

# STAY SMART ONLINE ALERT SERVICE

## Factsheet 8

### Securing the Mozilla Firefox Web Browser

Often, security and functionality are on opposing ends of a sliding scale in web browsers. The more functionality you allow, the greater the risk of the security of your computer being compromised.

This article describes the settings needed to secure Mozilla Firefox version 3.0.7, which at the time of writing is the most up to date version available of this web browser.<sup>1</sup> You should always ensure that the brand of web browser you choose to use (such as Mozilla Firefox, Microsoft Internet Explorer or Apple Safari) is the newest available, as these versions are the most secure.<sup>2</sup> To find out which version of Mozilla Firefox you are using, see below.

The settings should be enabled for each account on the computer (whether an administrator or limited user account) as the settings only take effect on the account from which they are set.

This means that each user has the ability to control the browser's security settings. However, if one user downgrades their web browser's security settings it could compromise the security of the entire computer.

---

#### Determining your Firefox version number

To find out which version of Mozilla Firefox you are currently using, run the following commands.

1. Log in to your account and open Firefox
2. On the Firefox menu bar click the "Help" label
3. Select the "About Mozilla Firefox" label

---

<sup>1</sup> <http://www.mozilla.com/en-US/firefox/>

<sup>2</sup> 'Beta' versions of software are pre-release versions and should be avoided as these have not been fully tested under all circumstances and are more likely to affect software stability or contain security bugs.

## Securing Firefox with Options

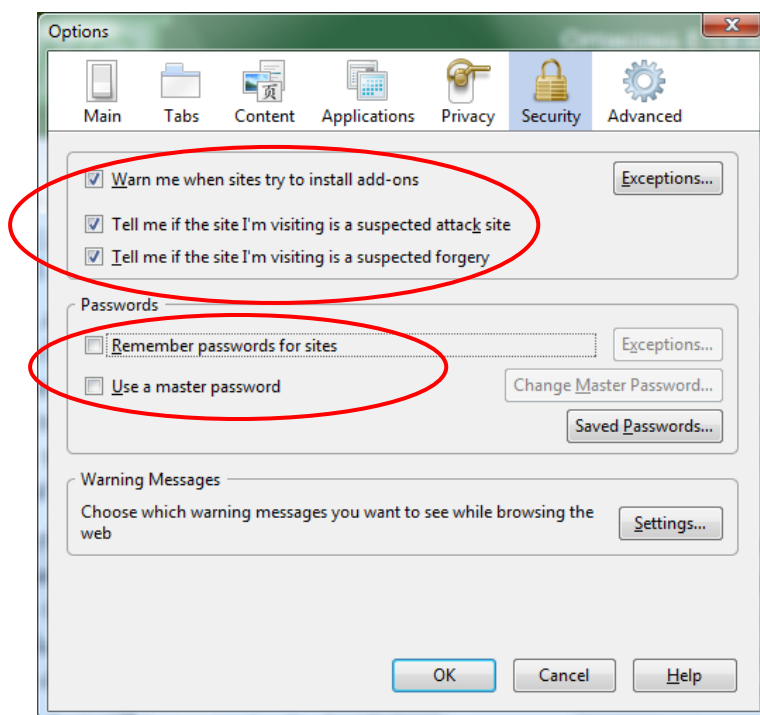
Apply the following settings to each user's account. This may mean that you will have to perform these steps more than once if you have several family members with personal accounts.

1. Log in to your account and open Firefox
2. On the menu bar click the "Tools" label
3. Select the "Options..." label.



4. Click the "Security" icon
5. As shown in the diagram below, tick the check box for all three options:
  - Warn me when sites try to install add-ons
  - Tell me if the site I'm visiting is a suspected forgery
  - Tell me if the site I'm visiting is a suspected attack site

This will help alert users to the possibility that a site potentially contains malicious software that could harm your computer or they are visiting a phishing site (which is a web site impersonating a legitimate organisation for fraudulent purposes).



