

# White Paper

**“This Site May Harm Your Computer”**

**How to Remove the Google Website Warning**

# Introduction

Businesses are increasingly using their websites as a critical marketing, lead generation and sales generator. In addition, cloud computing and business web applications for all of an organization's functions, from administration and accounting to product development and sales, are becoming increasingly popular. For some industries, business conducted purely online has become the default standard.

These increasingly critical gateways to businesses are under constant threat of attack by hackers leaving malicious code that can infect computer systems of the organization, partners and its web visitors. As well, unexploited websites that link to sites that have been infected also risk spreading malware.

Now organizations have even more incentive to ensure their sites and applications remediate all known web vulnerabilities effectively.

The most popular search engine today, Google, has taken steps to ensure browsers online can be protected from online threats. Google regularly scans websites to check for hazards like spyware, malicious code and software that could be used to infect computer systems of website visitors. If Google should discover such a site, they post a warning in any list of search results which shows that "this site may harm your computer".

Even if web surfers proceed to click through to the potentially hazardous website, a second screen shows a dire warning by Google about the consequences of proceeding to the site. These sets of warnings are likely to choke web traffic almost completely, since Google is the default search engine for so many people. For businesses reliant on web traffic for serving customers and operating their business, Google's warning poses a serious threat to business continuity, potentially even greater than the effect of being hacked by a cyber criminal, whose disruptive work may remain undetected.

This white paper will outline the steps that could be taken to remove the Google warning for a website. While PCIS has always recommended proactive security measures, this information will help organizations that have already been found to have exploited vulnerabilities to fix the problem and restore business operations.

# Steps to Remove Google Warning

For companies affected by malware insertions or other online threats, removing the Google warning "This site may harm your computer" from search engine results of the corporate website can be as much of a priority as remediating the problems on their site. While web visitors (and the website owner) may be unaware of threats lurking on the site, once Google has posted its warning in the search results, the ability of organizations to continue operating optimally, if at all, can be severely compromised.

Remediating vulnerabilities and fixing a website to remove problems will put an organization well on its way to getting rid of the Google warning, but there are other steps that may expedite the process.

## **1. Diagnose The Problem Google Discovered**

Google's Safe Browsing diagnostics page may help you determine what kind of badware (malware, spyware) Google detected on your organization's website. Use the URL, <http://www.google.com/safebrowsing/diagnostic?site=http://malware.testing.google.test/testin g/malware/> and insert your own website address into the section after /diagnostic?site=

This page will show you the following information:

- Whether the current listing status for the site is suspicious or not suspicious in search engines
- What happened when Google visited the site
- If the site acted as an intermediary for malware distribution
- Whether the site hosted malware
- How malware became present on the site.
- Instructions for next steps to take

## **2. Get The Information You Need To Fix Your Vulnerabilities and Remediate Problems On Your Website**

There are two common routes for getting the expertise that you need to fix the problems that led to a website being listed as harmful by Google.

The first method is checking the community forum such as the ones hosted by the Google partner organization Stopbadware.org for answers to how to fix your specific problem. The forum, Badwarebusters.org allows users to post questions and look for prior threads of discussions where their problem may have been dealt with.

Some information in this forum may be out of date or only applicable to a specific situation. On the other hand, as web threats are evolving day to day, this forum may contain highly relevant information to help your remediation steps proceed.

However, the administrators of Badwarebusters.org warn that the forum's resources are not exhaustive. Since it is a moderated open forum where anyone can contribute, users are advised to use the information provided at their own risk.

Other resources provided by the Stopbadware group include:

- Tips for cleaning and securing your website. <http://stopbadware.org/home/security>
- Stopbadware discussion group. <http://groups.google.com/group/stopbadware>
- Stopbadware frequently asked questions.  
<http://stopbadware.org/home/faq#partnerwarnings>

Alternatively, organizations may wish to use professional services such as a web security assessment to run a thorough check of a website's vulnerabilities and to recommend fixes. This may be a preferred method if your organization does not have the internal IT resources to find the problems and fix them. Particularly for businesses that require a solution that is as comprehensive and effective, this may be the preferred route.

Whether an organization chooses to use a Stopbadware forum or outside professional services, the solution may involve removing malicious code inserted by hackers onto a website. Further remediation may be necessary, such as dealing with hacked databases and other computer systems, exploited before or after the website was penetrated. It is important to ensure that known vulnerabilities are closed off to prevent a recurrence of the incident.

### **3. Request A Review of the Website from Google**

After an organization has taken the steps to make its website secure, the next step is requesting a review by Google to be re-scanned. If the site no longer contains or links to badware, the warning in the search results for the website will be removed.

Google will eventually re-scan all such sites automatically, but for businesses dependent on websites for considerations of operational continuity, it will be important to have the warning

removed as soon as possible. Requesting a scan may speed up the process, even though Google makes no guarantees about how soon such a re-scan will take place.

The request for a re-scan of a website can be done in two ways.

The first way is to create a Google Webmaster Tools account, ensure you are verified as the owner of the website, and follow Google's instructions for requesting a review.

The second way is to request an independent review by Stopbadware.org. Do this by finding the website to be reviewed in the Badware Website Clearinghouse by searching at <http://stopbadware.org/home/reportsearch>. Next, click the link for the site to be taken to the Stopbadware report for the site. Then click the "Request Review" button and fill out the form provided to submit your request.

If Google should conduct a review and the warning still remains, an organization may need to repeat this process. It is possible that some security vulnerabilities or malicious code were overlooked in the remediation process. Further steps to improve security may be required in this case before Google will de-list a site's warning.

# Conclusion

The steps required to remove a Google warning for a website are generally fairly straightforward. However, the details of the code review, vulnerability fixes and remediation to compromised systems can be extremely complex and require extensive resources.

Some website owners may be satisfied with the recommendations they find on public forums such as [Stopbadware.org](http://Stopbadware.org) for finding remediation solutions.

However, for organizations that depend on websites for important business functions and revenue generation, a web security assessment by a professional services provider can be the preferred route. This may be particularly relevant for organizations with very large websites that may require extensive remediation.

The efforts of the world's most successful search engine to improve security for users with warnings are laudable and a great improvement on the less-safe environment that transpired previously. The Google warning provides added incentive for website owners to ensure security for their website visitors, since the warning may be even more effective at deterring traffic than the effect of malicious code, which expert hackers can obfuscate.

Ultimately, website owners are responsible for ensuring their online presence does not harm visitors and users. By following good practices such as using a web application firewall, undertaking code reviews and ensuring compliance with security and privacy regulations, organizations will ideally be able to avoid undergoing the process outlined in this white paper and provide a safe online environment.

# About

## Pacific Coast Information Systems Ltd.

Pacific Coast Information Systems (PCIS) Ltd. is a full-service technology and consulting firm based in Vancouver. Founded in 1995, PCIS provides technical assessment & services, business analysis, and IT project management. More information about PCIS can be found at [www.pcis.com](http://www.pcis.com)

## Boonbox

Boonbox, a division of PCIS, was created in 2007. Boonbox specializes in productivity solutions that deliver immediate results in support of business challenges like security compliance, password protection and data backup issues. More information about Boonbox can be found at [www.boonbox.net](http://www.boonbox.net)