

# Google Security Blog

The latest news and insights from Google on security and safety on the Internet

---

# HTTPS as a ranking signal

August 7, 2014

Cross-posted from the [Webmaster Central Blog](#)

Security is a top priority for Google. We invest a lot in making sure that our services use industry-leading security, like [strong HTTPS encryption by default](#). That means that people using Search, Gmail and Drive, for example, automatically have a secure connection to Google.

Beyond our own stuff, we're also working to make the Internet safer more broadly. A big part of that is making sure that websites people access from Google are secure. For instance, we have created resources to help webmasters [prevent and fix security breaches](#) on their sites.

We want to go even further. At [Google I/O](#) a few months ago, we called for "[HTTPS everywhere](#)" on the web.

We've also seen more and more webmasters adopting [HTTPS](#) (also known as HTTP over [TLS](#), or Transport Layer Security), on their website, which is encouraging.

For these reasons, over the past few months we've been running tests taking into account whether sites use secure, encrypted connections as a signal in our search ranking algorithms. We've seen positive results, so we're starting to use HTTPS as a ranking signal. For now it's only a very lightweight signal—affecting fewer than 1% of global queries, and carrying less weight than other signals such as [high-quality content](#)—while we give webmasters time to switch to HTTPS. But over time, we may decide to



strengthen it, because we'd like to encourage all website owners to switch from HTTP to HTTPS to keep everyone safe on the web.

In the coming weeks, we'll publish detailed best practices (we'll add a link to it from here) to make TLS adoption easier, and to avoid common mistakes. Here are some basic tips to get started:

- Decide the kind of certificate you need: single, multi-domain, or wildcard certificate
- Use 2048-bit key certificates
- Use relative URLs for resources that reside on the same secure domain
- Use protocol relative URLs for all other domains
- Check out our [Site move article](#) for more guidelines on how to change your website's address
- Don't block your HTTPS site from crawling using robots.txt
- Allow indexing of your pages by search engines where possible. Avoid the noindex robots meta tag

If your website is already serving on HTTPS, you can test its security level and configuration with the [Qualys Lab tool](#). If you are concerned about TLS and your site's performance, have a look at [Is TLS fast yet?](#). And of course, if you have any questions or concerns, please feel free to post in our [Webmaster Help Forums](#)

We hope to see more websites using HTTPS in the future. Let's all make the web more secure!

Posted by [Zineb Ait Bahajji](#) and [Gary Illyes](#), Webmaster Trends Analysts



**55 comments :**

 **Igor said...**

I like the idea of more websites becoming secure.

But, what about websites that don't have login forms or any other user input? I believe users on these kind of websites would not benefit from HTTPS in any way, or am I wrong?

[August 7, 2014 at 2:25AM](#)

 **Anonymous said...**

I think the biggest barrier may be the lingering perception that TLS certificates are expensive. They don't have to be, anymore, but people still think of them that way. This is also a major reason people still use self-signed certs.

[August 7, 2014 at 2:32AM](#)

 **patrickcoombe said...**

Just read about:

<http://www.startssl.com/>

which does appear to offer a decent certificate for free. Not sure if it has all of the characteristics G is looking for and it does have limitations but a good option for some.

[August 7, 2014 at 2:55AM](#)

 **Unknown said...**

Any thoughts on people using Github Pages? There's no way to make that secure. Our site, <http://kili.io> is public and I really want https there, but it's not doable right now.

[August 7, 2014 at 2:56AM](#)

 **C.Hofmann said...**

That is the End of every cache based ISP, because there is no Standard distinguish "Important" things like Money Orders from "Unimportant" ones where it may use full using https enabled cache. Also Virus functions in firewalls are lost their function. I know, in nearly every Company there are "old" Computers for more ore less exotic application. Theses apps are still need but it is to expansive to port them to a newer operating system, for example the vendor have discontinue development of the software and an alternative is only avail within a bigger other package.

If Google prefers transmits "https" link to external sides, i am not sure about a security

increase. Its more a business Boost  
for Googles Drone Based Internet.

