

By: [Andrei Popa](#), Security and Search Engines Editor

[Google Rolls Out Anti-Phishing Filter](#)

Beside malware notifications, Google now provides phishing warnings

Since Google provides access to a huge number of websites, powerful security measures are obviously "a must," so every once in a while, the Mountain View-based company implements a new function or improves an older one. Today, Ionut Alex Chitu informs that Google now provides phishing warning, which means the user who searches for a certain query and then clicks on a phishing website included in Google's results, will get a notification telling him that the page may be a scam. As you know, Google integrated malware protection a long time ago and, with the help of StopBadware.org, it detected and blocked numerous dangerous websites which could deploy infections or other malicious files on visitors' computers. "Warning - phishing (web forgery) suspected. The site you are trying to visit has been identified as a forgery, intended to trick you into disclosing financial, personal or other sensitive information. If you are the owner of this web site, you can request a review of your site using Google's Webmasters Tools," the message displayed by Google's new anti-phishing filter reads. What's interesting to note is that some of the websites which were previously flagged as malware-infected pages are still indexed by Google and moreover, they can be visited without any security notification provided by the search engine. Although I'm not sure if this is a consequence of the new security filter, removing the "This site may harm your computer" alert may prove to be quite a bad idea. Until now, thanks to the partnership with StopBadware.org, the search engine displayed two malware notifications, one of them under the link returned on SERP and the other one displayed once the visitor clicked on the link. "This warning message appears with search results that we've identified as sites that may install malicious software on your computer. We want our users to feel safer when they search the web, and we're continuously working to identify such dangerous sites and increase protection for our users. Malicious software is often installed without your knowledge or permission when you visit these sites. Some examples of malicious software include programs that delete data on your computer, steal personal information such as passwords and credit card numbers, or alter your search results," Google described the feature at that time.