6. In the event that your computer becomes compromised by malicious software, generally passwords that have been “remembered” (or saved) on your computer will be captured and transmitted to a criminal. Therefore, it is important **not** to routinely save passwords on your computer.

As shown in the diagram above make sure the check-box “Remember passwords for sites” is not ticked. If you select this option, it is important not to undo it later by subsequently choosing to save passwords you type into the Firefox web browser.

### More advanced options for securing Firefox

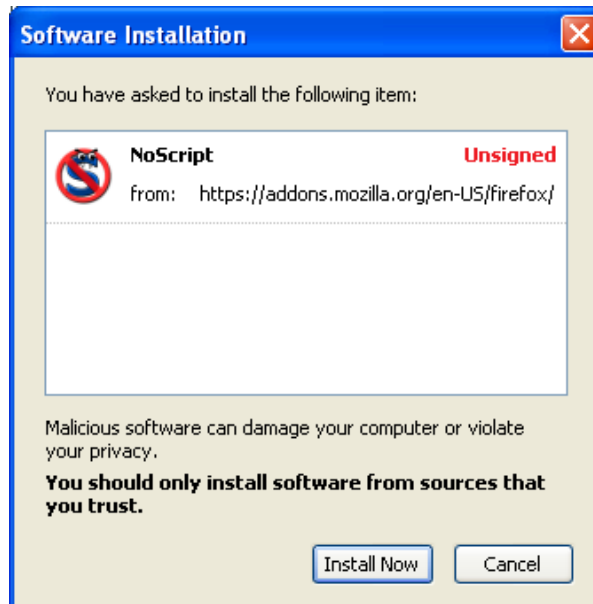
For extra security you can stop dynamic scripts and controls from running in your browser automatically.

*This section should only be attempted by more experienced users who are confident about their ability to make judgements as to when a web site should be trusted and when it should not be trusted.*

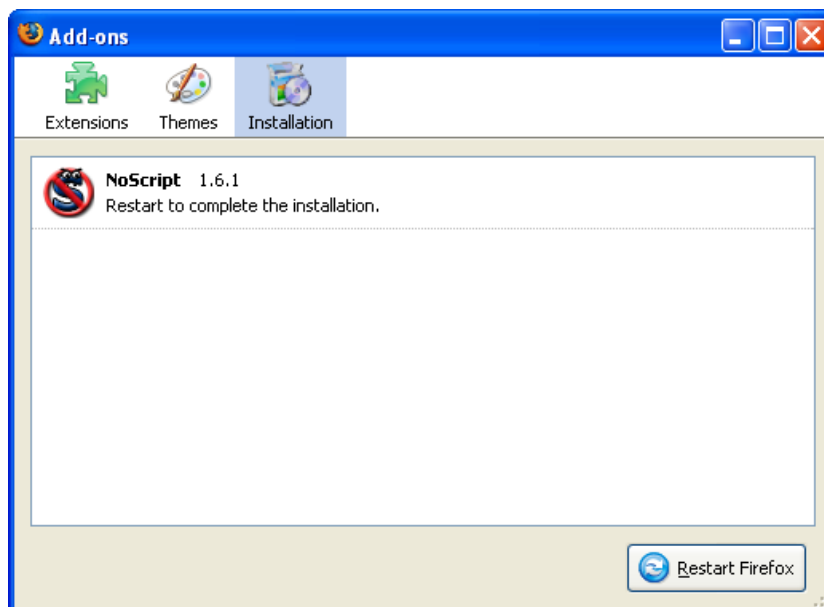
As a general rule, trusted sites are those that you would allow to run dynamic content, such as Java, Javascript and ActiveX, on your computer to provide additional functionality and untrusted sites are those you would not.

On its own, Firefox can't be configured to selectively enable JavaScript for web sites that you trust, whilst keeping it disabled for others. There is a solution, however, in the form of the NoScript add-on. NoScript will allow you to more selectively control when dynamic content functionality should be allowed and when it should be blocked on the basis of whether you have trust in a particular web site. It is available from <http://noscript.net>.