[August 7, 2014 at 3:23AM](#)

**e** **Persephone Hallow** said...

Firstly, it annoys me that Google has lifted the term "HTTPS everywhere" with no reference or citation of EFF (the Electronic Frontier Foundation), who made a plugin with that exact name, for that exact purpose (<https://www.eff.org/https-everywhere>). Great that you want to support the concept, but at least refer to the original creators of the plugin (it is the first link when you Google the term - congrats on using your own most popular product so well!)

Secondly, doesn't this scream irony? Google scans Gmail regularly as a matter of course, and will report users storing or sharing child pornography to authorities. Whilst I of course find child pornography abhorrent, isn't it ironic that Google - who has decided to police the information we share when using their services - wants to improve internet security?

Two questions of morality have been raised and overlooked here: one of the literal "moral rights" to the intellectual property of "HTTPS everywhere", and one about trusting the intentions of a company who seeks to erode online anonymity and has taken it upon itself to police our communications. Would love to know how you reconcile all this with your noble goals of providing better internet security for all.

[August 7, 2014 at 3:46AM](#)

**e** **Unknown** said...

Maybe the blog should be on https then, that would be a good first step.

[August 7, 2014 at 4:42AM](#)

**e** **Unknown** said...

The https requires a dedicated IP address and considering the shortage of IPv4 addressees and the cost involved in buying SSL certificate and IP address, this ranking signal is going to give undue benefit to the websites over those who may not be willing to invest on https. It should be put off until IPv6 is fully implemented and the cost of SSL is drastically reduced.

[August 7, 2014 at 5:00AM](#)

**e** **Chris W** said...

As I understand, an SSL certificate requires a dedicated IP address and RIPE don't like giving us IP addresses as it stands already.

If we go down the route of 1 website = 1 IP, won't we run out of IPv4 addresses in a heartbeat?

[August 7, 2014 at 6:07AM](#)

**e** **Ed** said...

Ironic this post is an http, not https. Otherwise, a welcome move!

[http://googleonlinesecurity.blogspot.co.uk/2014/08/https-as-ranking-signal\\_6.html](http://googleonlinesecurity.blogspot.co.uk/2014/08/https-as-ranking-signal_6.html)

Reported on [inbound.org](http://inbound.org)

[August 7, 2014 at 6:16AM](#)

** AndroTux said...**

I'm not sure if this is a good idea. It will slow the page down and isn't required for simple blogs like this one or other static content.

[August 7, 2014 at 6:27AM](#)

** gcds said...**

Sometimes the problem is not the HTTPS but the thing that you have to buy certificate from specific list of providers. Your own signed certificate its like hacking attempt to user browser... I wish google would give away certificates for verified websites and we all would see many websites transitioning to HTTPS

[August 7, 2014 at 7:01AM](#)

** Robbie said...**

It's mildly amusing that the Google Online Security Blog, arguing for the importance of "HTTPS everywhere", gives me a 302 redirect from HTTPS -> HTTP. What's up with that?

[August 7, 2014 at 8:06AM](#)

** Paul van Brouwershaven said...**

Will strong authenticated SSL Certificates (OV, EV) have a bigger impact on my ranking than domain validated SSL Certificates?

[August 7, 2014 at 8:14AM](#)

** Anonymous said...**

If you care so much about TLS, go run a proper CA with free Class 1 certs. The current CAs are at least 2 of these: not trustworthy, careless, not free. I'd go and deploy it everywhere if there wasn't a cost barrier. And before people start screaming StartCom: They are scum. They tried to charge people for wanting certs after heartbleed revoked and where straight up dicks about it on Twitter too.

[August 7, 2014 at 10:16AM](#)

** Unknown said...**

On a positive note this will probably really improve the quality of search results as spammy/malware site will be highly unlikely to use SSL. In fact this could be really quite efficient!

On a side note though, In terms of privacy/security I personally think this is all rather pointless. If your site needs HTTPS chances are your using it. For all other sites this is kinda a useless feature. Government organisations will not have issue decrypting the data. Determined people can already break HTTPS within a \$10,000 budget and a couple of days. All this does is add a useless extra layer of complexity and also cost - which might make lots of SSL vendors very happy. Sure there is 1 single company in the world that apparently does free SSL (StartSSL), but the average user will pay for one. Not to mention the performance overhead you now introduce.

