Provident Technology: Internet Explorer Security Flaw

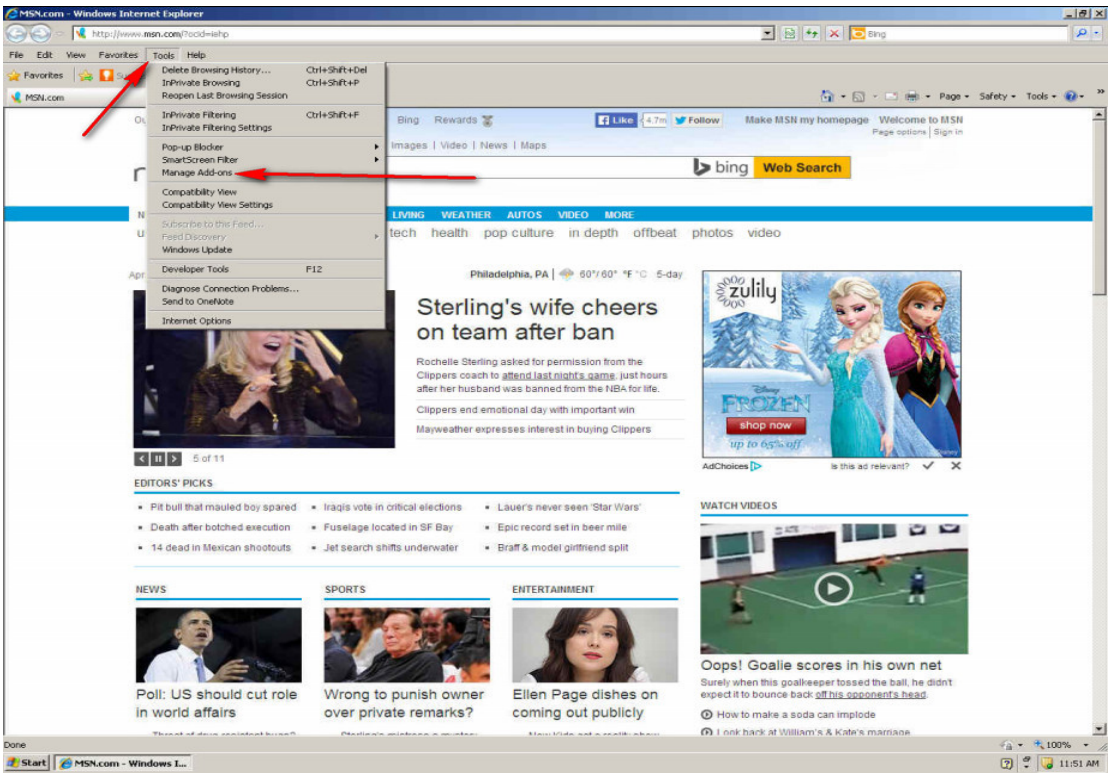
On Saturday April 26th, 2014 it was announced that a flaw has been discovered in the Microsoft Internet Explorer web browser that presents a significant security risk. The flaw affects Internet Explorer versions 6 to 11 (the most recent version). The department of Homeland Security has made a statement advising everyone to avoid using Internet Explorer until a solution is found and released by Microsoft. The bug allows a hacker to use a corrupt Adobe Flash file to attack a computer. The bug does not work if the Adobe Flash Add-On is disabled. However, doing so will also disable Internet Explorer's ability to properly display Flash content in websites. If you would like to read more specifics about this issue, I have included a link to the related USA Today website posting at the end of this document.

Until this issue is resolved, we have compiled the following options to keep your computers and data safe. The options will vary depending on your version of Windows and your internet browsing requirements. The options are listed below by Windows version, please read the recommendations for your version.