1. To install NoScript, log in to your account and open Firefox.<sup>3</sup>
2. type <http://noscript.net> into the address bar of the Firefox web browser
3. Click on the "Get It" link
4. Click the "Install Now" link and you'll get a popup box like the following

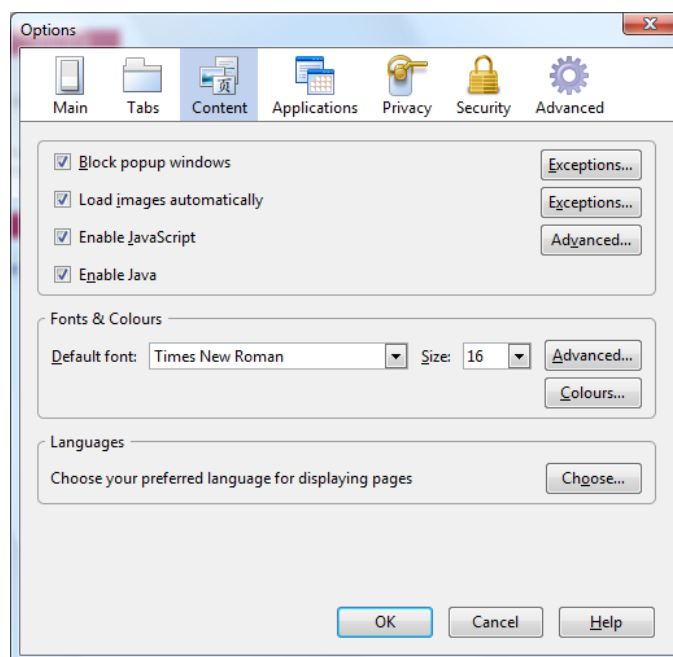


It will install the add-on and prompt to restart Firefox.

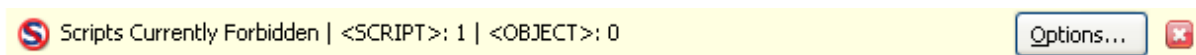


<sup>3</sup> NoScript must be installed for each and every account in which it will be used, whether administrator or limited user.

