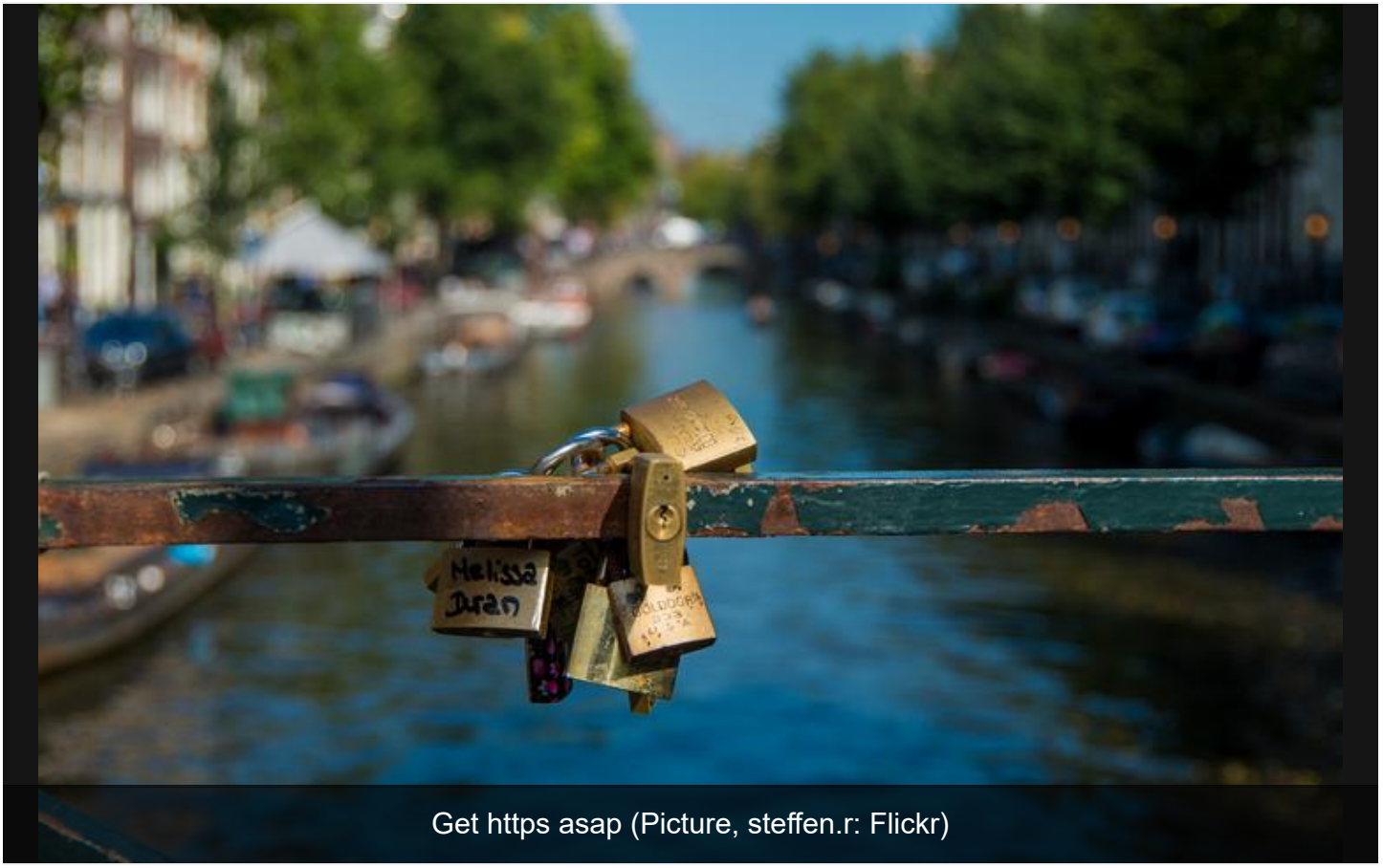
Why you need https on your website right now

How Google's new algorithms will affect your business.

George W. Helon (PC World) on 20 January, 2017 09:36



Get https asap (Picture, steffen.r: Flickr)

You might have noticed when browsing the internet lately that strange icons are appearing to the left of the URL in your browser address bar: a grey circle surrounding the letter i; a green padlock; a green padlock followed by the word Secure; a white exclamation mark within a red triangle, or a white exclamation mark within a red triangle followed by the words Not secure?

