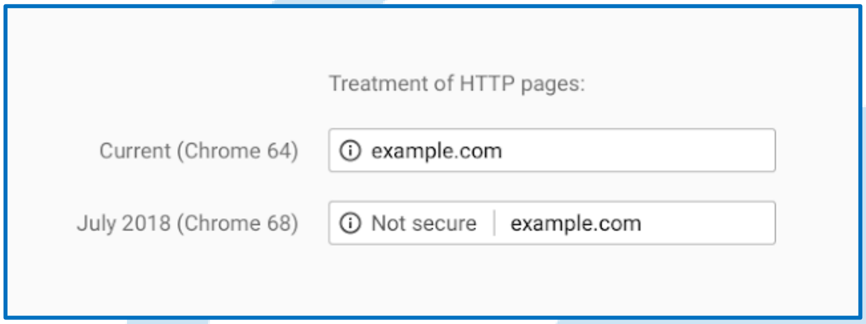
BAYSHORE SOLUTIONS
Digital Expertise to Grow Your Business

GOOGLE CHROME UPDATE – SECURE VS. UNSECURE WEBSITES
JULY 2018

What’s Happening?

- In July 2018, Google will release version 68 of their Chrome web browser. This is important since 60% of all web traffic comes from Google Chrome.
- This new version will begin showing a grey “Not secure” tag next to the website address in the address bar on all websites that do not have HTTPS.



Treatment of HTTP pages:

Current (Chrome 64) ⓘ example.com

July 2018 (Chrome 68) ⓘ Not secure | example.com

What is HTTPS?

- HTTPS is a way to encrypt the data that your visitors send between their browser and a web server. It protects personally identifiable data like names, emails, phone numbers, logins, and credit card data.
- The SSL certificate used by HTTPS identifies you as a trusted and verified website owner.
- Over 50% of web traffic is now encrypted on both computers and mobile devices, a jump of over 10% from a year ago. Thanks to improvements in modern server and browser software over the years, the performance impact of HTTPS encryption is negligible at best.

Benefits of HTTPS:

Security

- HTTPS adds security and trust. It keeps the contents of your web traffic private.
- One of the major benefits of HTTPS is that it protects users’ internet data from being compromised over public WiFi networks.
- Some ISPs inject ads into users’ unencrypted web traffic. HTTPS can prevent this.
- Hackers can use unencrypted website connections to inject phishing attacks, redirecting users to nefarious sites.
- Authentication insures that your users communicate with the intended website.

Search Engine Optimization (SEO)

- Google started to factor in HTTPS as part of the overall search ranking for a website back in 2014, meaning HTTPS sites get an advantage in search results over the older HTTP sites.
- HTTPS preserves referrer data. Referral information from non-secure HTTP sites is ignored by analytics tracking tools.

Brand Trust

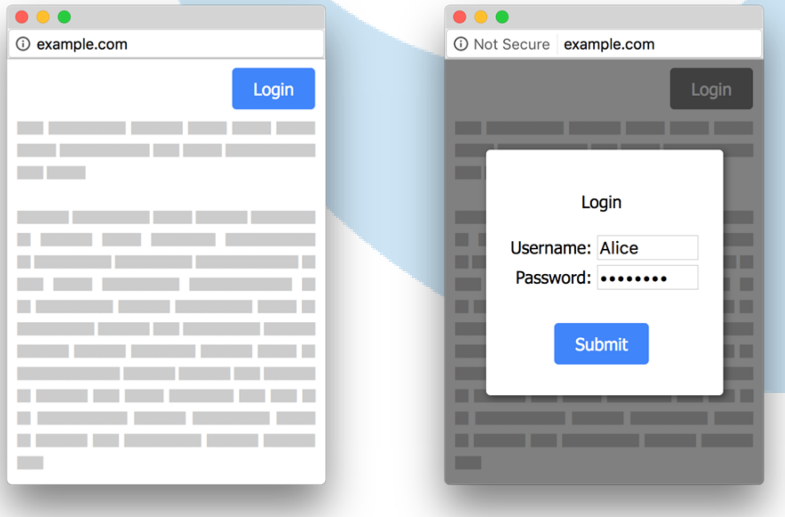
- HTTPS and the familiar padlock icon, along with the new “Secure” tag next to your website address in the address bar, builds trust with your website visitors.
- Increased customer confidence means increased conversions.

HTTP to HTTPS Migration Process with Bayshore Solutions

- A required SSL certificate will be added to your website. This facilitates the encrypted connection and establishes website owner trust.
- Your website will be configured to automatically redirect all traffic to use HTTPS.
- A website audit will be performed to find any hard-coded HTTP links and provide a report identifying any necessary updates to the content.
- We will insure 301 redirects are in place and submit a new sitemap to Google and Bing.
- A 30-day search engine ranking monitoring is included.

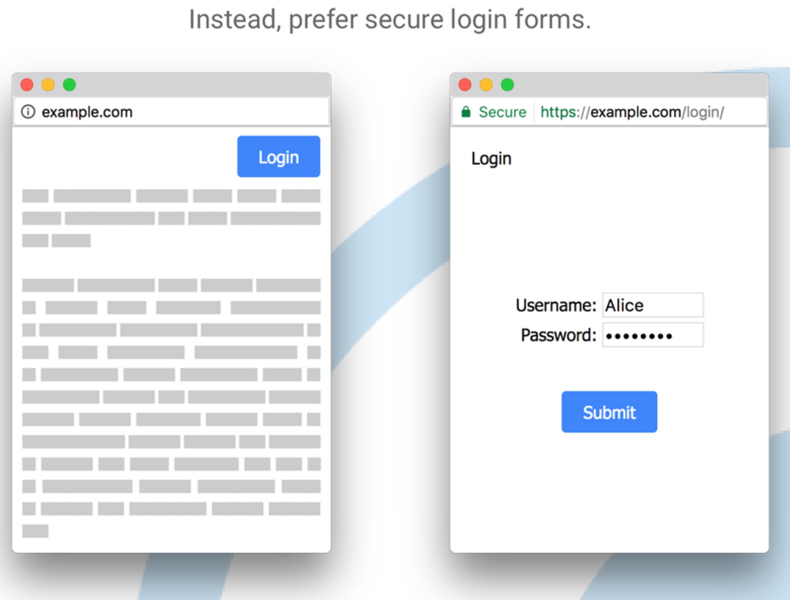
Examples

Non-secure login forms in Chrome will display the “Not Secure” warning [developers.google.com]


Non-secure login forms trigger the new **Not Secure** UI treatment.

Username: Alice
Password: ••••••••

Secure login forms in Chrome will display the “Secure” confirmation [developers.google.com]



Instead, prefer secure login forms.

FAQs

1. How can I tell if my site is secure?
    a. Using Google Chrome, input your domain into the address bar and if there is a green secure tag to the left of the address, or if there is a padlock, you are secure. If nothing appears, you are not running HTTPS and thus, not secure.
2. What makes my site not secure?
    a. Not having the SSL certificate, which means data is not being encrypted when users are on your website.
3. What makes a site secure?
    a. An SSL certificate allows a website to run under HTTPS. HTTPS is what encrypts all your users’ traffic between the browser and the server. It protects their data when they are using public wifi networks or mobile networks.

To learn more about how Bayshore Solutions can help your website become secure, call us at 866-352-4791, email us at info@bayshoresolutions.com or contact your project manager today.