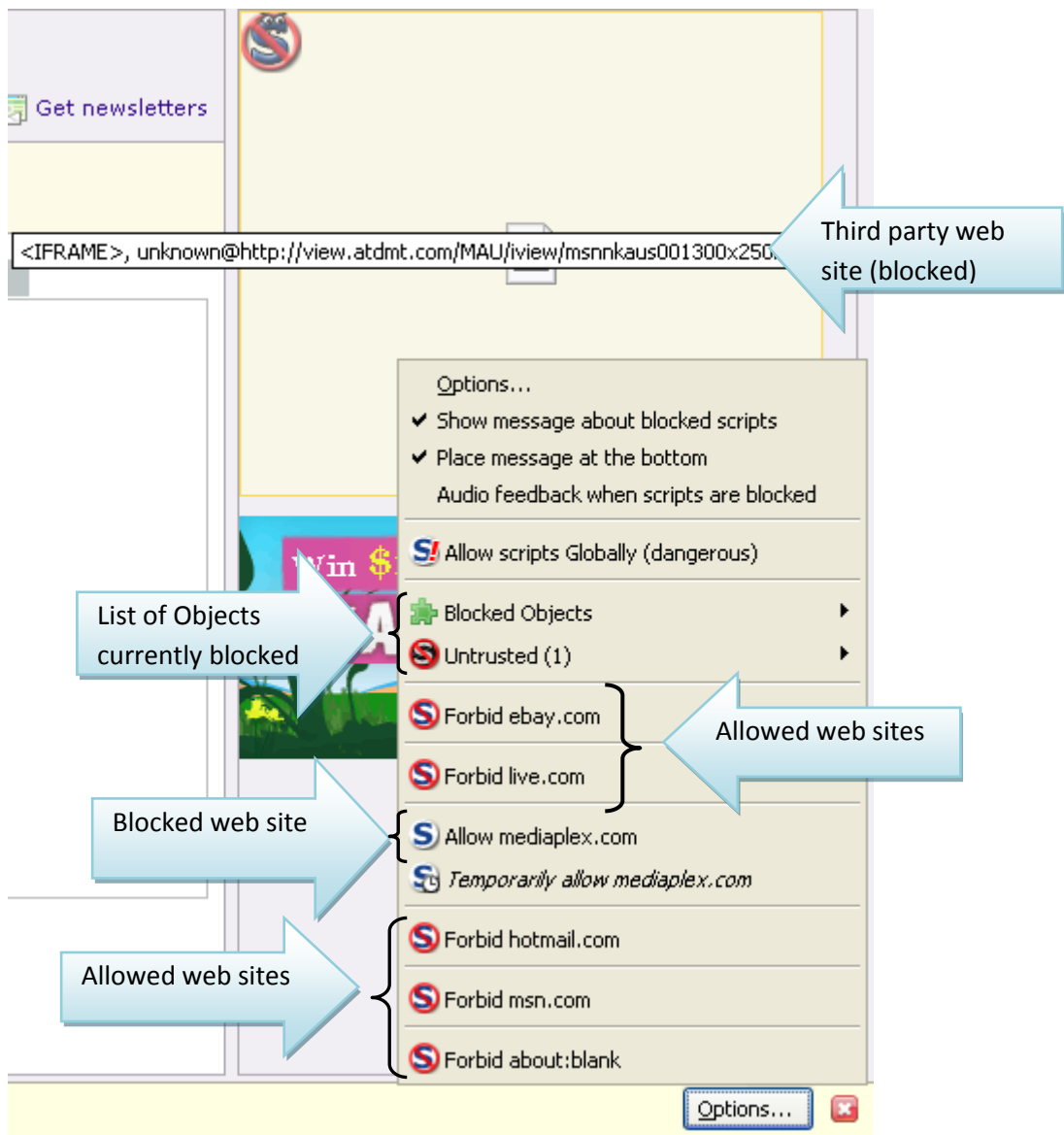
5. Check that Java and JavaScript are enabled in the browser by opening the Tools menu, select Options and then the Content icon as shown below.



6. After installation, NoScript will by default prevent dynamic content, like Java and JavaScript, from running in your browser – just as if you had disabled this content in the Firefox options. You can easily tell when NoScript has blocked dynamic content when you visit a web site, because this prompt will be clearly visible at the bottom of your browser window:



Many web sites make use of dynamic content for full functionality, so if the NoScript prompt is visible you'll often find that the site no longer 'works' normally. If you need this functionality, the "Options..." button will allow you to selectively enable dynamic content for web sites that are reputable and which you trust. Many web sites will include content from multiple sources, as this example shows:



The above image is an example of a NoScript configuration menu for a site that contains content from more than one source. In this example, the user has already chosen to allow content from live.com, as well as some other well-known sites that have included content on this page.

Allowed sites are shown with "Forbid" in front of them, indicating the action that would be taken should you select the menu item. In the same way, sites that have "Allow" in front (here only mediaplex.com) are currently **not** allowed to run dynamic content in your browser.

The option to "Allow scripts Globally", if selected, will effectively disable NoScript and re-enable dynamic content from all sites to run – just as if NoScript was not installed.

It's important to remember at this point that NoScript settings are retained only on a per user basis. If you want all users of your computer to have the same settings, you must repeat the actions described here for each user account.

NoScript is a powerful tool, and is more configurable than most users might prefer, but it provides an effective layer of malware protection by allowing you to choose when dynamic and potentially harmful content is allowed to run on your computer and when it is not allowed.

Report prepared March 2009

---