And I'm personally surprised that Google would chose to push such broken and poorly implemented technology rather than using it's collective power of geniuses, engineers and influence to create and push a better more secure SSL replacement (Everyone wants one, everyone agrees SSL sucks. There have been a few attempts, but lack of technical and corporate influence is really stalling the process from moving mainstream). It sure would be a hell of a lot easier PRIOR to essentially forcing the whole internet to adopt SSL. Then again if there is anyone

that knows how to shoot themselves in the foot with this stuff it's certainly Google. I mean I really love you guys, but you do have a track record of making life harder for yourself in the future by doing the wrong things at the wrong time.

What does your foresight tell you about the pain it will be to, in future years, to convince the (generally) incompetent and lazy mass known as webmasters to adopt a new technology after you effectively forced them to finally get off the couch and start using SSL after all these years? Perhaps this is actually a great opportunity to try to finally introduce something better? Please think about it. I'm not sure there is any other entity on this planet at present that could pull it off other than you. Please fix the internet (again!) because right now it's kinda broken... :(

[August 7, 2014 at 10:34AM](#)

 **Anonymous said...**

Regarding the last bullet point:

"Allow indexing of your pages by search engines where possible. Avoid the noindex robots meta tag"

Can you please clarify if this is general advice, or if you are specifically referring to HTTPS pages.

[August 7, 2014 at 10:43AM](#)

 **Unknown said...**

I'm not sure how this actually makes the user more secure.

OTOH, it will drive up costs and place barriers to entry for new sites.

For any non-ecommerce site, like those that are advertising-based, this initiative is a non-starter until all advertisers move to HTTPS. Until then, any move to HTTPS in their base page will preclude any advertising.

[August 7, 2014 at 11:44AM](#)

 **OanaG said...**

First of all I find it a bit odd to say the least to get SEO recommendations from the security team at google.

My question is regarding the last bullet point: "Allow indexing of your pages by search engines where possible. Avoid the noindex robots meta tag"

Is this applicable to webmasters using wordpress as a CMS?

wordpress is widely used as well as well known for its habit of creating multiple pages with duplicate & thin content see tags, taxonomies and so on, pages where a canonical tag cannot be used. What happens when a custom solution is not available?

[August 7, 2014 at 11:53AM](#)

 **Anonymous said...**

I'd love the idea of having encryption everywhere, but Google has been giving mixed signals on this. Recently DuckDuckGo's XMPP Server stopped being able to communicate with Google Talk users because Google Talk supports server XMPP Federation but not over an encrypted channel. (See <https://duck.co/blog/xmpp-s2s>)

And as others have said, why not at least start with your own blogging platform?

[August 7, 2014 at 12:27PM](#)

**e Unknown said...**

My site uses Https, but only for the sites it needs to, like the payment system, cart, user login site and other pages where users post information to.

Is this what you want?

Or are you looking for a complete https integration?

[August 7, 2014 at 1:09PM](#)

**e mdav (IRC) said...**

I get this and endorse it. I would also be perfectly fine with IPv6-reachability as an additional ranking signal.

[August 7, 2014 at 1:11PM](#)

**e sebas said...**

In my current project I had to disable https on the request of our seo, because Google was ranking it actually down due to slightly lower page speed. Since the signal is not strong yet, the step from google is just a correction of the current practice of punishing developers for being concerned about user security.

[August 7, 2014 at 1:38PM](#)

**e inkovation said...**

So an e-commerce site that currently uses SSL on account and checkout pages should now redirect the entire site to https?

[August 7, 2014 at 5:20PM](#)

**e Unknown said...**

To both Chris W and Santosh Mishra:

TLS has an extension capability called SNI, this capability enables the client to send the requested server name within the TLS session, and in turn allow the server to present the correct certificate.

The biggest downside to SNI, is from a network monitoring approach, things like netflow cannot distinguish the requested sites within the volume of TLS traffic. Historically this has been pretty simple to manage with a 1:1 relationship between IP and TLS cert, it just means now you have to shift the investigation to the webserver logs, and in turn more overlap between network people and systems people, then again that may not be such a bad thing.

[August 7, 2014 at 6:46PM](#)

**e Jonathan said...**

It's 1765 all over again!

