Tabnabbing.
By: pjlantz
OP: http://www.pjlantz.com/2010/05/tabnapping.html

A new potential phising attack has been detected by a Mozilla developer. When a user has several tabs opened in the web browser and visits a malicious website, a Javascript code is executed which alter the contents of a specific tab. This can for example render a fake login page for the Gmail but could be used for any page. The code example waits until a user switches tabs and after a short time it renders a Gmail login image in the tab where the malicous page was visited. An attack would go like this, lets assume Gmail: The user would enter his credentials to login and he gets redirected to his inbox, since he was never logged out in the first place the login will appear as successful and the credentials could be sent to the attacker.

Security measures against this attack is to turn off Javascript in your browser. Running Noscript addon for mozilla-based browser can be a valuable defence. This code example works for Safari too and the post will be updated when tested out on more browsers.