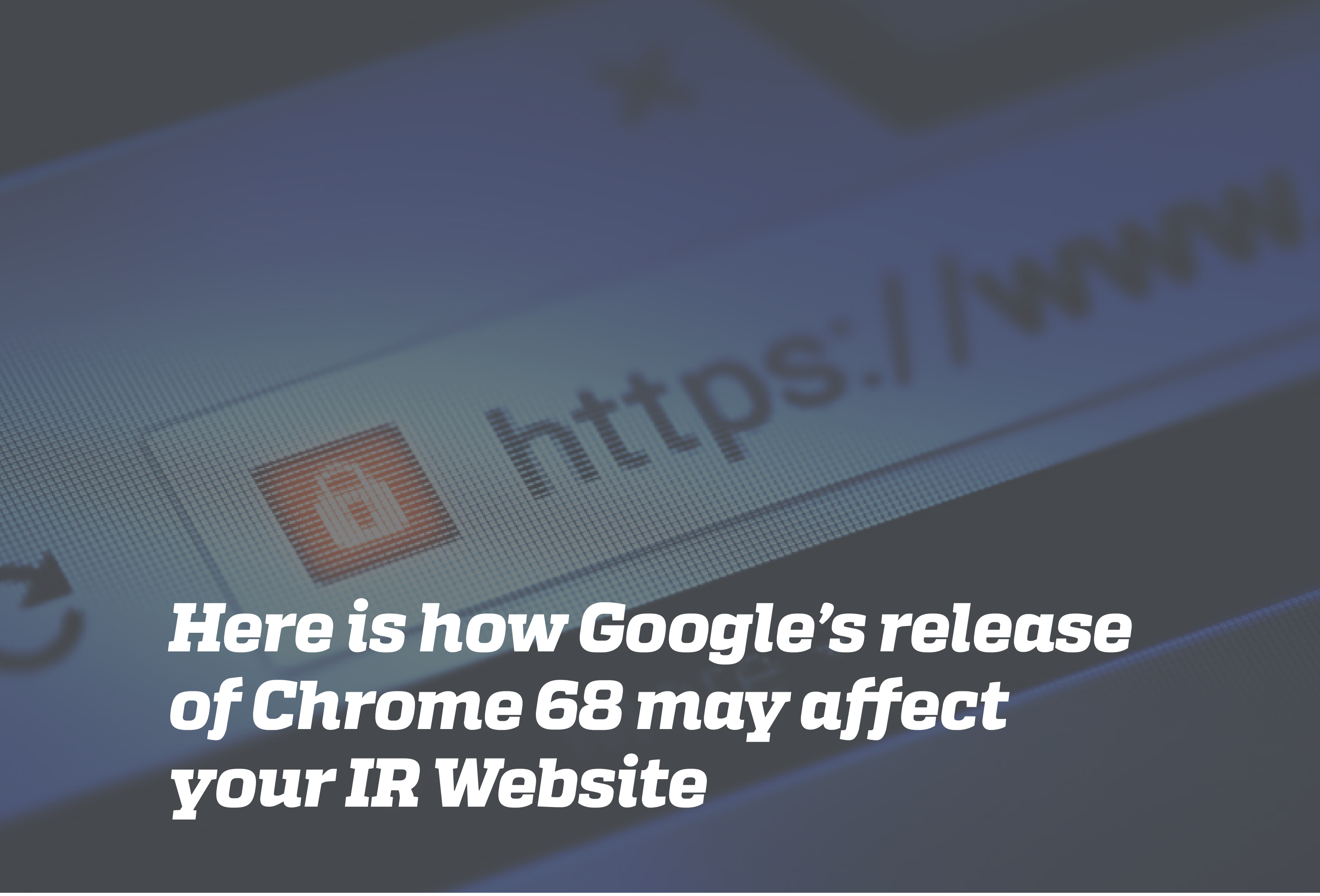
Will a "Not Secure" Warning Show Up On Your IR Website in July 2018?

HTTPS IR Website Whitepaper

Tom Runzo, Equisolve

EQUISOLVE



Here is how Google's release of Chrome 68 may affect your IR Website

This July (in less than 60 days) Google will release version 68 of the Chrome browser, which will affect every website in the world. This release will require websites to be secure, using HTTPS, which encrypts data in transit between the website and servers. Beginning this July, any website that uses HTTP, and not HTTPS, Chrome will display a "Not Secure" warning.

