

Technology

By Welton Hong



Website Security

Secure Your Website Now to Avoid a Massive Visitor Exodus

Picture this for a moment: You're an average person searching for a funeral home. You find one and click the link.

In the address window, you see this message from Google:

NOT SECURE

What are the chances you'll be sticking around that site for more than a few seconds? If you're like most people, you'll immediately "bounce" – the industry term for leaving a site or page instead of exploring further.

That's really bad news, and it's exactly what funeral home websites are facing if they're still not using HTTPS technology. And if you're not sure what HTTPS means, don't worry: I'll explain in a moment.

First, to help you understand how critical this is, let's look at how many of your website visitors could

be affected by this serious change by Google.

This change will only immediately affect Google Chrome browsers, although browsers such as Internet Explorer, Firefox, Edge and Safari are likely to follow suit in time.

Chrome is by far the most popular web browser in America, used by more than 60 percent of searchers. The next two highest-ranking browsers, Internet Explorer and Firefox, have less than 25 percent of the market share *combined*. Edge and Safari each own less than 5 percent of the market share.

Let's create an arbitrary round number for the number of unique visitors to your website in a month: 1,000. On average, about 600 of those visitors will be using Chrome. Come July, if you're not using HTTPS, all 600 visitors will see that "Not secure" admonition from Google.

Let's be conservative and say that will only scare off 50 percent of visitors. (It probably will be more, because who wants to stick around on a site that's not secure? But again, we're being conservative.)

That means you just lost at least *30 percent of your unique visitors* in a flash. In the digital age, with more people searching for burial and cremation services every day, that kind of drop-off can sink a death-care business.

What is HTTPS, anyway?

I'm sure some readers already are familiar with this term, but it's fine if you're not. Essentially, HTTPS indicates that all communications between your browser and a particular website are encrypted, and thus much safer from hackers and other malicious actors. In addition to encryption, HTTPS provides protections for authentication and data integrity.

Technically, HTTPS stands for Hyper Text Transfer Protocol Secure, which just means it's the secure version of the HTTP protocol. HTTPS pages are typically encrypted either with the SSL (secure sockets layers) or the TLS (transport layer security) protocol.

And no, you don't need to remember all of those technical details. You just need to know that your website needs to be HTTPS, not HTTP. It should be HTTPS already, but if it's not, it must be, starting now.

How do you know if your website is already using HTTPS? It couldn't be easier.



Simply open your website in Chrome and look in the address bar. If it's HTTPS, you'll see "https://" at the start of the address. You'll also see a padlock icon with the word "Secure" on the left edge.

If it's not HTTPS, you'll likely see nothing except the main domain name (e.g., "thisisafakedomain-name.com"), possibly preceded by "www."

Even prior to the recent change, if your site wasn't HTTPS, users saw a warning sign from Google. There

was a small information button (a lowercase "i" in a circle) on the left side. Clicking on that, visitors received a message that read:

"Your connection to this site is not secure. You should not enter any information on this site (for example, passwords or credit cards), because it could be stolen by hackers."

Does that sound like something you want to convey to potential customers? Me neither.

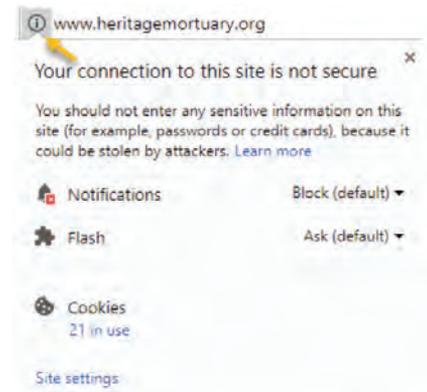
My website isn't HTTPS – what do I do?

If you've had your website for a long time and haven't done any redevelopment for a while, you might be in this camp. Just searching local funeral homes across America for five minutes, I found more than a dozen that do not run HTTPS, so it's a big concern.

Again, running HTTP means that visitors using Chrome who previously saw a warning will now see a more explicit warning.

While it's true that converting from HTTP to HTTPS is inexpensive and really not very complicated, it is complex enough that it's best handled by a seasoned IT professional.

A major mistake in the transition process could impede your website's functionality or even render it useless. Even if there's no harm to the



functionality, a subpar transfer could hurt your site's search engine optimization (SEO) and/or user experience. So it needs to be done right.

If you're not sufficiently worried about the "Not secure" message that will now display to your visitors, rest assured, Google will keep on making that warning more explicit until all sites are compelled to upgrade.

Google wants to protect online users, and it considers HTTPS a foundational aspect of doing just that. In fact, it typically ranks HTTPS sites better than HTTP sites in organic search – another great reason to make the change.

At the end of the day, if Google wants every site to be HTTPS – and it certainly does – that's going to happen. So now is the time to make the transition. Don't wait until it's too late. •

THE FUNERAL PROFESSION IS EVER CHANGING.
Now more than ever, you need to adapt to keep up. Are you looking for change that will help your funeral home run smarter not harder?

- **FAST FUNDING**® – most claims paid in 1 to 2 days with paperwork
- **NO RISK** – Non-Recourse Funding to your firm
- **SIMPLE & EASY** – many assignments only require 1 signed document
- **Revolutionary Online Assignment Funding Management System™**

Stop Waiting
WEEKS
Or Even
MONTHS
to receive payment on your
INSURANCE CLAIMS

CHOOSE
C&J FINANCIAL
and get paid today!

C&J Financial, LLC
The Leader in Insurance Assignment Funding™

www.CJF.com | 800.785.0003