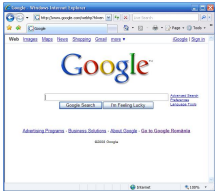


22 March 2008

By: Bogdan Popa, Security and Search Engines Editor



Google is now one of the most popular names on the web

[Fake Google Email Attempts to Steal Your Money](#)

Extra-care is recommended

We all know that Google, the Mountain View super search giant, communicates with its users by phone or by email every time users have to be informed about important matters. And if the emails' subject concerns AdWords, Google's money machine, the message is bound to be important and has to be read as soon as possible. Some Internet users have received recently a "Google" notification asking them to "update their billing information". Hmm, quite weird I would say, Google has never contacted me before in order to request such a thing. Let's have a closer look at the email message: it is titled "Please Update Your Billing Information" and seems to be sent by `adwords-noreply[at]google[dot]com`. The text message reads: "Dear Google AdWords Customer! In order to update your billing information, please sign in to your AdWords account at `https://adwords.google.com`, and update your billing information." The end of the email, "Sincerely, The Google AdWords Team," could make you swear that the message came from Google. OK, and now the juicy info. As you can see in the adjacent pictures, the links are supposed to get you to the Google AdWords page. There's even the https URI scheme meant to represent a secure HTTP connection. However, moving the mouse over the link (without clicking it!), shows the real link in the status bar of your browser/email client: `http://adwords.google.com.*****.cn/select/Login/`. That's right, it's a fake domain hosted in China. Classic, I would say but let's see some other details. Clicking on it gets you to a fake Google AdWords website that looks similar to the genuine one. In case you're one of those naïve folks out there and you simply avoid looking in the address bar, you may be tempted to enter your AdWords information. As you can see by yourself, the address bar reveals the real URL of the website, other than the genuine Google one. Getting back to the https syntax, the website doesn't really reveal any security measure. Moreover, the real link of the fake website actually contains the http syntax so it's obvious that leaving the page without entering your information would be a smart choice. But let's see how this page is different of the genuine Google website. Clicking anywhere on the Google AdWords website brings you the https URI scheme, informing you that you're 100 percent safe while browsing it. Have a look at the adjacent pictures. The email claims it was sent by a Google official. However, analyzing the email's headers proves that the phisher wasn't too focused on hiding his identity. Beside other information, we got his IP which reveals the fact that the phisher has sent the fake emails from Amsterdam. However, we can't know for sure if the sender was an infected computer, part of a botnet, or the actual scammer. I guess it's obvious that this is just a phishing scheme and a pretty smart one considering the fact that it attempts to trick you by using several genuine-like elements such as the links included in the email address or the message text which may lure you in disclosing your credentials. However, it uses the same classic and old-fashioned phishing techniques like the fake URL and fake website similar to a genuine one. So, next time you receive a suspicious website asking for your credentials, do not disclose them unless you check twice that revealing the information keeps you on the safe side; don't forget to check the links in the status bar BEFORE you click on them; install any security software that may help you in identifying phishing websites; look for the https syntax in the address bar of your browser; contact the service provider just after you notice you've been tricked. While I was writing this article, the Firefox guys have already added protection for the phishing website so every time a Mozilla user visits the page, he'll get informed that it's not a genuine one. We're still waiting to see similar action from Internet Explorer. Hopefully, the page gets shut down as soon as possible.