxFilter, it does not make sense to enable the same options in Public Fox; however, Public Fox offers only a fraction of FoxFilter’s capabilities when it comes to blocking undesirable content.

Although Public Fox has a blacklist of undesirable URLs, it does not search the metadata or source code for keywords, and there is no exception list. On the

other hand, Public Fox has one feature that FoxFilter lacks: Downloads of any kind of content can be globally blocked.

Additionally, Public Fox has an option



Figure 5: Public Fox access via the Add-ons menu.

for taking specific file endings into consideration when blocking downloads. For example, if you want to prevent users from downloading JPEG images to the local machine and allow PDF files, just enter the *.jpg* file extension in the input box. The feature also supports wildcards.

Public Fox also can block bookmarking and outputting of lists of visited addresses. If needed, the tool can block the

Add-ons menu, the browser’s *about:config* function in the main window, and Firefox’s internal settings. The latter option prevents unauthorized users from modifying the configuration to work around the security mechanisms. An administrative password also is supported (Figure 6).

Conclusions

FoxFilter and Public Fox are two useful extensions that effectively help you keep undesirable content off your machine. FoxFilter has a well-planned configuration that helps non-experts set the required preferences.

On top of this, the tool is not limited to scanning web addresses for predefined keywords but also will search through a site’s metadata and source code for default and administrator-defined search keys. The excellent filtering this provides puts some commercial alternatives to shame.

Tests in our lab determined that the search routines are extremely efficient; there were no noticeable delays loading websites. Configurable surfing time limits would be a useful extension to functionality in a future version of FoxFilter.

Although Public Fox lacks the mature filtering capabilities that FoxFilter offers, it does add a couple of useful features that its competitor lacks, including support for extremely granular blocking of Internet downloads.

Public Fox also blocks access to add-on lists, bookmark extensions, and Firefox options to firmly close the door on attempted workarounds.

Both extensions provide password protection to prevent manipulation of the filter settings, which makes both Firefox extensions useful for family PCs and classroom machines. In fact, from a functionality point of view, a combination of the two leaves practically nothing to be desired. ■

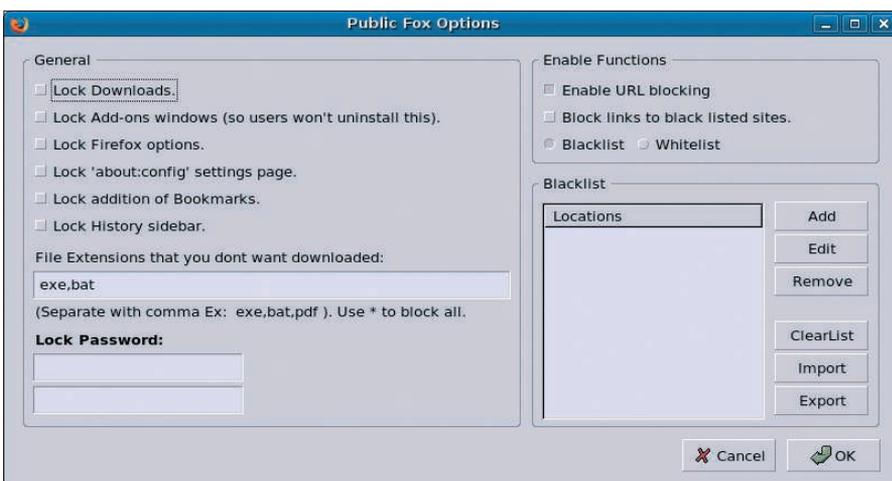


Figure 6: The Public Fox Preferences window does not have a lot of options.

INFO

[1] FoxFilter 5.1 (download):
<http://addons.mozilla.org/firefox/addon/4351>

[2] Public Fox 1.04 (download):
<http://addons.mozilla.org/firefox/addon/3911>