

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

[Google Talks about Phishing](#)

The Mountain View-based giant gives advice to remain on the safe side

Phishing attacks are extremely dangerous because they usually target financial details or other private information belonging to ordinary users. Unfortunately, the last few months came with a huge amount of phishing scams and the avalanche of attacks doesn't seem to look for an end anytime soon. Because of that, security companies around the world assault users with all kinds of advice, all of them with the same purpose: help consumers stay on the safe side and be protected when it comes to phishing scams. Even Google went out to give advice on phishing and, mostly like the security companies which talked on this matter, it recommended users to keep an eye on the links included in suspicious emails and to use browsers equipped with anti-phishing filters. Although you may have heard the same advice in the past, here are some scraps of the one [published](#) by Ian Fetter, Google Security Team, on the official Google Blog: *Be careful about responding to emails that ask you for sensitive information. Go to the site yourself, rather than clicking on links in suspicious emails. If you're not sure about a request you've received, don't be afraid to contact the organization directly to ask. If you're on a site that's asking you to enter sensitive information, check for signs of anything suspicious. Check the URL to make sure the page is actually part of the organization's website, and not a fraudulent page on a different domain (such as mybankk.com or g00gle.com.). If you're on a page that should be secured (like one asking you to enter in your credit card information) look for "https" at the beginning of the URL and the padlock icon in the browser. Be wary of the "fabulous offers" and "fantastic prizes" that you'll sometimes come across on the web. If something seems too good to be true, it probably is. Use a browser that has a phishing filter. The latest versions of most browsers -- including [Firefox](#), [Internet Explorer](#), and [Opera](#) -- include phishing filters that can help you spot potential phishing attacks.*