BRAFTON
FUEL YOUR BRAND

Converting HTTP to HTTPS:

A CONTENT MARKETER'S GUIDE

> As if the world of content marketing needs more acronyms, we're now faced with the **real-world dilemma of HTTP and HTTPS.**

In 2014, Google announced its intent to make the internet more secure. To do so, it moved its Google domain-specific websites over to HTTPS with the goal of forcing other sites to do the same.

As of summer 2017, the **volume of encrypted traffic surpassed the volume of unencrypted traffic,** meaning we've reached a promising tipping point for global internet security. It also means that sites that do not currently utilize HTTPS gain the reputation of unreliability and lax customer privacy standards.

For marketers, converting from HTTP to HTTPS is a business decision that impacts every user (prospect) that comes to your site. So make the switch now.

TERMS TO KNOW

To navigate the conversion from HTTP to HTTPS, let's walk through the key terms to know:

- **HTTP (Hypertext Transfer Protocol)** - The foundation of online communication (how information is sent from a server to a browser).
- **HTTPS (Hypertext Transfer Protocol Secure)** - HTTP but within an encrypted layer of security.
- **Encryption** - Encoding information so it's only accessible by authorized parties.
- **SSL (Secure Sockets Layer)** - Technology protocol that creates encrypted communication links between servers and browsers.
- **SSL Certificate** - Data files that encrypt digital information and activate secure connections when installed on web servers.
- **DNS (Domain Name Servers)** - Directory of domain names that are translated to IP addresses.

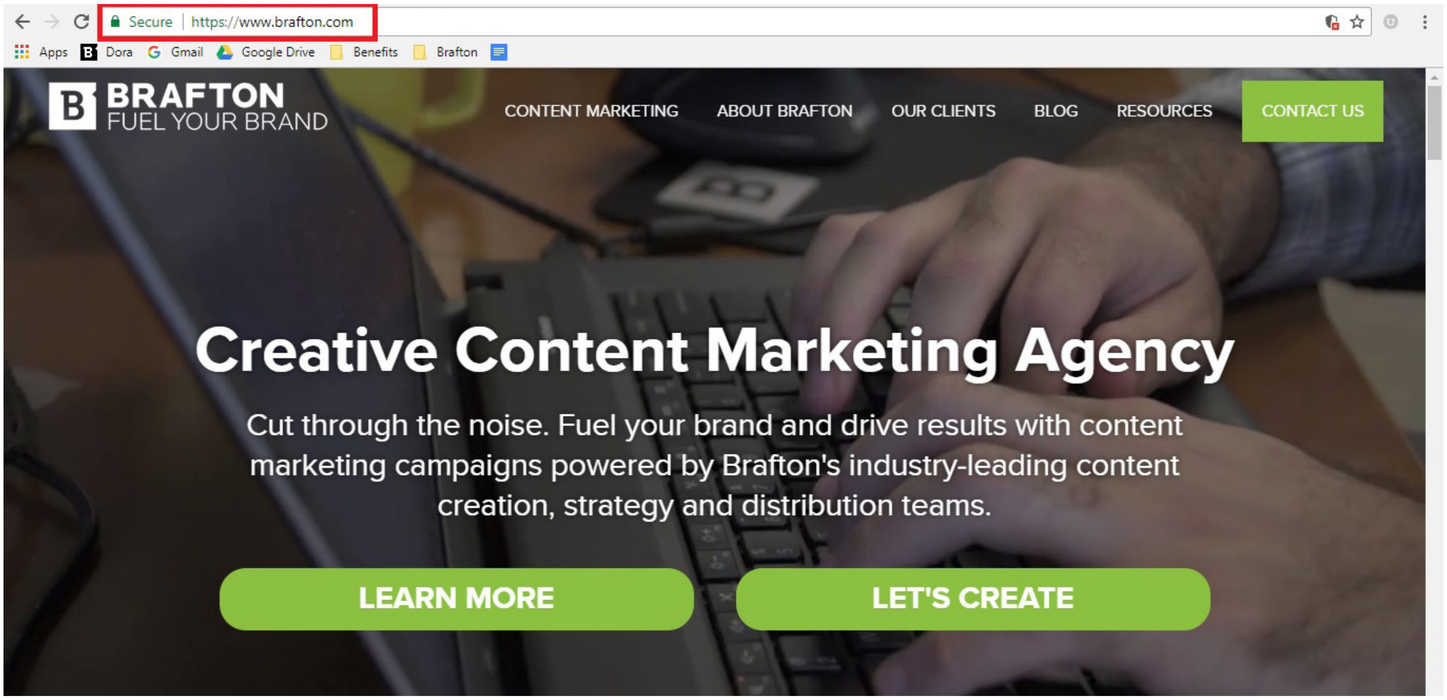
WHY THE CHANGE?