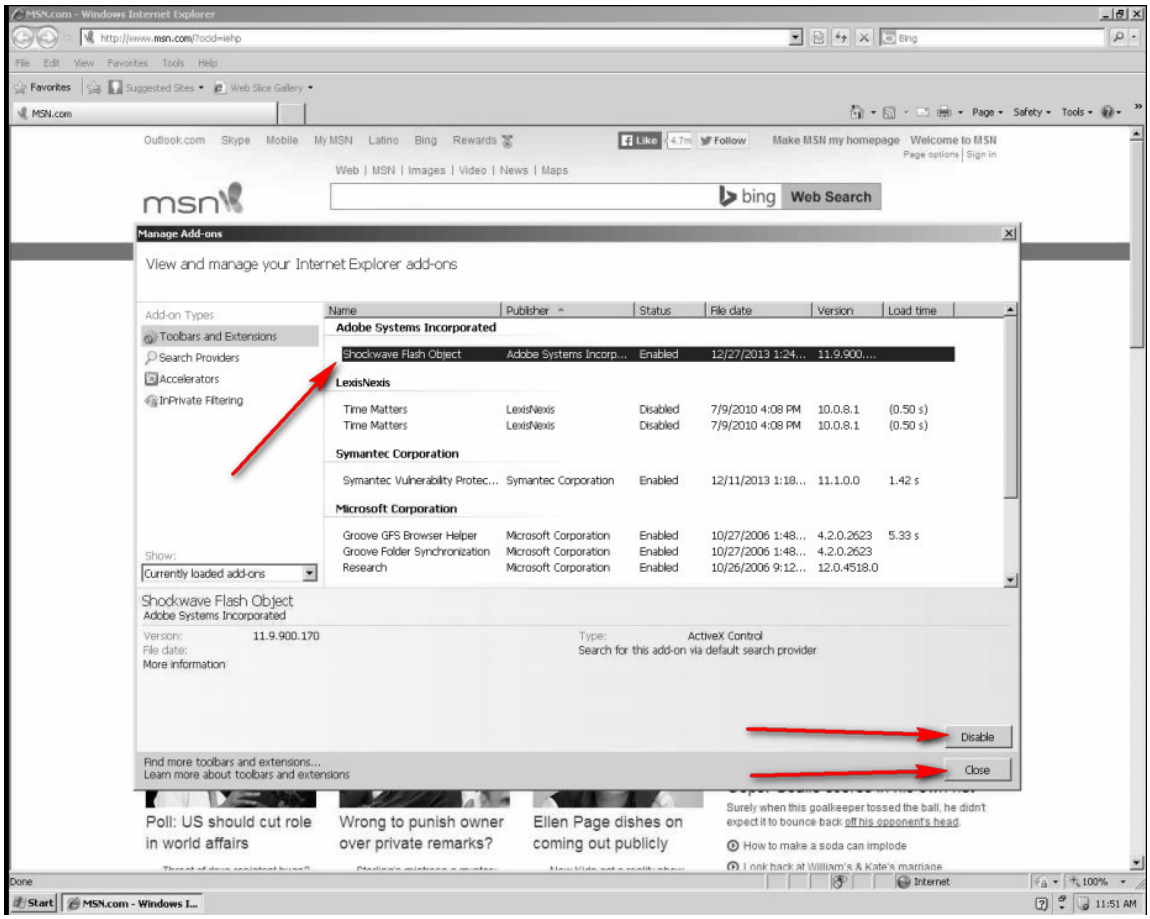
Windows XP:

As Microsoft support for Windows XP ended on April 8, 2014 there will be no security update to fix this issue for XP users. To keep your computer and data safe, the best option is to stop using Internet Explorer and instead, use another web browser such as Google Chrome or Mozilla Firefox. You can download and install one of these browsers for free. To download Chrome, go to https://www.google.com/intl/en/chrome/browser/. To download Firefox, go to http://www.mozilla.org/en-US/firefox/new/.

If you must use Internet Explorer in order to use a particular website, or you don't want to use another browser, you can disable the Adobe Flash add-in for Internet Explorer. To do so in Internet Explorer 8 (the most current version supported by Windows XP), open Internet Explorer, click on the Tools Menu, then select Manage Add-ons (See picture for reference)



In the Manage Add-Ons Window, find the Adobe Shockwave Flash Object, select it, and then click on Disable before closing the Manage Add-Ons window (See below picture for reference).



