8 Reasons

to Adopt Always-On SSL

We've made rapid gains in a relatively short span of time when it comes to securing our presence, activities and assets on the web with SSL. Serious criminal attacks on web assets, including high-profile data breaches at large corporations, the extensive reach of hackers in various parts of the globe and other online behaviour that threatens how we conduct business online are all catapulting us towards securing *everything* and doing so *all the time.* We're now entering the era of "secure by default" and there's never been a better time to adopt always-on SSL. Here are some of the top reasons why now is the right time to go secure:

1 **Google will enhance your SEO ranking:** Many websites live and die via their discovery in search engines. Organisations have historically resorted to all sorts of tricks to elevate their SEO, not all of which have fallen into what we would deem to be ethical behaviour either! But last year Google announced that they would begin using HTTP as a ranking signal, that is they'll actually improve a website's discoverability if they serve up traffic securely.

2 **Google is recommending that browsers warn when the connection is insecure:** Recently, the Chrome security team proposed that browsers should begin warning users when the connection is not secure. This is a fundamental shift from the current state where there is only an indication when the connection is secure, to overtly pointing out that a plain old HTTP connections simply can't be trusted.

8 Reasons to Adopt Always-On SSL

3 **Users are more at risk than ever as they become more mobile:** The majority of Internet traffic now originates from mobile devices. Users on the go are at significantly higher risk of connecting to malicious wireless networks when they're out and about. More than ever before, the assumption has to be that the users cannot trust the connection and that's the very problem that SSL sets out to address.

4 **SSL is now fast:** There was a long-held view that SSL came with a performance overhead; after all, it involves the negotiating of keys and implementing of encryption so there must be *some* overhead. But as browsers and web servers have evolved and SSL has matured, the CPU and latency costs are now negligible. Secure communications are also fast.

5 **It stops you leaking information via referrer headers:** On a website served over HTTP, navigating to an external site via a hyperlink will send the URL of the origin page with the request via the referrer header. However, when navigating away from a page served over HTTPS, the user agent must not send the referrer header. This further protects user privacy when they follow external links.

6 **You can now enforce it by baking HTTPS into the browser:** We've had HTTP strict transport security (HSTS) for a while now and it's finally present in the current generation of all major browsers. Not only does HSTS ensure a connection remains secure after it's initially loaded by the user, you can preload this rule into the browser before it's even shipped by the manufacturer thus ensuring a site can never be loaded over an insecure connection.

7 **Ad networks now comprehensively support SSL:** A long held argument against SSL was lack of support by ad networks. Serving a page securely, then embedding ads via an insecure connection resulted in browser warnings that made it infeasible for sites to go SSL only. Fortunately, ad networks such as AdSense now comprehensively support SSL and this argument is rapidly fading into the distance.

8 **SSL certificates are easier than ever to obtain:** As awareness grows and the popularity of SSL increases, it's getting easier and easier to obtain certificates and load them into modern web platforms. The web is finally moving to a "secure by default" transport layer and there's never been a better time to adopt always-on SSL through a trusted brand like GeoTrust.