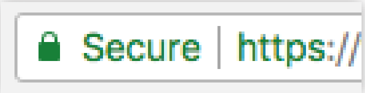
IR Websites are behind in the transition to HTTPS, with only about 25% of them being HTTPS, while about 70% of all other websites are HTTPS. Additionally, around 90% of all IR Websites are outsourced to a handful of companies. This may create a backlog in the upgrade process as the deadline nears and other companies start to recognize the need to upgrade to HTTPS right away.

Not sure if you should upgrade now? Ask yourself one simple question: How will investors react when Google labels your IR Website as "Not Secure?"

What is HTTPS?

HTTPS first made an appearance back in 1995 and has been widely used by e-commerce websites and financial institutions since the early 2000s. HTTPS, also known as SSL or TLS, protects the data exchanged between your web browser and the website you're viewing by using encryption. This prevents eavesdropping on your browsing and any private information you provide to a website, while also ensuring that the site you're browsing is really the site you intend to browse, and not a malicious hacker attempting to steal your data.

You will likely recognize this green "secure" designation:



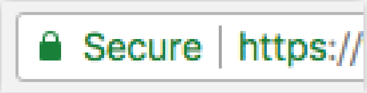
Secure | https://

Fast forward more than 2 decades. In January 2017, Google announced that through a series of updates to its Chrome browsers, it will require all websites to be HTTPS, or it will soon mark them as "Not Secure."

In October of 2017, as a soft launch, it released Chrome 62 which started to display the "Not Secure" warning on sites that are not HTTPS, but only if there was a password field on the page or if a visitor typed into a form field of any kind. At the end of January 2018, Google announced that in July 2018, it will release Chrome 68, which will require every web page on every website worldwide to be HTTPS or it will mark it as "Not Secure."

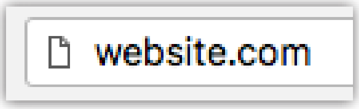
How can I tell if my IR Website will be affected?

Directly below are visual examples of the difference between Secure (HTTPS) & Not Secure (HTTP)



Secure | https://

Secure

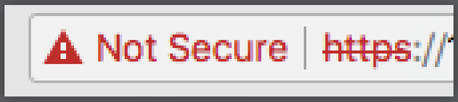


website.com

Not Secure

What will the changes look like in July 2018?

The image below shows what Chrome will display if you don't upgrade to HTTPS:



⚠ Not Secure | ~~https~~://

Imagine the reaction when investors and analysts see Google label your IR Website with a "Not Secure" warning.

Chrome is only one browser. Why should I care?

Google Chrome is used by over 57% of all internet users. When Google announces a major update that requires all websites worldwide to be HTTPS or it will mark it as "Not Secure," you better get on board because the clock is ticking.

Over 90% of all Chrome users get their browser update automatically as new versions are released, so when Chome 68 is released in July it will affect everyone within days.

IR Websites don't store credit card data or HIPPA information so why does HTTPS matter?

In addition to the negative perception of a security problem when Google labels your website as "Not Secure," HTTPS will help protect against malware, code injections and spying from Wi-Fi networks which can make the following vulnerable:

1. Shareholders/investors data
2. Material, non-public information hosted in your CMS or on your computer/network
3. Your computer and those on your network

How do you get your IR Website to be HTTPS?

For companies who outsource their IR Website, it is as simple as contacting your vendor and asking them to upgrade your IR Website to HTTPS. They may try to charge you, but don't let them. They have had a full year notice and should have done it before Chrome started warning users about non-secure forms in October 2017.

For those of you who manage your IR Website in-house, you will need to obtain an SSL certificate from a Certificate Authority and take the following steps to ensure not only that your website is SSL, but that you don't ruin years' worth of hard work on your website. Here are several things to complete and consider once you have your SSL certificate:

- Perform a complete backup of your website
- Update all internal links to HTTPS
- Check your code libraries to ensure HTTPS URLs are used
- Create 301 redirects
- Test every page on your site for SSL warnings and errors
- Update your Google Search Console
- Update paid search links
- Update directory listings
- Update all your social media links and share functionalities

Conclusion

HTTPS is the standard used by companies around the world to secure their websites and protect the privacy and security of customer data. Soon it will be a requirement unless you want a "Not Secure" warning on your site.

So whether you run your own IR Website or use a third party to host your IR Website, you have until July to upgrade to HTTPS. Additionally, if your IR Website has an email alert sign-up form, you need HTTPS to protect your visitors' contact information to comply with the new **GDPR** regulation. Look for our GDPR IR Website whitepaper coming soon.

EQUISOLVE

Tom Runzo, CEO
2455 E. Sunrise Blvd., Suite 1201
Fort Lauderdale, FL 33304
954-858-8550
tom@equisolve.com
equisolve.com