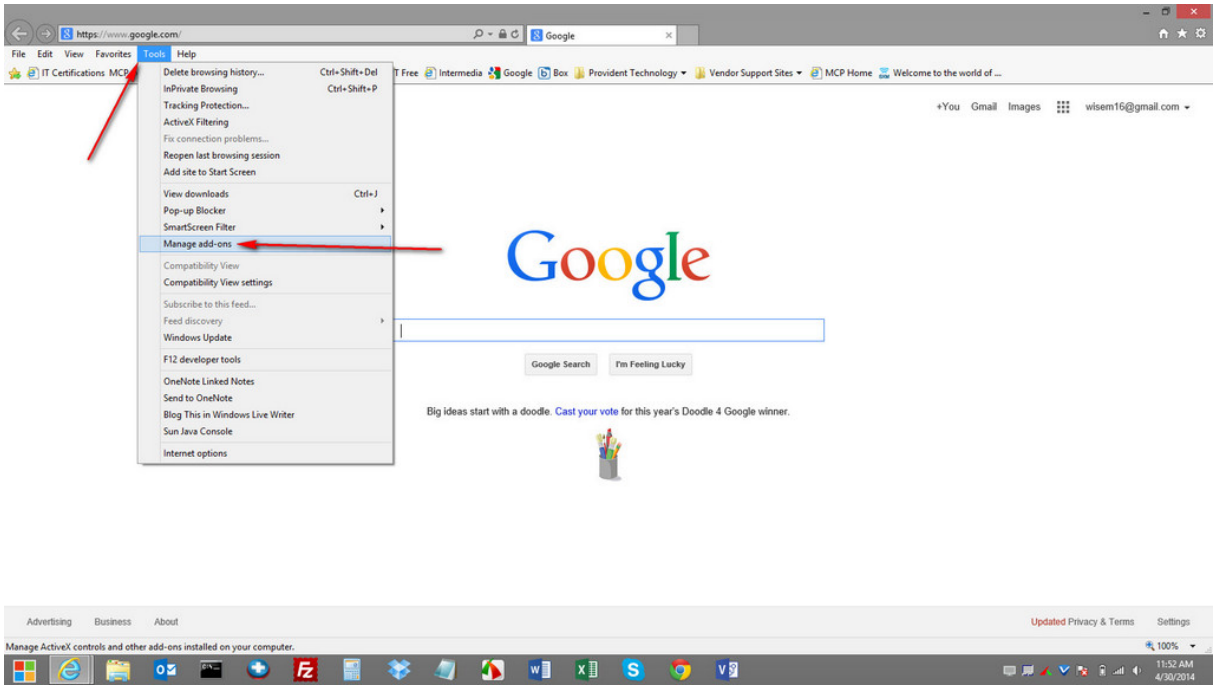
Windows Vista, Windows 7 and Windows 8:

To keep your computer and data safe, the best option is to stop using Internet Explorer until Microsoft releases a security update, and instead use another web browser such as Google Chrome or Mozilla Firefox. You can download and install one of these browsers for free.