As a veteran of dotcom boom 1.0, I learned that every old idea will be reintroduced with "on the Internet" pasted on the end. Apparently, in the dotcom boom 2.0, we now have the certificate-industrial complex conspiring with Google to implement a private-sector version of the Stamp Act

of 1765.

Despite having a keen interest in information security and a desire to see strong crypto everywhere, I find this change unacceptably exclusionary, superficial and self-serving in the present context. A previous commenter suggested Google offer free class 1 certs to all comers, and I think that would be a fair mitigation of the elitism inherent in favoring https URLs. Ideally, the entire system of rent-based trust would be scrapped and replaced with something more public-minded, but I understand that parasitic rentiers don't just curl up and wither away when asked nicely.

I allow Google ads through my firewall because it is democratic, in the weak sense that everyone's money is just as green. There's no reason for me to continue using Google services and staring at Google ads if gentrifying the Web is any part of the company's agenda.

[August 7, 2014 at 6:48PM](#)

 **A Hettinger said...**

Do these "SEO Bonus Points" apply to all sites which serve on both HTTPS and HTTP, or just ones which send all traffic to HTTP?

[August 7, 2014 at 7:42PM](#)

 **Greg Grothaus said...**

*This comment has been removed by the author.*

[August 7, 2014 at 8:01PM](#)

 **Unknown said...**

We need guide for best practices, stackoverflow is overload for "HTTPS Issue".

[August 8, 2014 at 4:32AM](#)

 **Unknown said...**

We're 17 comments in and everyone has missed the primary reason for insisting on an SSL cert nowadays: encryption of *\*all\** traffic - especially cookies.

Take a look at the Firesheep vulnerability (<http://en.wikipedia.org/wiki/Firesheep>) and the solution. Firesheep let you sit on a public hotspot and borrow peoples Facebook, Twitter and Amazon logins (etc) as the cookies that represented a valid logged in user were passing unencrypted through the hotspot. This problem prompted many companies to go SSL only.

Any website that allows membership or logins should now be SSL only. Better search engine results are a great encouragement - people will do the right thing for the wrong reasons and a tipping point may be reached.

Site identification, or even form encryption, is now secondary to traffic encryption - unless you want strangers using your accounts via a single click.

SSL is no longer a significant burden on clients or servers (unless you have barely sufficient hosting resources.) and the right kind can be cheap and work in shared environments as their *\*only\** goal is encryption.

[August 8, 2014 at 4:35AM](#)

**e Pooja said...**

What is the use of SSL certificates for information or content based websites?

August 8, 2014 at 4:58AM

**e The Dill Design said...**

I made a blog post about my experiences with HTTPS and SEO which goes right in line with this article. Even though SSL is great (and I do recommend it), there are implication in design and SEO that a webmaster should be aware of: <https://www.virginiaseo.org/blog/how-does-ssl-affect-your-search-engine-optimization/>

August 8, 2014 at 8:38AM

**Anonymous said...**

For those concerned with firewalls not being able to detect problems, you can use SSL DPI to mitigate this issue. I only recommend this for corporations, not public wifi etc., but it is a nice option.

See this for more information:

[http://www.sonicwall.com/downloads/SonicOS\\_Enhanced\\_5.6\\_DPI-SSL\\_Feature\\_Module.pdf](http://www.sonicwall.com/downloads/SonicOS_Enhanced_5.6_DPI-SSL_Feature_Module.pdf)

August 8, 2014 at 9:49AM

**e Unknown said...**

What?? 1) https is slower than http and 2) most sites do not take any personal information, 3) need dedicated IP4 addresses until IPv6 becomes 100% adopted, which will not be possible. I really hope you are not penalising sites like that, you are forcing customers into high running costs for no reason. There ay be cheap SSLs out there, but customers will end up paying techies like me to install them each year, \$\$.

August 8, 2014 at 10:04AM

**e Ivan Rojas said...**

1% for just having ssl certificate is worth the expense, im going to aply this setting to our dedicated servers

August 8, 2014 at 10:08AM

**e Unknown said...**

Perhaps Google should start offering free multi-domain SSL certificates, if they're ~~really~~ serious about this. StartCom is useless for any domain that has more subdomains than just 'www', and they don't care about security either (as evidenced by their paid revocation). CACert is great, but not widely trusted by browsers or operating systems.