The three primary reasons Google has pioneered the push toward HTTPS are encryption, data integrity and authentication.

By making online information encrypted and authentic, sites contain a higher level of integrity. Google rewards sites with integrity, as they have proven to be more valuable to searchers and are more likely to serve relevant content that is free from errors or potentially suspicious activity.

Just as you wouldn't purchase items from shady online stores, you wouldn't hand over your personal information to websites that don't convert to HTTPS. And it's very clear to see who has made the switch and who hasn't.

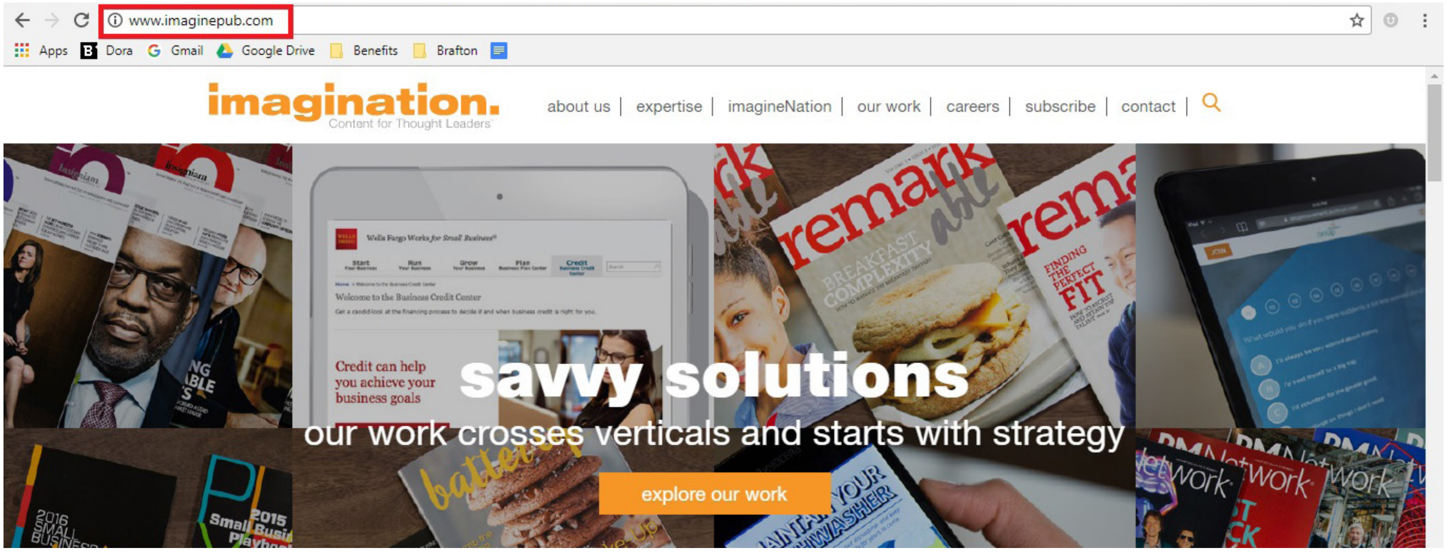
Google Chrome defaults to showing **"Secure"** and a **green padlock** as well as clearly labeling "https" before a URL. We know this site is good to go.



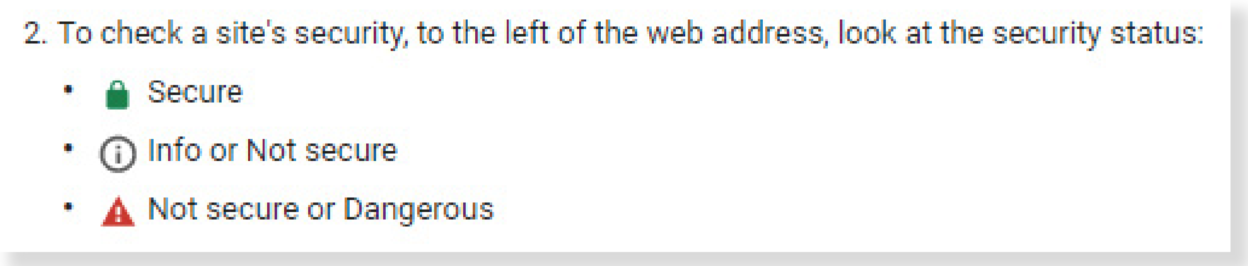
Creative Content Marketing Agency

Cut through the noise. Fuel your brand and drive results with content marketing campaigns powered by Brafton's industry-leading content creation, strategy and distribution teams.