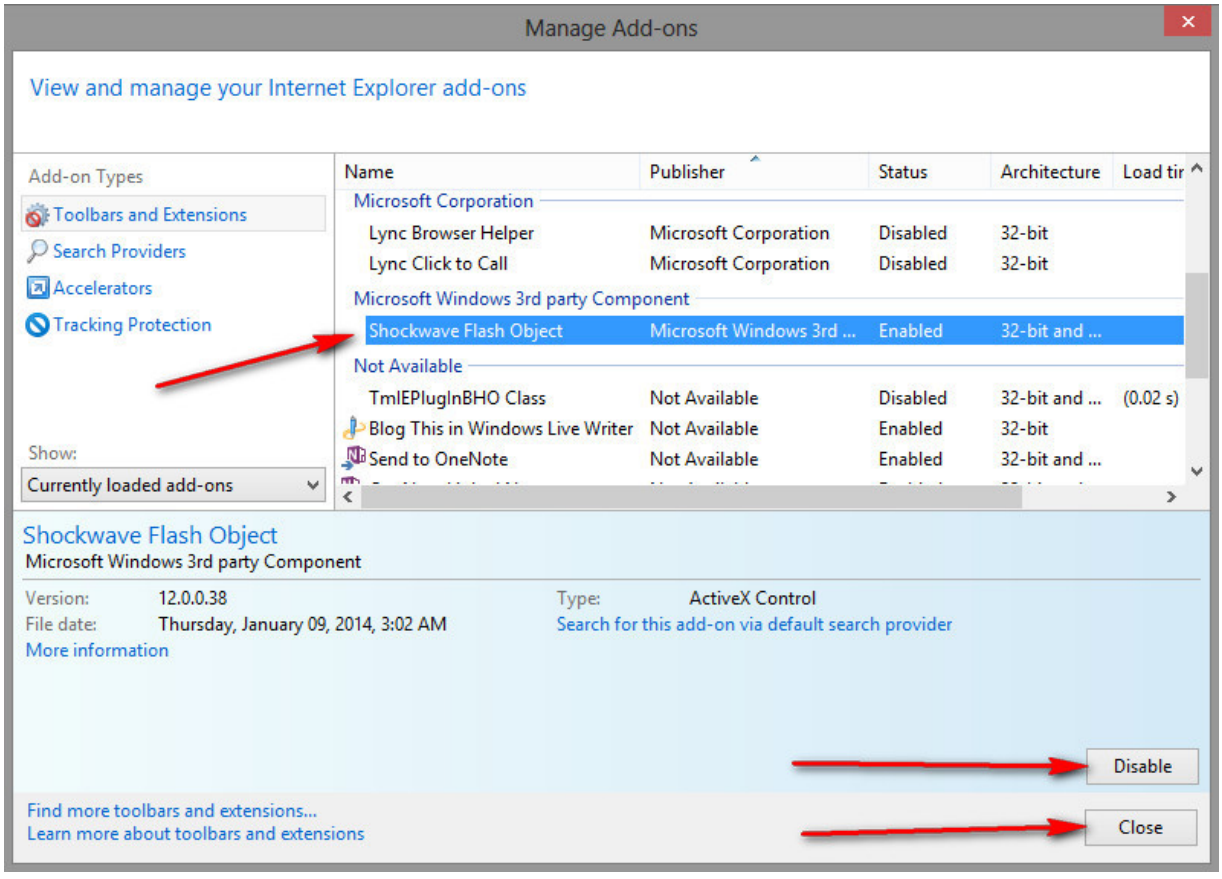
To download Chrome, go to https://www.google.com/intl/en/chrome/browser/.

To download Firefox, go to http://www.mozilla.org/en-US/firefox/new/.

