

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

guys.

Dave McClure • Jul. 07, 2013

From the [Bleeding Edge blog](#).

If you are still relying on a firewall and anti-virus programs to protect your computer from malware and other problems, your security is about 10 years behind the bad guys.

Today, the battlefield is no longer email (though there are still lower-level bad guys pushing their phishing schemes, spam and infectious viruses through emails). The real threat is through your browser, and in particular the add-ons that you use to enhance your browsing experience. If you are looking for the browser that does the best job of keeping you safe, though, you may be shocked.

One of the leading culprits today, when it comes to making your computer vulnerable, is the suite of Java scripting add-ons from Oracle. Java is a technology used by a wide range of Internet sites, from porn video sites to less salacious sites like YouTube, to deliver video and other graphics services to your desktop. Java, being extremely popular and extremely easy to hack, has been for the past year the first choice of malware writers to invade your machine and seize command of your desktop.

For months now, security specialists (including myself) have recommended that you remove all Java add-ins and applications from your desktop. Sadly, while this might be prudent security advice, it is not practical. Too many web sites use Java to deliver content to your desktop. Sadly, Oracle has made this mess even more difficult by releasing a succession of patches to Java that don't really fix the problems. And more difficult still because they use the Java updates to shovel all types of unnecessary crapware programs onto unwary consumers.

Oracle, once a formidable technology force, has been relegated to the level of a cheap

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

against a sample of 754 "active and malicious" URLs (web page addresses) to see what percentage were caught by each browser's defenses. You can read the [complete NSS browser safety report](#), but the summary results are simple and stunning.

The browser that does the best job of protecting your computer is...Internet Explorer. Followed closely by Google Chrome. And almost no one else. Here's the simple chart of browsers and their levels of protection, as Rankin notes:

| BROWSER | PROTECTION |
|----------------------------|------------|
| Internet Explorer 10 | 99.96% |
| Google Chrome 25/26 | 83.16% |
| Safari 5 | 10.15% |
| Firefox 19 | 9.92% |
| Opera 12 | 1.87% |

“Clearly, only IE 10 and Chrome can be taken seriously if you are looking for a browser that protects you from malicious Web content. But what accounts for the dismal performance of Safari, Firefox, and especially Opera, and the narrower but significant difference between IE and Chrome?”

Firefox, Safari, and Chrome all use the Google Safe Search API, a ‘reputation’ system that blocks access to URLs that are labeled ‘malicious’ in a database compiled by Google in the course of its Web indexing and from user reports. Safe Search is all that Firefox and Safari use, so it's no surprise that their effectiveness rates are very similar in this test. The test indicates that Safe Search alone is only about 10% effective in blocking Web-based malware.

Chrome also includes Google's Download Protection, which judges the reputation of

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

system blocks executable files, as Google's Download Protection does. But there is an important difference between the approaches to "reputation" taken by Google and Microsoft.

The NSS study tested IE10, the latest version of Microsoft's browser. I can't extrapolate from the NSS study, but IE9 offers both Smartscreen Filter and the Application Reputation feature. So my guess is that it would perform on par with IE10 as far as blocking malicious websites. For those on XP systems, IE8 has Smartscreen filter, but not Application Reputation.

How this will affect future efforts to secure the desktop for accountants and tax preparers remains to be seen, but it is clear that in the current generations of software, the safest browser is still the Internet Explorer system built into Microsoft Windows.

Firm Management • Small Business

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved