Dealing with Security Certificate Warnings
Posted By : Ken Colburn of Data Doctors on July 27, 2016

Question

What do I do when I get this message: "There is a problem with this website's security certificate"?

Answer

We've all been taught to look for HTTPS: (HyperText Transfer Protocol Secure) at the beginning of a website whenever we're going to make a purchase online.

This ensures that the information you're typing on the page is encrypted between you and the trusted website so that your information stays secure.

The warning message you're asking about typically appears on sites that require this level of security, such as any site that requires you to log in or make purchases online.

A security certificate is a means to ensure that the site owner is who they say they are resulting in the famous 'lock' image that helps you know that you're on a secure site.

Think of them as a way to authenticate the owner of a website much like your username and password are used to authenticate you as a user.

The complexity involved in Internet security can get a bit technical, but for the most part, whenever you see this error on a site where you are being asked to provide sensitive information, you should be very cautious.

When you see this message pop up, your browser is essentially telling you that it can't verify the authenticity of the website you are visiting because there is a problem with the security certificate.

The causes for this warning message can vary greatly and often times does not necessarily mean that something nefarious is in play, but you should still always be cautious.

Something as simple as your computer's date and time being off can cause this but so can a slightly mistyped URL that lands you on a scam site.

A common cause is that the website owner hasn't renewed their security certificate (as in it was once valid, but has since expired) or they're using a free Certificate Authority service such as CAcert.org (http://cacert.org) that isn't necessarily trusted by some browsers.

If you know for sure that the website is legitimate, you should alert the website owner of the warning so they can fix the problem on their end.

Keep in mind, this can also be a clear alert that the site you're visiting isn't a legitimate site and can't be trusted.

Creating very convincing duplicate websites is not very hard to do these days, so you've got to always pay close attention to security indicators like the picture of the lock and these security warnings that can come from Google, your browser or from your security software.

If you're not sure about a site, you can use a third-party site checker such as Sucuri's SiteCheck scanner (https://sitecheck.sucuri.net) to get a full report on the site that will check for known malware, blacklisting status, website errors and out-of-date software.

If you regularly visit a site that you know is legitimate but gives you this error, there are ways to bypass the message for just that site, but I'd only suggest this for tech savvy users (by doing a Google search).