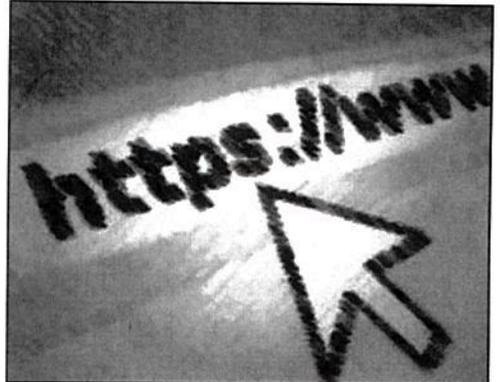


Browse the Web Securely with These Tips

Operate Under the Principle of “Least Privilege”

Do you browse the web using the administrator account? If your PC has only one user account, then the answer is ‘yes.’ Instead, you should create/utilize a separate user account for browsing the web and doing routine tasks. Malware typically operates under the rights of the currently logged-in user. If your computer is infected with malware when you’re logged in as administrator, the malware pretty much owns your PC. Browsing the web using a normal user account minimizes the impact of the malware by limiting it to actions that only a normal user can take. Adopt this best practice today!



Java or No Java?

According to Websense, 75% of users run a version of Java in their browser that's at least six months out of date. Are you one of them?

Java in browsers is a huge malware magnet. Using an exploited Java weakness, the bad guy can steal your data or use your PC for malicious purposes. What to do about it?

1. Disable Java – unless you absolutely need it. See <http://www.pcmag.com/article2/0,2817,2414191,00.asp>.

2. Keep Java updated. If you're going to use Java, make sure you are running the latest version, which gives you a fighting chance against the adversary. Right click on the Java update icon and set it to *Check for updates automatically* with a frequency of *daily*.

Keep Your Browser Up-To-Date

This is crucial, as new patches are often released to fix existing vulnerabilities in browser software. This recommendation doesn't apply solely to browser software – it is critical to keep operating system software and any other software you have up-to-date for the same reason.

Use HTTPS

The “s” in “https” stands for secure, meaning that the website is employing SSL encryption. Check for an “https:” or a padlock icon in your browser's URL bar to verify that a site is secure before entering any personal information.

Avoid public or free Wi-Fi

Attackers often use wireless sniffers to steal users' information as it is sent over unprotected networks. The best way to protect yourself from this is to avoid using these networks altogether.

Disable stored passwords

Nearly all browsers and many websites offer to remember your passwords for future use. Enabling this feature stores your passwords in one location on your computer, making them easier for an attacker to discover if your system gets compromised. If you have this feature enabled, disable it and clear your stored passwords.

Turn on your browser's popup blocker

Popup blocking is now a standard browser feature and should be enabled any time you are surfing the web. If it must be disabled for a specific program, turn it back on as soon as that activity is complete.