There are currently no usable free certificate providers, and it's effectively an extortionist market ("pay us or browsers will complain about you!"). Not everybody has money to spend on SSL certificates. If and only if you can change that, this kind of "HTTPS everywhere" attitude has actual teeth.

August 8, 2014 at 3:14PM

**e the Ramen Noodle said...**

So this means we can now pay to have our websites rank higher ... but be slower.

Prioritizing faster sites is smart and human.

But I don't think humans care about whether their favorite blog is HTTPS.

[August 8, 2014 at 3:51PM](#)

**e VIMLESH said...**

So, what now? without https sites have to see the drop in ranking or to use https service.

[August 9, 2014 at 1:47AM](#)

**e Unknown said...**

SSL / TLS and encryption in general should be **only** be used where it is needed when it is needed, but NOT everywhere Google! (What a significant waste of resources and CPU!). Why would a public blog ever need SSL? Why would a online newspaper need it's posts encrypted? Seriously you must have a hidden agenda behind this since there is absolutely no technical grounds behind your ssl everywhere proposal for a safer internet.

If it does become a significant signal then we can all say bye bye green (eco friendly) computing! And hello to thousands of wasted megawatts per day! Preposterous & appalling!

[August 9, 2014 at 3:37AM](#)

**e Unknown said...**

Why on earth would i secure my site if i am running blogs or something like that? I mean i dont have to deal with customers, or their billing stuff.

[August 9, 2014 at 7:20AM](#)

**e Unknown said...**

But you don't think this blog deserves SSL encryption?

[August 9, 2014 at 2:15PM](#)

**e AmericanDissident said...**

@Igor, while there isn't quite as much at stake on a page that has no login or other forms, there are some positives to HTTPS everywhere, even on a static webpage – especially in light of, er, recent revelations. There are two that I can think of offhand, though I'm sure there are more:

1. An eavesdropper on the network won't be able to tell which pages you're visiting on a site. For example, if I visit youtube.com on an encrypted connection, an eavesdropper will know I'm visiting youtube.com, but will have no idea if I'm watching a video related to an embarrassing medical condition, questioning one's sexual orientation, police brutality, or a cat video. With HTTPS, anything after the domain name is encrypted and can't be intercepted (assuming it's been properly implemented).

2. With HTTPS, you are also assured that you're not being connected to an impostor site and that the site's contents are not being altered in transit (assuming the ~~entire~~ site is delivered over HTTPS). This can help reduce the chances of malware being delivered to you via a man-in-the-middle attack. Also, a repressive government might want to alter the content of dissidents' websites in transit for the purposes of character assassination. Properly implemented, an HTTPS connection can help prevent this.

[August 9, 2014 at 4:26PM](#)

**e Unknown said...**

To those who are claiming that this is a bad idea because SSL requires a static address, and we are running out of IPv4 addresses, I'd encourage you to check out RFC4366 (SNI or Server Name Indication) which resolves this issue. It does require a webserver that supports SNI (most modern http servers do) as well as a client that also supports it. As with servers, most major modern web browsers also support it. So limited IPv4 space, while an issue in other ways, is not an issue here.

[August 10, 2014 at 1:35AM](#)

**e <> said...**

@David If you have your content both on HTTP and HTTPS, and your HTTPS URLs have a noindex robots meta tag, then Google won't be able to index the HTTPS URLs.

[August 11, 2014 at 4:09AM](#)

**e Nick West said...**

To clear up a couple misconceptions in the comments, you no longer need a dedicated IP per domain for SSL to work. With the end life of XP, all modern browsers now support SNI. This means your server can host multiple domains with a single IP with minimal effort on the sysadmin's part, and have valid certificates on each domain. SNI is also supported in the latest version of cPanel/WHM, so big hosts can now support SSL without selling dedicated IPs too.

Certificates also don't have to be expensive. There are plenty of places that offer low cost (sub \$10/year) certificates, and startssl (as mentioned earlier) has free, perfectly valid Class 1 certs.

[August 11, 2014 at 2:37PM](#)

**e Chris W said...**

To the guys who mentioned SNI - THANKS!

[August 13, 2014 at 4:12AM](#)

**e Unknown said...**

@Chris W, np!

