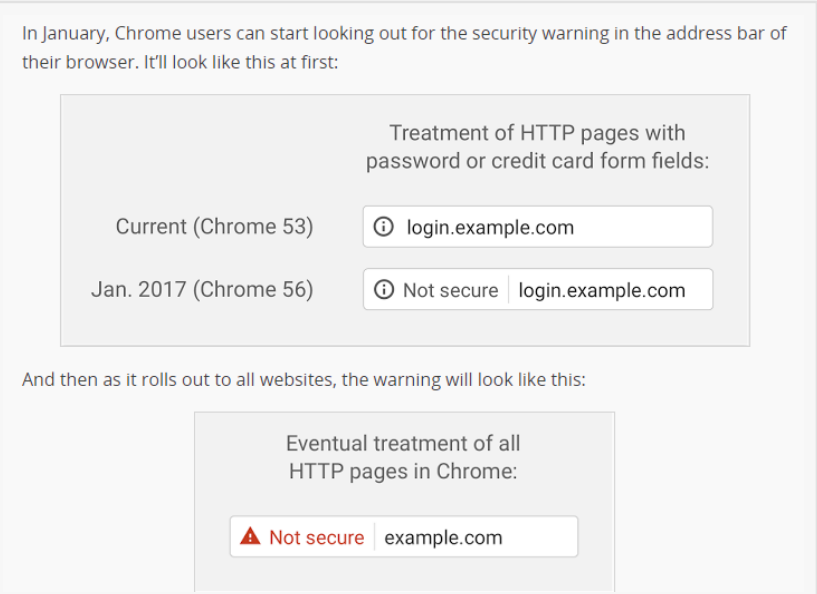
Canadian Web Hosting Sites Need to replace SSL/TLS Certs by Symantec, Thawte, VeriSign, GeoTrust and more Immediately!

PSA: Canadian Web Hosting Sites Need to replace Your SSL/TLS Certs by Symantec, Thawte, VeriSign, Equifax, GeoTrust and RapidSSL Immediately!



Chrome Https Warning

Canadian web hosting leader

CALGARY, ALBERTA, CANADA, March 22, 2018 /EINPresswire.com/ -- This is a PSA (public service announcement) by HostedinCanada.com, a leading Canadian Web Hosting provider. This is a reminder to all website owners. Google's Chrome browser, which currently makes up 77.9% of browsers used on the internet, and has grown almost every year since 2008, starting at 3.1%, has already started the process of ending support for Symantec SSL/TLS certificates. This includes companies owned by Symantec including Thawte, Verisign, Equifax, GeoTrust and RapidSSL.

Chrome 66 is ending support for Symantec certificates issued before June 1, 2016 on the following schedule:

• The 'Canary' release already ended support for these certificates. It was released on January 20th, 2018.
• The Beta release for Chrome 66 will be released on March 15th.
• The Stable release for Chrome 66 will be released on April 17th.

If you are running a Symantec certificate issued before June 1, 2016, and you do not replace that certificate, then from April 17th onwards this is what your site will look like to site visitors (See attached Image)

As you can clearly see, the error is described as NET::ERR_CERT_SYMANTEC_LEGACY, meaning that your website is using a legacy Symantec certificate that is no longer supported.

Starting with Google Chrome version 70, all remaining Symantec certificates will completely stop working, including those issued after June 1, 2016. Chrome 70's release schedule for Canary, Beta

and Stable is July 20th, September 13th and October 16th respectively.

To check if your certificate will be affected by this change, you can visit this page and enter your website's hostname in the form provided: https://www.websecurity.symantec.com/support/ssl-checker.

If your website has an issue, the page should give you a warning. Make sure you just enter the hostname and remove the https:// prefix and the ending slash.

An alternative way to check if your website will have a problem is to download Chrome's bleeding edge 'canary' version and visit your website. Then check the DevTools in Chrome for any warning message regarding your SSL/TLS certificate.

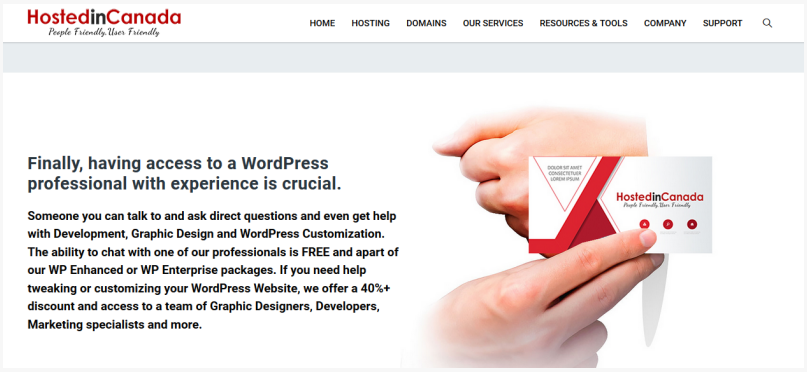
You can find more info on the official Google Security Blog.

If you need assistance contact HostedinCanada.com toll-free from anywhere in North America at 1-866-730-2040, as they can help you transition to a supported SSL Certificate. If you host with them they will provide a FREE SSL Certificate for a limited time. (Use Code FREESSLMARCH if ordering or switching to HostedinCanada.com) Also, please help spread the word. If you know anyone else who owns a website share this message, so they are not caught by surprise when this change goes live next month.

Dean Wolf
HostedinCanada.com
866-730-2040 #207
email us here

WordPress Hosting Canada

Best web hosting Canada



Best WordPress Hosting in Canada