

What To Do When Pop-Ups Pop Up



Almost since the Web's inception, pop-ups have been an insistent and annoying part of the online experience. The presence of intrusive advertising has been one of the few constants through years of browser wars, Internet booms and busts, the explosion of broadband, and the transition to mobile computing. Sometimes, you can just ignore pop-ups or close the new window, though that's not always easy. Pop-ups can be more than just a nuisance, however. They also can be dangerous on their own or signals of even more perilous threats. We'll help you understand more about pop-ups, how to avoid them, and how to protect yourself from the dangers they pose.

All About Pop-Ups

The first thing to understand about pop-ups is how they work. Technically speaking, any window or

tab that opens without you explicitly launching the application can be considered a pop-up. Most people associate pop-ups with Internet



To configure Internet Explorer 8's pop-up blocker, click Tools, Pop-Up Blocker, and Pop-Up Blocker Settings. You can easily add sites that the pop-up blocker will overlook.

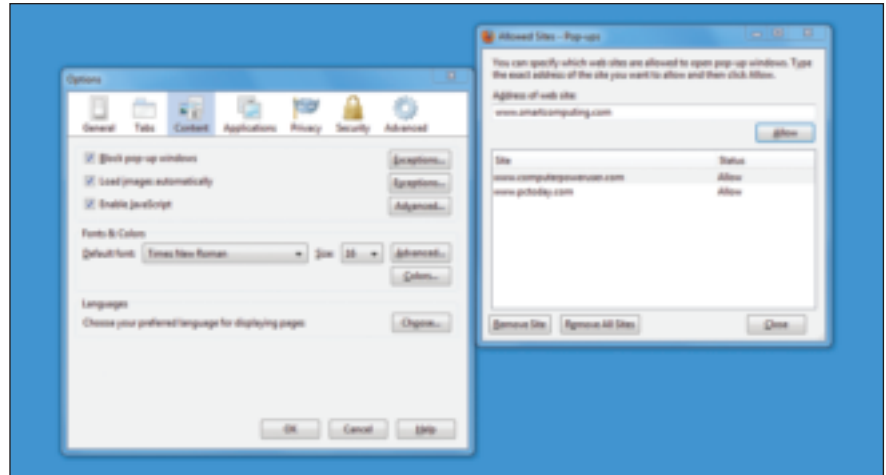
browsers, and it's true that they are the most common variety. Pop-ups sometimes appear automatically when a page loads, sometimes when the page closes, sometimes when you click a blank space on the page, sometimes when you follow a link, and sometimes when you just hover over a certain area of the page. Programmers are creative, and there is no shortage of coding tricks (or coding languages) in which to build new ways of catching your eye. "Pop-unders" illustrate this phenomenon. Essentially the same thing as a pop-up, pop-unders open *underneath* the current window in order to remain unnoticed until they're the last thing open on your Windows Desktop. Some pop-ups don't spawn from an existing browser window or Internet site at all. If you've ever had windows start opening (and then navigating to their own predefined destinations) when you weren't even browsing the

Tech Support

Web, you've experienced the most worrisome variety—those spawned from malware infecting your machine directly.

An important thing to keep in mind, however, is that not all pop-ups are created equal. Some sites legitimately open links in a new window as a way of displaying or collecting additional information without interrupting the current page. Think about the little window that opens to reveal helpful tips when you click a Help link on a Web site. Another legitimate pop-up is the calendar control you can use to populate date fields. Another: hyperlinks embedded in the text of one news story that reference a source or background article. There are a lot of cases where it's perfectly valid, and even desirable, to open a new tab or window. The key difference is whether each new window serves a valid purpose and results from an intentional action (on your part). Those aren't the kinds of pop-ups we're talking about, and it's an important distinction to make.

The problem begins when pop-ups show up unbidden or without your knowledge, plying advertisements either real or phony. They're not just a nuisance. Especially beware those that launch without you even having a browser open or are disguised to look like warning tests, error messages, or dialog boxes. Even buttons labeled "OK," "Cancel," or "Close" can actually be tricks that install something or navigate elsewhere when you click them, which is exactly the opposite of what you intended. Remember that, by definition, the people and companies using deceptive advertising methods or distributing malware are unethical. Don't expect them to honestly label their buttons or actions. Don't trust any messages or prompts that arise unexpectedly online and scrutinize every click on any new window. The only safe thing is to close the window (and the pop-up) entirely.



Find the pop-up blocker settings in Firefox by clicking Tools, Options, and then clicking the Content tab. If you want the blocker to ignore certain sites, click the Exceptions button and add the addresses in the next window.

How To Avoid Pop-Ups

The best way to combat unwanted pop-ups is to avoid them in the first place. No trends are universal, but there are definite differences in the likelihood of running into pop-up advertising among different kinds of sites. The larger and more mainstream the site is, the less likely you are to be exposed to pop-ups (and the less harmful they're likely to be). It makes sense: These sites tend to have larger and more established revenue streams so they're less likely to resort

to trickery in an attempt to drive up ad revenue. Smaller sites with edgier content (especially adult entertainment, gambling, or free software downloads) are more likely to aggressively drive you to advertisers with pop-ups, redirection, or worse techniques. And it should go without saying that any site dealing with illegal or unethical subject matter isn't likely to be scrupulous with advertising or privacy practices, either. In short, be careful where you go on the Web, try to stick with trusted online sources, and avoid the seedier side of the Internet altogether.