[August 14, 2014 at 2:43PM](#)

**e Unknown said...**

I fully support the idea of using https. Enough of online data hijacking. After all people need some level of confidence when browsing, shopping online. If brands like google.com, mallena.com, paypal.com, and so on can move to safeguard data, then they are on the right path and Kudos to them.

[August 17, 2014 at 12:13PM](#)

**e Mite Mitreski said...**

Does google intend to enable https for blogger?  
It is kind of ironic that this blog post is served under HTTP..

[August 17, 2014 at 8:38PM](#)

**e Unknown said...**

To the guys that mention SSL is so expensive - it is not if you buy through a distributor rather than from the CA, e.g. here: [Cheap SSL Certificates](#)

Starting at less than US\$10 per year - and you also do not have to send a copy of your ID to a Middle-East company (as with StartSSL)...

August 18, 2014 at 1:48AM

 **ISTTM said...**

Some very helpful advice! The one which I think most people forget is the bonus tip at the bottom- simply thank people who link to you! Same goes with people who retweet one of your tweets or someone who takes the time to follow you on Facebook. Granted, some are simply doing this to help market themselves but some are not. So take a couple of seconds and send a "Thanks". You never know what it may lead to.

[seo services in Hyderabad](#)

September 16, 2014 at 9:16AM

 **Robin Mathew Rajan said...**

For many who commented here, erroneously said, a dedicated IP is a must to employ SSL/TLS cert. While it's partially true, a dedicated IP is not a must **We can enable SSL/TLS cert even without a dedicated IP.** Check my blog.

<https://www.robinmathewrajan.com/ramblings/>

My website is running without a dedicated IP and yes, it does have TLS cert.

All the latest browsers which support **SNI (Server Name Indication)** can load a SSL/TLS webpage without a dedicated IP on it. While it's true that SNI is not supported in older browsers, that's not much a problem I think.

Refer: [http://en.wikipedia.org/wiki/Server\\_Name\\_Indication](http://en.wikipedia.org/wiki/Server_Name_Indication)

On the other hand, **a dedicated IP is a must when enabling an anonymous public FTP server.**  
have two such servers.

[September 17, 2014 at 3:55AM](#)

 **eco said...**

I just mentioned on Google+ about Wordpress issue with HTTPS.<a href="https://plus.google.com/115781251724773943513/posts/YSgBwpkjcFK">Link </a> There are thousands of Wordpress based website owners that have no idea that playing with cache or changing permalink can wipe clean their htaccess file. Obviously, the default htaccess file has no http to https redirect either 302 or 301. This reverts the web server to http unless you type https address directly. Wordpress plugins can solve the problem, but how many website owners use them? The strongest encryption keys or EV SSL Certificates .. all depends on a simple plaintext file.

[September 19, 2014 at 9:11AM](#)

 **Unknown said...**

Where I work we moved quickly to https, and while we have been able to deal with all kind of small fires, we're still having problems with the ads, since sometimes we serve adtags from other adservers that are not https, and therefore, ads don't show up.

If the market as a whole doesn't move forward together, there will be several problems among partners and 3rd party services.

If someone has an idea of a workaround for this, please share, if not, but in your way to move to https, be careful with that.

[September 19, 2014 at 6:36PM](#)

 **Unknown said...**

Does anyone know whether PayPal engagement helps in PageRank? In other words, rather than measuring how many customers buy item(s), do the search engines, especially Google, reward a site with a higher PageRank if customers engage with the site by buying through PayPal? Obviously engaging through using PayPal would mean the customer would spend that much more time on the site, but that alone would not help me as my average site view time is about 5 minutes, and the 30 seconds added just to use PayPal alone would not justify me having to pay the PayPal fee. So I need to know whether to justify the PayPal fee which I would only know if I knew if Google had a way of knowing and tracking whether customers actually used PayPal and how often and whether these PayPal engagements factored significantly in increasing my PageRank? I will be sure to get your response, and get it ASAP, if you could please follow the link at the end and leave it on my blog page. My site is in the business of saving lives, so you would really help me in that effort. Thank you! <http://www.curbnumbers.com>

[September 20, 2014 at 2:50AM](#)

[Post a Comment](#)