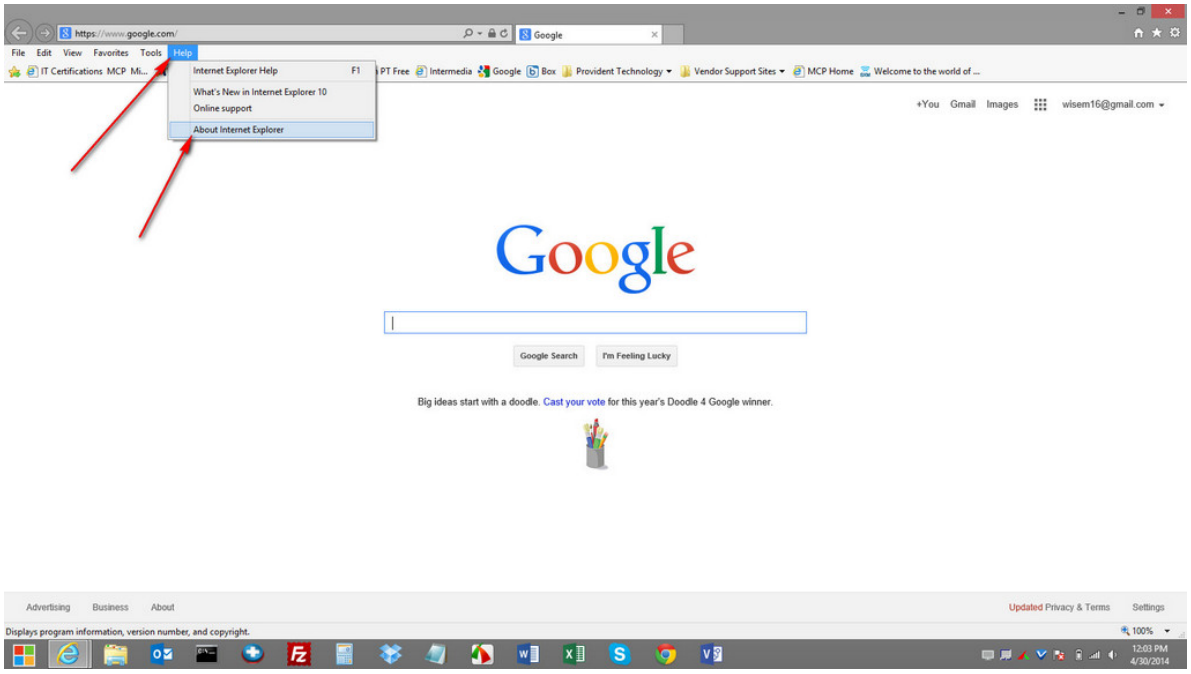
If you must use Internet Explorer in order to use a particular website, or you don't want to use another browser, you have two options. First, you can disable the Adobe Flash add-in for Internet Explorer. To do so, open Internet Explorer, select the Tools menu, and then click on Manage Add-Ons (See below picture for reference).



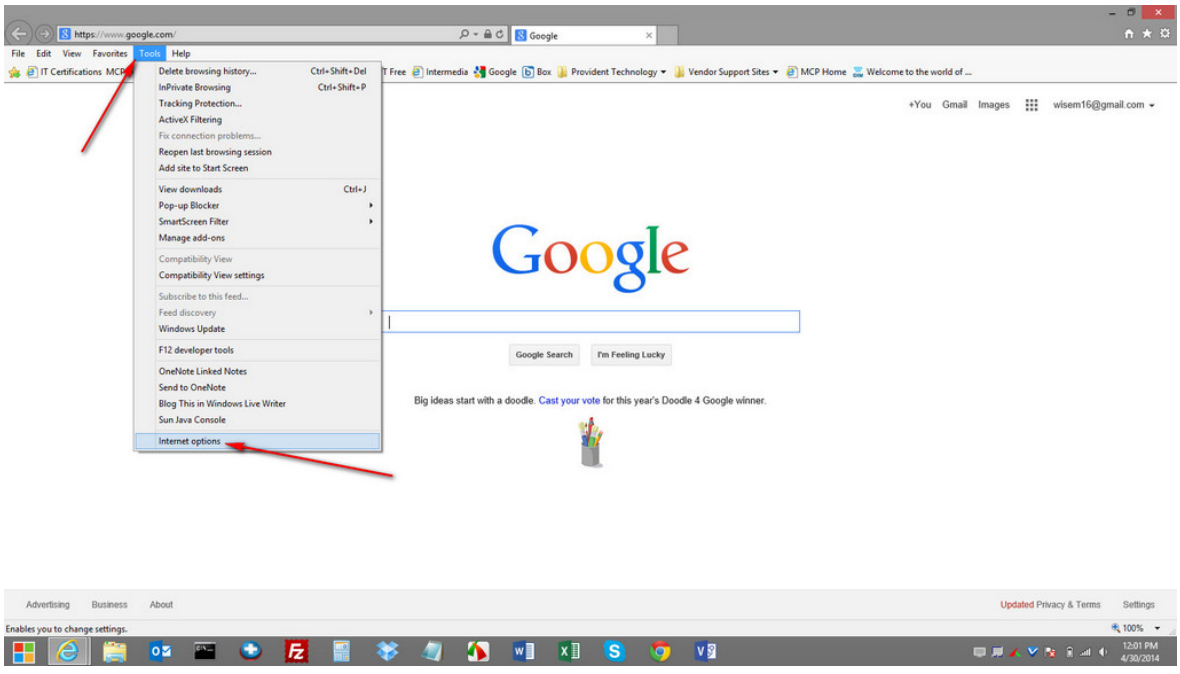
In the Manage Add-Ons window, scroll down until you see the Microsoft Windows 3rd Party Component Heading with the Shockwave Flash Object underneath. Select this object, then click Disable before closing this window (see below picture for reference).