And if you can't access a website, sign-in to a subscription, are unable to complete an online transaction, or you are seeing error or warning messages popping-up on your computer screen, chances are it is not because of any data drop out or fault with your digital device.

In September last year Google announced that beginning in January 2017 it would mark "all HTTP pages that collect passwords or credit cards as non-secure"; this

effectively means that nearly every website on the internet is now labelled as NOT SECURE or DANGEROUS until website owners can prove otherwise.

In an attempt to clean-up the internet - and as part of its Safe Browsing technology rollout - Google is using advanced algorithms and robots to scan the web for 'unsecure' sites that host deceptive pages with ads that target people with unwanted software, those that contain harmful downloads or malicious content, and those that contain malware or phishing content.

Although Google's official intent is to alert users to websites that it deems unsecure, unsafe and vulnerable to data compromising, its real motivation might be more questionable.

According to Google, "Chrome currently indicates HTTP connections with a neutral indicator. This doesn't reflect the true lack of security for HTTP connections. When you load a website over HTTP, someone else on the network can look at or modify the site before it gets to you. Eventually, we plan to label all HTTP pages as non-secure, and change the HTTP security indicator to the red triangle that we use for broken HTTPS."

Branding a website with an unsecure label is sure to dissuade many potential customers and clients from trading online with a business, company, corporate, government, or other entity; with existing customers and subscribers being left frustrated and confused!

Many of those business owners who aren't aware of Google's new algorithms will soon find that they are suffering from a significant decline in online business and a real reduction in sales turnover because their websites are either blocked, or not showing-up in Google search results.

"To help you stay… safe on the web, Chrome (now) requires websites to use certificates from trusted organizations" and Google now requires that all websites be authenticated for the protection, privacy and integrity of sensitive data transmitted and exchanged over the internet.

READ MORE

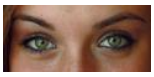
Social Media-based investing in 2017

To protect against third-party eavesdropping, data interception, tampering, and the forging of the contents of any communication, between a client and service provider, all data must encrypted.

Encryption is via HyperText Transfer Protocol (HTTP) Transport Layer Security, or HTTP Secure (HTTPS); previously known as Secure Sockets Layer (SSL) which is the global standard in security technology for establishing an encrypted link between a client, web server and a browser – vice versa.

HTTPS connections were previously utilised only by government authorities and corporate bodies for the transacting of private and confidential financial dealings and the transmission of sensitive data over secure networks.

“Data sent using HTTPS is secured via Transport Layer Security protocol (TLS), which provides three key layers of protection: encryption, data integrity, and authentication.”



READ MORE

A changing climate creates opportunities for IT

If you own an ecommerce website, or transact business via the internet, you will need to pay a third-party Certificate Authority (CA) for the issuance of a SSL Certificate.

Without an SSL Certificate and the https URL prefix, customers will have no confidence to transact business with you.

It is the job of the Certificate Authority (CA) to verify your domain name, your legal identity, that your entity owns it, and that your associated credentials are validated.

Depending on your requirements, SSL Certificates can cost from a few hundred dollars, right up to thousands of dollars.

READ MORE

Virtual and Augmented Reality – reshaping business futures

Although you might be tempted to engage the services of a free Certificate Authority, be warned, because the Certificates that they offer don’t have the same layers of security as some of the larger, more known and trusted big names, some browsers will not recognise your site’s Certificate Authority.

Google recommends that you check a site's security before transmitting any data or sensitive information online; this can be done by looking at its security status which is indicated to the left of the URL (Uniform Resource Locator) in the address bar: a grey circle surrounding the letter i, the website isn't using a private connection - someone might be able to see the information that you are sending; a green padlock, the website is secure - the information you send to the site will be

private; a green padlock with the word Secure, the website is fully secure – the information exchanged is fully encrypted; a white exclamation mark in a red triangle indicates that the website is either not secure or dangerous – the site is NOT SECURE and DANGEROUS, proceed with caution, or better still avoid the website altogether.

To see further information about a website's security status, left click on the visible security icon to the left of the URL in the browser address bar.

George W. Helon is founder and CEO of MedicReady