

Is Internet Explorer 9 The Most Secure?

First, here's a little background on how a browser decides whether to warn you against proceeding to a website. –

The browser checks each URL (web address) you click on against an online database of reported malicious sites.

If a URL is not in the database, the browser just lets you go there.

If the URL is in the database, a warning window pops up and you get to choose whether to proceed to the site or not.

Three major browsers - Firefox, Safari, and Chrome - use Google's Safe Browsing database of malicious links. Opera uses technology provided by antivirus developer AVG. Microsoft has its own database called SmartScreen URL Filter. Apparently, Microsoft's database is vastly superior to the others.

NSS Labs, an independent security testing facility, turned all six browsers loose against a set of 650 malicious URLs. The results are rather alarming for anyone who doesn't use a recent version of Microsoft's Internet Explorer:

- Internet Explorer 9 blocked 92 percent of the malicious links. (IE8 scored at 90 percent.)
- Only 13 percent of malicious links were blocked by Firefox, Chrome, and Safari.
- Opera scored a pathetic 5 percent.

But wait, it gets even better. (Or worse, depending on your preferred browser.) Internet Explorer 9 has a new feature, Application Reputation, which boosted its blocking rate to an astonishing 100 per cent in NSS Labs' test.

Application Reputation focuses on downloadable files rather than Web pages. It examines a file's "reputation" in the SmartScreen database: how many times it has been downloaded; is it digitally signed; is the publisher known and reputable; have there been any reports of malware in the file.

If a file is known and trusted, the download proceeds without interference from SmartScreen.

If it is known malware, you are warned of that fact and given a chance to cancel the download.

If it is unknown, you receive a cautionary message before the download is allowed to proceed.

The methodology used by NSS Labs has been criticized. The sample size and test run were too limited, say critics. You can read the entire [NSS Labs report](#)

(22 pages, PDF) and decide for yourself. It should be noted that NSS Labs did not receive funding from any of the browser developers.

So, is IE 9 the most secure browser? That would be too broad a statement. There are many other ways a browser can let malware enter your computer, or allow hackers to take over control of your system. Some criticize Microsoft for tightly integrating the browser into the operating system, which can allow a browser security hole to penetrate deeper than it would otherwise. But as far as the tested methods are concerned, both IE8 and IE 9 seem to protect you from malicious links and downloads better than any other browser, by a long shot.

Read more:

http://askbobrankin.com/which_browser_is_the_most_secure.html#ixzz1XftGGmPC

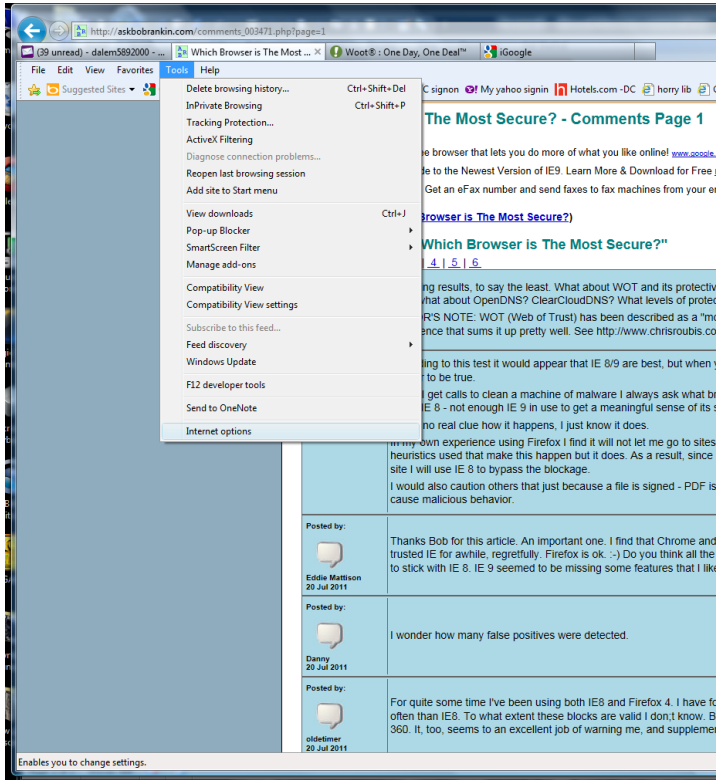
This report is dated July 20, 2011

My intention here is not to tell you which browser to use. You should use what you like or what you believe is the safest.

Next, let's take a look at some settings in Internet Explorer. These settings will be within the *Tools* menu. We will look at *Options*

By the way, if you use Firefox or Chrome, you can also find the *Options* settings under *Tools* also. With Chrome you click first on the *wrench* icon on the top right, then on *Options*.

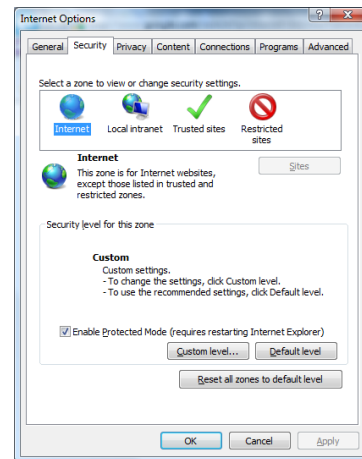
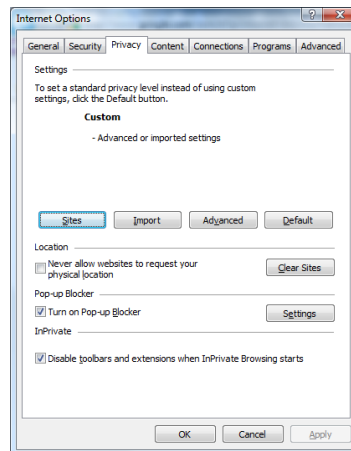
Notice the drop down under Tools



For each of us it is important to look at the settings for Tracking, Active X, Pop-up Blocker, and SmartScreen Filter. Just take a look at them, and use the default settings that will be there. If you want more security change anything you want to give you more.

Finally, click on Internet options, and click on the Security tab. Make sure you have *Enable Protected Mode* checked.

Also look at the Privacy tab, and spend a minute to look into options there. If you have questions, click the ? on the top right and read more.



Do not tho, change any default setting to a lower level of security, for any reason.

Keep your Anitvirus up to date with new definitions as soon as they are available, and run something like Mware Bytes weekly. Do not ignore warnings, and do not click for more info if you get scareware popup windows- close the windows instead.