



Google Chrome to Start Labelling Non-HTTPS Sites as “Not Secure”

*By Paul O’Neal, President,
International Networking, Inc.*

The purpose of this article is to help you ensure your website is a secure and trusted website for your patients to visit. Google has big changes in store for the way their Google Chrome browser will handle access to websites in the very near future. The first change will occur in July 2018 with the release of **Chrome 68**. Google Chrome is by far the most widely used browser on PC’s and laptops with its market share around 60% and the next closest competitor coming in around 10%.

But first a little core technology background. Hypertext Transfer Protocol (**HTTP**) was created in 1989 and is the foundation of communication for the World Wide Web.

When the World Wide Web (www) came on the scene in 1989 users needed a friendly interface which would allow them to view pages

graphically on the internet, thus in 1990, the birth of the first internet browser.

Later in 1994, Netscape Communications would go on to create for its Netscape Navigator a HTTP Secure (**HTTPS**) web browser. Originally, HTTPS was used with the SSL protocol. As SSL evolved into Transport Layer Security (TLS), HTTPS was formally specified by RFC 2818 in May 2000.

As an example. If you want to see what model cars Ford currently has to offer you most likely would open your favorite internet browser and type “Ford” in the browser bar, press enter and voilà a world of information appears.

But here is what actually happens. Like 90% of internet users you probably used Google as your search engine. If you are a Google user when you searched for “Ford” Google returned search results of the biggest players (aka: ad payers) at the top of the search results. If you were to click on the first Ford result at the top of the page you would seamlessly



be redirected to **https://www.ford.com**.

Google uses a variety of signals and algorithms to calculate search engine positions in order to determine what/who you see when you enter a query. Which brings us to Google SEO (Search Engine Optimization) and analytics. In the early days of the Internet all this convenience did not exist. If you wanted to access a site or page you had to specify a protocol such as ftp or http followed by :// then type the name of the computer usually www or ftp, the domain name followed by the extension (com, edu, org, net, etc.) looking something like this: *http://www.exampledomain.com*.

Thankfully, many strides have been made requiring less information to be typed in the browser bar because programmatically values have been set so there is no longer a need to include the *www* OR *http* because the DNS and/or the web host should configure how to handle web traffic. If we want direct access to a website and it is properly configured simply typing *Ford.com* will take us directly to their website.

As mentioned earlier, Google has plans to begin enforcing stricter security policies with the release of **Chrome 68**. If you have Chrome installed on your computer(s) it should roll out to end users automatically.

But now lets talk about how this will affect your practice's website and possibly patient portals. If your practice/business website isn't configured

properly then your patients/site visitors will see a **"Not secure"** warning in the browser bar which will potentially expose them to security breaches and insight FUD (fear, uncertainty and doubt!)

It's quick and easy to see if your website is set up correctly. Simply follow the steps below:

1. Ensure your website has a valid and trusted SSL certificate installed. For this test, I strongly recommend you use a Google Chrome browser. In the browser bar type: **http://www.ininc.com** (of course you will type *http://www.your own domain name and specific extension such as org, edu*). If you see a lock and the word Secure you're in good shape.

Notice in the example below even though I sited that you should type in **http://** my site automatically redirected to **https://**

If you see the words **"Not Secure"** then you have some work to do in order for your site to be redirected correctly. When you contact your tech support regarding this issue make sure you also have them ensure your website has a valid and trusted SSL certificate installed. If you do find yourself needing to acquire an SSL Certificate and your website does not directly handle the processing of money you probably do not need to buy an expensive certificate that a hosting company may try to upsell you. The main free CA or Certificate Authority is Let's Encrypt. <https://letsencrypt.org/>

[CONTINUED ON PAGE 15]

HOW VISITORS WILL SEE YOUR SITE DISPLAYED WITH & WITHOUT SSL



**WITH SSL
& HTTPS
REDIRECTION**



Secure https://www.ininc.com

with SSL certificate showing HTTPS



**WITHOUT SSL
& HTTPS
REDIRECTION**



Not secure www.ininc.com

NO SSL certificate showing insecure HTTP

[Chrome continued from page 9]

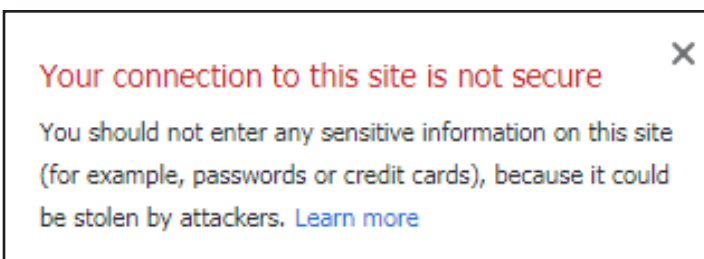
*NOTE: If you check your website before the **Chrome 68** rollout you will only see ⓘ
The words **Not secure** will not appear until after the rollout.*

2. Ensure your hosting service is set up to drive all traffic to use https. You will need to contact your hosting company to verify this is done.

3. Lastly make sure all your SEO is directed to and using the https protocol (https://www.yourdomain.com). If your website and hosting is set up correctly then searches should automatically be redirected; however, if you continue to use and promote http:// Google will deprioritize your website which will adversely affect your ranking.

That's it!!

I have also included an example below of a current Google Chrome 67 browser bar verses what the browser bar will look like with the July Google **Chrome 68** rollout. Notice they have added "**Not secure**" which is exactly what your patients/visitors will see. If your patient/visitor clicks the ⓘ Not Secure tab they will see the following message:



Do you think this message may scare away more than a few of your website visitors. I certainly wouldn't risk it

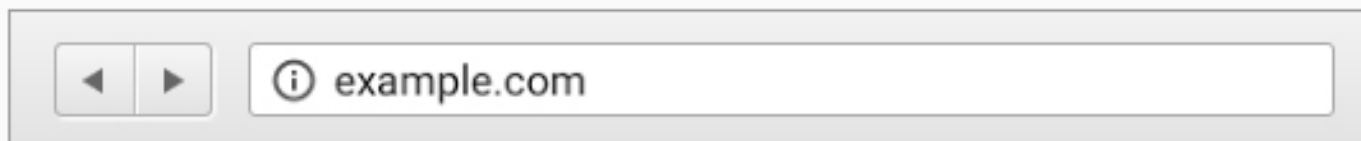
As I was writing this article I researched some Wake County medical practices and noticed quite a few that are not setup correctly. I hope this article has given you the information and motivation you need to get your website ready for the Big Google **Chrome 68** rollout.

Google has been deprioritizing websites that don't use **https** since 2014 so your search results have been suffering if you have been using **http** but with this new security push you run an even greater risk of losing precious traffic to your site if you can't provide a secure and trusted website for your patient's to visit. §

www.ININC.com • 919.845.1703 • paul@ininc.com

Treatment of HTTP pages:

Current (Chrome 67)



July 2018 (Chrome 68)

