Peter Cornish

From: Succinct Ideas [Succinct_Ideas@mail.vresp.com]
Sent: Friday, 11 September 2009 9:32 AM
To: peter.cornish@succinctideas.com.au
Subject: Website hacking on the rise

Click to view this email in a browser

succinct ideas

Succinct Update
Web site hacking on the rise

Sept 2009

Hi Peter,

Solar Spirit Australia

Solar Spirit Australia is a committed group of volunteers building a world class solar car for the World Solar Challenge 2009.

Facing competitors with budgets in the $ Millions this local SA team are operating on donations to build what is taking shape as a really viable entry.

Please help fund Solar Spirit Australia by purchasing a Watt Hour of Power

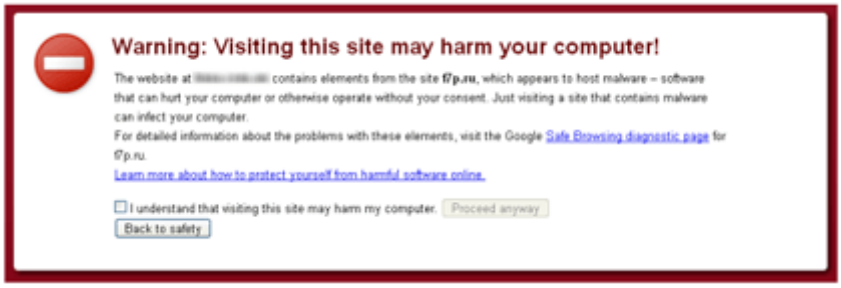
Please contact me on the details below if you have any questions at all.

I've encountered several 'hacked' websites recently and thought it was important to alert you to this disturbing trend.

The two forms of web site hacks I've encountered are those flagged by Google and a more furtive cloaked hack.

Flagged publicly by Google

This embarrassing alert is shown to visitors if Google determines your site has been hacked



I'm sure you agree that this is enough to scare off any prospective client, and so is commercially very damaging. Google displays this message if it determines your site has a connection with a known 'malware site'.

Malware means *malicious software*, and these sites use devious software to attack security vulnerabilities in your PC when you visit the site. The Google Online Security blog shows that reported malware sites have **doubled in 2009 to over 300,000!**

Although embarrassing, Google's message possibly avoids a costly litigious situation should a website visitor have their computer systems compromised and loose business as a result.

BTW Google will also freeze your AdWords advertising campaigns if your site is assessed as associated with malware.

Do you have a question on internet marketing that you would like answered ?

Email it to us and we will provide answers for the most popular questions in our next newsletter.

Your website's ability to promote your business comes to a grinding halt.

Cloaked hacking

Possibly more sinister because you don't know your website has been compromised, these hacks use your site as a 'link farm'.

The hackers add links from your site to their target sites to help improve the ranking of their sites. Read more about the value of links here.

The infected sites I've stumbled over have links to extreme anti-social and/or sexually explicit sites.

Apart from draining your Google PageRank, the links in this case are thankfully not visible to your visitors, but are visible to search engines.

Consequently your site runs the risk of reduced search ranking because as Google advises in its website guidelines:

"...avoid links to web spammers or "bad neighborhoods" on the web, as your own ranking may be affected adversely by those links..."

So these apparently benign links can seriously erode your website's search ranking.

Am I hacked ?

The most important aspect of this for business owners is how to detect and resolve any of this type of activity before clients or your business is exposed to any risk.

Google's **Safe Browsing Diagnostic** provides a quick and easy test to to assess the current status of your site:

www.google.com/safebrowsing/diagnostic?site=<insert your website address here>

De-hacking your site

If you find there is an issue with your site contact your web developer immediately to address it.

Normally the fix is technically simple; either removing the bad code or overwriting your published website with your offline

backup

You do have an offline backup of you website haven't you?

Declaring 'All Clear'

You could sit and wait patiently for Google to finally decide that you have eradicated the hack, but during this time your site continues to scare off new and existing customers.

Google WebMasters Tools provides a reconsideration lodgement facility to formally advise Google you have removed the hack. I note also that Bing now has a similar process.

You will need to register your site with Google WebMasters which itself may require assistance your web developer and/or an internet marketer.

It all takes time but eventually you will get the business stealing alert message removed.

Hack Prevention

How can you prevent hacks?

There is no simple answer; hackers are increasingly more sophisticated but here is a guide:

- Keep your PC's virus and spam software up to date
- Change passwords regularly
- Store your website's access details in a secure location
- Keep off-line backups of your site
- Monitor activity in your site
- Visit your own site occasionally

Summary

The internet provides global exposure to prospective customers as well as villains. Be vigilant and stay informed.

I hope you find this helpful information to coax your website into becoming a viable sales tool.

sincerely,

Peter Cornish
peter.cornish@succinctideas.com.au

If you think the information in this newsletter is useful, I encourage you to forward it to peers, business associates etc.

Previous newsletters; business presentations etc are available from www.succinctideas.com.au and my blog theinternetmarketer.com.au

Sincerely,
Peter Cornish

Forward this message to a friend

Succinct Ideas · (08) 8278 6545 · www.succinctideas.com.au
Unleash the internet sales potential in your business!