Crucial For Your Site: HSTS (HTTP Strict Transport Security)

Hacking is out of control this year. However, a solution exists that can completely shut down several common hacks.

HSTS is becoming the most effective anti-hacking measure against man-in-the-middle attacks. HSTS, or "HTTP strict transport security, forces web browsers to communicate with your website using the secure connection of HTTPS—and only HTTPS. Users will not be able to visit your site over HTTP, which will effectively make your site safer.

What Exactly Does HSTS Do?

HSTS protects websites against two primary types of man-in-the-middle attacks:

- Protocol downgrade attacks
- Cookie hijacking

Protocol downgrade attacks occur when a hacker changes the mode of communication from an encrypted connection to an older, un-encrypted version. Because many sites offer backward compatibility to accommodate older systems, they become vulnerable to protocol downgrade attacks.

For example, say you have SSL/TLS enabled for your site. It is a known flaw of SSL/TLS that a downgrade attack could force the protocol down to a lower version, which would make it easy for a hacker to steal a user's information.

Cookie hijacking happens when a hacker steals a session cookie over an unsecured connection. HTTP cookies save information like names, addresses, and credit card numbers for users' convenience. However, these cookies can be stolen or predicted by hackers, who can then gain unauthorized access to valuable customer info.

What HSTS does is remove the option to communicate via HTTP, effectively preventing these kinds of man-in-the-middle attacks.

How Does It Protect A Website?

> HSTS prevents any non-https communication; forces HTTPS #topsecure #seo
>
> CLICK TO TWEET

When a browser first looks up a site with HSTS enabled, the HSTS feature tells the browser that it should never load the site using HTTP. It also tells the browser to automatically change any requests using HTTP to HTTPS instead.

To implement HSTS, you'll need to add an HTTP header named "Strict-Transport-Security" to your domain. In this header, you'll need to provide a "max-age," which tells the browser how long to remember the policy; the maximum of 31536000 seconds is recommended so it doesn't time out.

Users only have to visit your site once for their browsers to remember the settings. However, users will still be vulnerable on their first visit to your site. Every visit after that will be covered, but there is still a possibility for a compromise during that first visit.

HSTS offers a solution for that, too.

As per Google's checklist for HTTPS , they recommend using a web server that supports HSTS with a policy that does the following:

- Includes all subdomains
- Is preloaded onto browsers

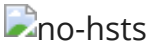
Including subdomains means that even if the user leaves off the "www" in the current domain, your site will still load using HTTPS. Many users visit sites without bothering to type the "www," which opens up the opportunity for getting hacked.

Preloading is also important, as it solves the "first visit" problem users face before they visit a site protected by HSTS. By preloading, HSTS is automatically enabled, even before a user's first visit.

At the end, your header should look like this:

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

Who Should Use It?



"Everyone" is the ideal answer here. Any website can benefit from additional safety measures, and HSTS is one that fixes a handful of very specific, very common attacks. HSTS is especially useful for eCommerce sites that save valuable customer information like credit cards and addresses. Basically, if you don't use HSTS, you're leaving your site wide open for hackers to take advantage of your visitors.

So far, HSTS is supported by Chrome, Firefox, Internet Explorer 11, Safari, and several other browsers.

More security means more approval from Google. Last year, Google stated they would begin crawling HTTPS pages over HTTP ones. This show of support from the biggest search engine in the world should make it pretty clear that you need to do everything you can to protect users. And now, that includes adding HSTS to your site.

How Do I Add The HSTS Header?

To add the HSTS policy to your site, you can either have your hosting site activate it (for a fee), or you can go into your server and enable it yourself. You may be comfortable doing this yourself, or you may want help to do it exactly right. Either way, adding HSTS to your site will be a tremendous benefit.

To preload your site for Chrome, you will also want to submit your domain. There are several requirements you must meet first, but once you do your site will have the added protection you need.

Remember—if you do not add the "preload" value, visitors may still be at risk before they first visit your site.

- Why Brands Should Rely on Influencer Marketing in 2018 and Beyond *by Shane Barker*
- Reading Your Audience: How to Incorporate Psychology into Social Media Marketing *by Rohan Ayyar*
- The Most Important Digital Usage Statistics Impacting Marketing Success in 2018 *by Liz Farquhar*
- How to Use Visual Storytelling to Improve Your Social Marketing *by Vikas Agrawal*

SUBMIT A POST

- About Us

There's always something more you can do to protect your website against hackers. With HSTS, you'll be able to stave off several of a hacker's most common, devastating attempts.

Hand-Picked Related Articles:

- How to Move Your Site to SSL
- How To Protect Your Website From Malware

* Adapted lead image: Public Domain, pixabay.com via getstencil.com

By Garry Grant | August 19th, 2016 | SEO, Web Design | Comments Off

About the Author: Garry Grant

Garry Grant is the CEO of Search Engine Optimization, Inc., a San Diego internet marketing agency. For over 20 years he has been improving rankings and integrating custom SEO services for businesses of all sizes.

SEO Inc

Related Posts

- Why Choose Us?
- The SEP Advantage
- Client Reviews and Testimonials
- Our Process
- Our Research
- PARTNERS
- In The News
- Contact Us

MENU

- OUR METHODS
- OUR TECHNOLOGY
- OUR WORK
- WHAT WE DO
- TESTIMONIALS
- ABOUT US
- CAREERS
- OTTAWA

THINKING DIGITAL BLOG

- How to Use Content Marketing Tools to Get More YouTube Views
- 10 Link Building Strategies To Avoid In 2018
- 7 Tactics to Skyrocket Your Conversion Rate in 2018
- Capitalizing on Marketing Knowledge: How to Monetize Your Expertise
- SEO Localization Roles and Support Systems

GIVE US A CALL

1-877-584-7304

NEWSLETTER SIGNUP

Email*

Your Email

SUBMIT

GET SOCIAL

Privacy Policy | Contact Us