HOW TO REMOVE THE ASK.COM MALWARE

Technically, Ask.com malware is not a virus because it does not reproduce and distribute itself. But it’s definitely one of the most irritating, widespread, and hard to eradicate specimens of marketing malware infections euphemistically called “potentially unwanted programs” (PUPs).

The Ask.com Web site started in 1995 as a Q&A style cross between an encyclopedia and a search engine. It allows users to pose questions in “natural language” and attempts to provide succinct answers from its knowledgebase as well as search results drawn from other sites.

Ask.com was born as AskJeeves, “Jeeves” being a fictitious question-answering valet. Jeeves “retired” in 2005 when InterActiveCorp (IAC) bought the AskJeeves business; his name was dropped, leaving just Ask.com. IAC owns about 150 Internet brands including About.com, CitySearch, Dictionary.com, Match.com, Tinder, and Vimeo. Dragging visitors to those sites is the company’s highest priority. The Ask.com malware is IAC’s lasso.

It's not malicious, at least in the sense that it doesn't turn your computer into a spam-spewing zombie, steal your passwords, or lock your files and demand a ransom. But it is a very annoying and difficult to remove example of adware. The prefix "mal" means "bad" so it’s appropriate to call it malware.

The Ask.com malware package does three things to victims’ computers. First, it adds the Ask.com toolbar to a victim’s Web browser. It also changes a browser’s default homepage and default search engine to Ask.com. Third, and most obnoxiously, search results are dominated by ads for IAC properties and its partners in an ad network.

Uninstalling the toolbar via Windows +X, then F will not reset your homepage and default search engine to their original preferences, nor will it get those sneaky ads out of your search results.

Manually resetting your homepage and search engine works fine until you close and restart the browser. But no matter how many times you do this, the Ask.com changes keep coming back. The Ask.com malware bundle hides itself in your operating system much like a rootkit, eluding detection by many anti-malware scanners. It takes special effort and specific tools to eradicate it entirely.

Recommended Removal Steps:

Step 1: Uninstall the Ask.com toolbar via Windows + X, then F. That's not as simple as it sounds. The Ask toolbar program may be masquerading as "VacationXplorer Internet Explorer Toolbar" or something else with "toolbar" in the name. Scroll down the "publisher" column in the list of programs you can uninstall, and remove anything whose publisher is Ask, Mindspark Interactive Network, InterActiveCorp, or APN, LLC.

Step 2: Reset your browser(s) to factory defaults:

For Internet Explorer instructions, go to IE RESET SUPPORT PAGE.

For Microsoft Edge instructions, go to http://www.groovypost.com/howto/reset-microsoft-edge-default-settings/

For Chrome instructions, go to CHROME RESET SUPPORT PAGE.

For Mozilla Firefox, go to FIREFOX RESET SUPPORT PAGE.

After resetting your browsers, do not open any browser until the rest of these steps are completed, or your browser(s) will be hijacked again.

Step 3: Run MalwareBytes Anti-Malware to root out the Ask.com malware and the changes it made to your registry settings. You can download and install the program at www.Malwarebytes.org.

Step 4: With a stubborn infection like Ask.com, it's always advisable to use two "antibiotics" in case one misses some deeply buried traces. Two good options for a "second opinion" are HitMan Pro and AdwCleaner.

Blocking Future Ask.com Infections

Preventing re-infection with Ask.com malware is a matter of vigilance. Ask doesn't sneak in as a "drive-by" download. It does take some user action to "allow" the installation of this nuisance. But it's often bundled with other software that you do want, using carefully hidden pre-checked boxes that give implicit permission.

One high-profile example is Oracle's Java software, which tries to foist the Ask Toolbar on you every time there's a Java security update. Adobe Reader is another culprit. These companies get money from IAC for every Ask install, so they have no incentive to stop (except for the fact that their reputation is further tarnished).

You must carefully read every screen of every new program or update that you install on your computer. Be sure to opt out of installing Ask.com and other “bonus” software bundled with what you really want. If you don’t trust your own diligence, use anti-malware software with real-time Web protection. This feature, which goes by other names, monitors Web traffic and your browser, detecting things like Ask.com malware before they’re downloaded and blocking attempts to change your browser settings.

Finally, you should know about Ninite, a nifty tool that automates many software installs, and ensures that you don't get nasty foistware.