







GOOGLE CHROME MARCARÁ LOS SITIOS WEB HTTP QUE NO SEAN SEGUROS

Los esfuerzos de Google por hacer de su navegador Chrome una herramienta más segura para los usuarios son cada vez mayores. Desde mejoras para detectar páginas de estafadores, [hasta eliminar los saltos al navegar en un sitio web](#). Asimismo, desde hace algunos años la compañía ha venido impulsando la transición de la web a https. Con la versión 56, Chrome comenzó a marcar los sitios http como 'Not Secure' en la barra de direcciones. Ahora, con la versión 62, la insignia 'Not secure' está programada para aparecer en más páginas HTTP.

De acuerdo con [9to5Google](#), el navegador mostrará la advertencia de seguridad si detecta formularios en la página que soliciten contraseñas, tarjetas de crédito o cualquier campo de entrada de texto que Chrome considere que necesita protección https. Dicha advertencia también se activará en todas las páginas http en modo incógnito.

	Treatment of HTTP pages outside Incognito mode:	Treatment of HTTP pages in Chrome Incognito mode:
Current (Chrome 58)	 example.com	 example.com
Oct. 2017 (Chrome 62) at page load	 example.com	 Not secure example.com
Oct. 2017 (Chrome 62) when entering data	 Not secure example.com	 Not secure example.com

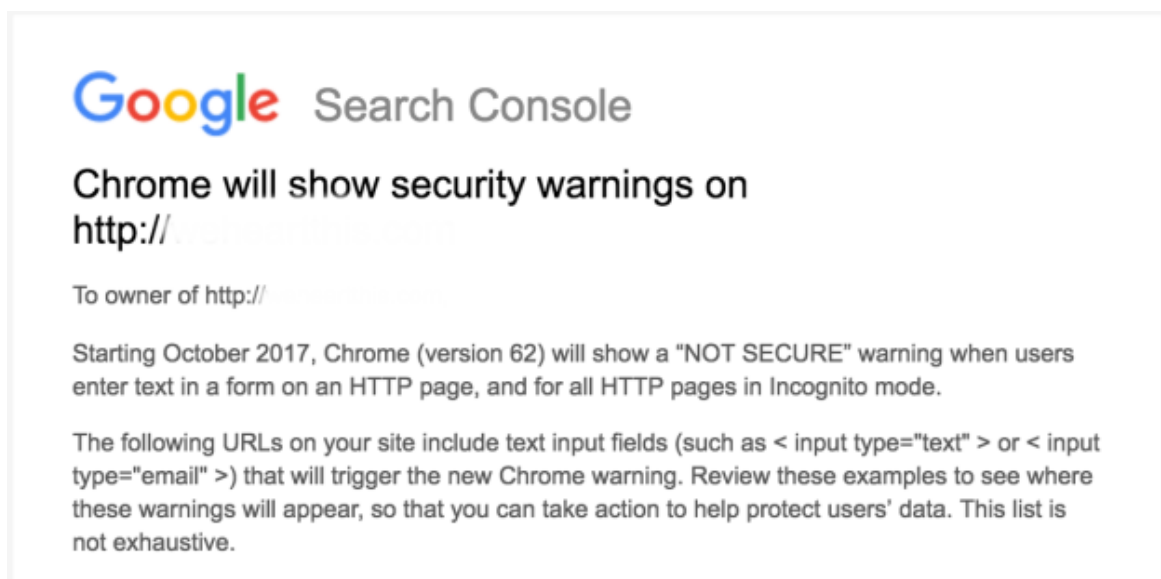
Así ha sido la transición de Chrome al marcar los sitios con conexión http como 'Not Secure' en cada actualización.

“Las contraseñas y las tarjetas de crédito no son los únicos tipos de datos que deben ser privados. Cualquier tipo de datos que los usuarios escriban en sitios web no

Lunes, 2 de octubre de 2017.

deberían ser accesibles a otros en la red. Por esta razón, a partir de la versión 62 Chrome mostrará la advertencia ‘Not Secure’ cuando los usuarios escriben datos en sitios HTTP”, explicó Google en su [blog oficial](#).

El objetivo final de Google con esta actualización es fomentar la adopción de páginas más seguras. La compañía señala que la transición a https es más fácil y más barata que nunca, al tiempo que permite una mayor funcionalidad.



Un reto para las empresas

Por otra parte, esto impone un importante reto para todas las empresas que tengan presencia en Internet. De acuerdo con Certicámara S.A, estas deberán implementar Certificados de Servidor Seguro, SSL, en sus portales, para evitar suplantaciones de portales y sitios web. Estos esfuerzos ya se están viendo pues, según Dean Coclin, directivo de Symantec, las entidades gubernamentales en todo el mundo están migrando a conexiones HTTPS en todos sus portales, lo cual garantiza que el acceso a los dominios .gov solo se permitirá por conexiones cifradas y si la página cuenta con la conexión segura.

Imagen: Google, [Pixabay](#).