Similar advice holds true for downloading and installing software. Even tools that promise to prevent pop-ups or other bothersome pests are often just delivery vehicles for their own adware, tracking software, or worse. Toolbars, utilities, freeware, and other gadgetry are also common sources for pop-ups and other problems. Of course, you can't avoid downloading software altogether, and you shouldn't. But be careful about who you trust, what you install, and where you get it from. Do your homework at sites such as www.smartcomputing.com before downloading and installing software with which you're unfamiliar.



Apple's Safari browser lets you easily enable or disable the built-in pop-up blocker. Click the Display A Menu icon and then click Block Pop-Up Windows. A check mark lets you know whether the blocker is enabled.

Non-Pop-Up Ads

Not all intrusive or annoying ads are pop-ups. Plenty of distracting (or even dangerous) content appears right on the page while you're trying to go about your business. Simple banner ads still proliferate, despite how good we've all become at tuning them out. "Floaters" (ads that slide out over the top of page content) are perhaps the most interruptive. Billions have been made by embedding search-sensitive ads and "sponsored" results within Web pages. You may not mind these ads, but you ought to know that they can be blocked.

Filtering embedded advertising isn't as easy as blocking pop-ups. It's not always as easy to tell when a banner image or Flash animation is an ad. But it is possible, and there are a number of ad-blocking utilities that can help reduce or eliminate the visual clutter created by non-pop-up ads. Kaspersky Internet Security 2011 (\$79.95; www.kaspersky.com), for example, includes an Anti-Banner feature, which also allows you to exclude the banner-blocking on certain sites.

Finally, just as with pop-ups, not all embedded ads appear when you're surfing the Web. Many applications, especially freeware and shareware, embed ads or spawn pop-ups right in the software. Often, you can purchase ad-free versions for a higher price. Alternatively, research and install software that isn't ad-supported in the first place.



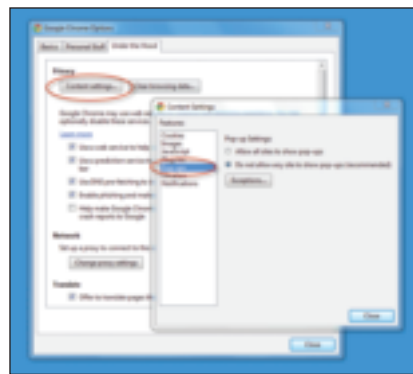
Sick of those banners flashing just above the text you're trying to read? Put a stop to them with Kaspersky's latest Internet Security suite.

Even exercising all reasonable precaution, it's impossible to avoid pop-ups entirely. That's where the pop-up blocking features on your browser come in. All the major browsers now offer some level of pop-up blocking functionality. Internet Explorer 8, for example, lets you choose from various levels of pop-up blocking aggressiveness. (You can also turn off the option entirely.) By default, IE8 will block pop-ups and display an Information Bar warning (with that distinctive sound) whenever it finds one. This not only lets you know when the browser is working on your behalf, but it also gives you the opportunity to override the blocker and direct IE to allow the pop-up temporarily. You can also configure most blockers, including in IE8, to trust some sites entirely (allowing pop-ups) while continuing to block them on others. This is an invaluable option for sites that use pop-ups in a legitimate way and come from a source you trust. IE8's general pop-up settings are available from the Tools menu by selecting Pop-up Blocker Settings, and you can also configure detailed settings for sites in different zones

via the Security tab in the Internet Options dialog box.

Manage Malware

Simple advertising can be irritating but isn't necessarily harmful. The dangerous aspect of pop-ups arises with their frequent relationship to malware. Either as a method for malware to seek out unsuspecting hosts or as a product of malware that's already on



To configure Chrome's pop-up blocker, click the wrench icon and click Options. Click the Under The Hood table and then click the Content Settings button. Click the Pop-Ups tab.

the machine, some pop-ups indicate a much deeper problem.

Watch out for pop-ups or advertisements that appear out of nowhere when you're on trusted sites or not using the browser at all. Watch also for strange behaviors with no apparent cause, such as changes to your home page or redirections from your intended destination. General computer (or network) slowness, suspicious crashes, or disabling of antivirus and security software can all indicate malware running with its own purposes behind the scenes.

The most important way of fighting malware is to always use anti-malware tools such as anti-virus applications, firewalls, Registry cleaners, and antispyware utilities. Security suites combine multiple tools into a single package providing convenience and a guaranteed compatibility. All products are slightly different, and all require different configuration, but it's worth spending some time with your user guide to ensure that you know how to get the best protection possible. ■

BY GREGORY ANDERSON