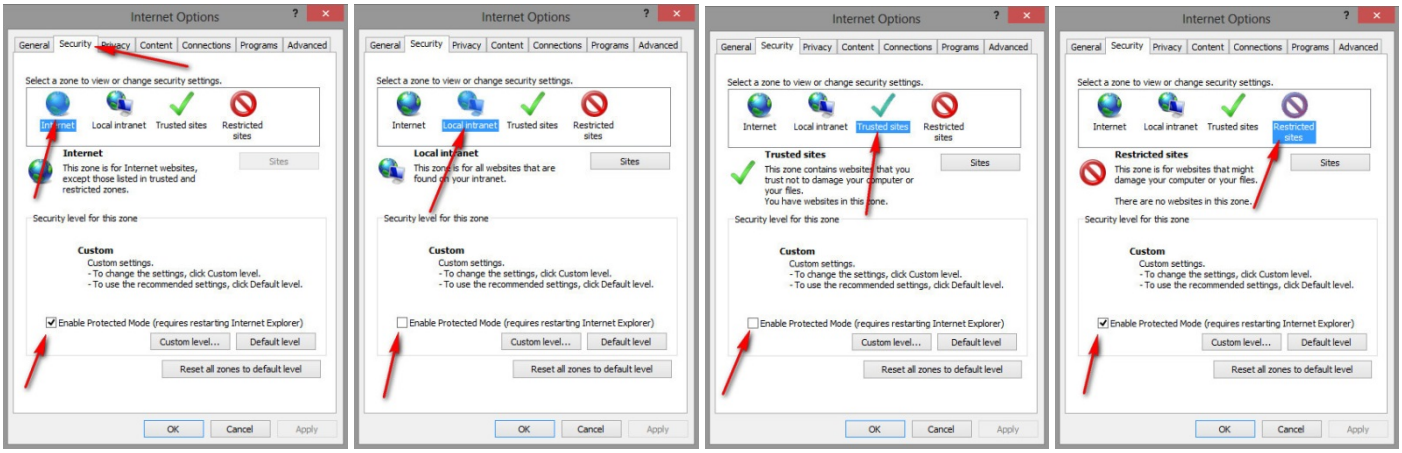
The second option is to enable protected mode for all zones in Internet Explorer. This option is only for Internet Explorer 10 and Internet Explorer 11. If you are using an earlier version of Internet Explorer, you can upgrade to Internet Explorer 10 to take advantage of this option. To determine which version of Internet Explorer you are currently using, open Internet Explorer and click on the Help Menu. In the Help menu, select About Internet Explorer (See below picture for reference).



To enable protected mode, open the Tools menu in Internet Explorer and select Internet Options (See below picture for reference).



In the Internet Options window, click on the second tab labeled Security. Across the top of the security tab, you will see the four zones (Internet, Local Intranet, Trusted Sites, and Restricted Sites). Click on each zone, then check the box below to enable protected mode. Once you have done so for all four zones, click Apply and then Close. Now you must close Internet Explorer and reopen it to apply the change (See the below pictures for reference).



For more information, here are links to the USA Today posting and the FireEye blog related to this issue:

http://www.usatoday.com/story/tech/2014/04/28/internet-explorer-bug-homeland-security-clandestine-fox/8409857/

http://www.fireeye.com/blog/uncategorized/2014/04/new-zero-day-exploit-targeting-internet-explorer-versions-9-through-11-identified-in-targeted-attacks.html