On the other hand, we see the URL below does not contain these security features and instead has an “i,” which provides information on why this domain is not secure.


www.imaginepub.com
Apps
Dora
Gmail
Google Drive
Benefits
Brafton
imagination.
Content for Thought Leaders
about us | expertise | imagineNation | our work | careers | subscribe | contact |
savvy solutions
our work crosses verticals and starts with strategy
explore our work

For unsecure sites, Google sends you to this page for more support:



2. To check a site's security, to the left of the web address, look at the security status:

- 🔒 Secure
- ⓘ Info or Not secure
- ⚠ Not secure or Dangerous

For sites that have even greater security flaws, the red warning triangle appears in front of the URL.

Some cyberexperts have taken to calling these designations “security-shaming.” Google has in effect security-shamed sites to switch to HTTPS or else risk the Scarlet Letter of insecurity.

An unsecured HTTP site will likely be ranked lower than one that’s secured with HTTPS, all other factors withstanding, so SEO cannot really be discussed until after an HTTPS conversion. That’s because Google provides a rankings boost to HTTPS sites but only does so if it the content itself is relevant.

EASY 4-STEP PROCESS

Converting to HTTPS is simple.

1. BUY AN SSL CERTIFICATE

It's best to buy an SSL Certificate directly from your hosting company as they can ensure it is activated and installed correctly on your server.

2. INSTALL SSL CERTIFICATE ON YOUR WEB HOSTING ACCOUNT

Have your hosting company install the SSL Certificate. If you purchased from a third party, you'll have to import the certificate into the hosting environment, which can be quite tricky without support.

3.DOUBLE CHECK ALL WEB LINKS ARE SWITCHED TO HTTPS

Before going live with the conversion, ensure every website link has the proper HTTPS URL. Going live with links that mix HTTP and HTTPS will confuse readers, impact SEO and cause some page features to load improperly.

4.SET UP 301 REDIRECTS SO SEARCH ENGINES ARE NOTIFIED

Through a CMS plugin, you can automatically redirect all server traffic to the new secure HTTPS protocol. Sites that don't use a CMS will need to be updated manually. 301 redirects alert search engines that a change to your site has occurred and that they will need to index your site under the new protocol. Users who had previously bookmarked your site under the old unsecure protocol will now be routed to the proper secure URL.

In addition to providing server-to-browser security, activating and installing SSL certificates improves organic rankings, builds trust and and increases conversion rates.

TROUBLESHOOTING AND HOSTING CONCERNS

Though it may be an easy process for an experienced developer, the average marketer with little tech support can run into a few problems. Here are a few to know in advance:

1. SHARED HOSTING SOLUTIONS THAT MAKE CONVERSION DIFFICULT

GoDaddy, Bluehost, HostGator and other shared hosting models require a dedicated IP for SSLs. As such, if you're changing your IP in the process of converting to HTTPS, your DNS records may need to be updated accordingly and your hosting provider will need to be much more involved in the conversion process.

2. CONFUSION WITH CMS OR LACK THEREOF

Sites on CMS platforms like Wordpress or Joomla often have modules or plugins that can successfully convert protocols, though assets on the site that aren't uploaded to those platforms may still be directing traffic to unsecured connections. Further, sites that are custom built without a CMS will either need a third party to oversee the entire manual updating to secure protocols or will need to transition to a CMS with a plugin.

Each option is different, so marketers believing one company's experience with an HTTPS conversion will be the same as theirs will likely only get so far before needing assistance.

3. THIRD-PARTY RESOURCES ACCESSING INSECURE ASSETS

Some third-party resources not only host assets on secure URLs but also separately on other servers depending on location. Other third parties may still be attempting to access unsecured assets (those that weren't originally directed to HTTPS during the conversion process), thus creating a convoluted web of source traffic and routing.

UPDATING SEARCH CONSOLE A MUST

Marketers will need to ensure they submit a new sitemap from their secure URL to Google Search Console. Because Search Console views secured and unsecured sites as different properties, any protocol conversion is incomplete without your backend being able to properly track, store and measure data.

A new sitemap entry keeps your site analytics running smoothly.

HTTPS IS GREAT BRANDING

Today's branding is all about trust. Not just in your product or your company name but in your responsibility to customers' privacy and your technological capabilities.

An unsecured HTTP in front of your URL is essentially the same as still having an AOL email address or a Myspace account: It clearly shows site users that you're outdated, unserious about the future and grossly out of step with the latest security demands. You're practically begging cybercriminals to hack your site and steal customer data.

HTTPS is the exact opposite. It's the Tesla of security protocols, the verified blue check mark of domains. It means your site is authentic and has integrity – just as Google intended nearly four years ago.

These are great attributes to have attached to your brand.

So don't think of HTTPS as another tech update – **it's a full-scale business refresh.**

BRAFTON
FUEL YOUR BRAND

WWW.BRAFTON.COM

webmasters.googleblog.com/2014/08/https-as-ranking-signal.html | moz.com/blog/https-tops-30-how-google-is-winning-the-long-war