Subject: Phishing notification regarding dataminingtools.net
From: noreply@google.com
Date: Sun, 24 Jul 2011 00:01:43 +0000
To: abuse@dataminingtools.net, admin@dataminingtools.net, administrator@dataminingtools.net, contact@dataminingtools.net, info@dataminingtools.net, postmaster@dataminingtools.net, support@dataminingtools.net, webmaster@dataminingtools.net

Dear site owner or webmaster of dataminingtools.net,

We recently discovered that some pages on your site look like a possible phishing attack, in which users are encouraged to give up sensitive information such as login credentials or banking information. We have removed the suspicious URLs from Google.com search results and have begun showing a warning page to users who visit these URLs in certain browsers that receive anti-phishing data from Google.

Below are one or more example URLs on your site which may be part of a phishing attack:

http://dataminingtools .net/images/rm/www.paypal.co.nz/paypal.co.nz/paypal.co.nz/https/cgi-bin/webscrcmd=_login-run/webscrcmd=_account-run/updates-paypal/confirm-paypal/index.htm

Here is a link to a sample warning page:
http://www.google.com/interstitial?url=http%3A//dataminingtools.net/images/rm/www.paypal.co.nz/paypal.co.nz/paypal.co.nz/https/cgi-bin/webscrcmd%3D_login-run/webscrcmd%3D_account-run/updates-paypal/confirm-paypal/index.htm

We strongly encourage you to investigate this immediately to protect users who are being directed to a suspected phishing attack being hosted on your web site. Although some sites intentionally host such attacks, in many cases the webmaster is unaware because:

1) the site was compromised
2) the site doesn't monitor for malicious user-contributed content

If your site was compromised, it's important to not only remove the content involved in the phishing attack, but to also identify and fix the vulnerability that enabled such content to be placed on your site. We suggest contacting your hosting provider if you are unsure of how to proceed.

Once you've secured your site, and removed the content involved in the suspected phishing attack, or if you believe we have made an error and this is not actually a phishing attack, you can request that the warning be removed by visiting
http://www.google.com/safebrowsing/report_error/?tpl=emailer
and reporting an "incorrect forgery alert." We will review this request and take the appropriate actions.

Sincerely,

Google Search Quality Team

Note: if you have an account in Google's Webmaster Tools, you can verify the authenticity of this message by logging into https://www.google.com/webmasters/tools/siteoverview and going to the Message Center, where a warning will appear shortly.