







Google se sert une nouvelle fois de Chrome pour pousser le HTTPS

D'ores et déjà, Google Chrome considère les sites HTTP demandant des mots de passe ou des informations de paiement (comme des numéros de carte bancaire) comme non sécurisés. Une logique apparue avec Chrome 56 que Google s'apprête à étendre avec la sortie de la version 62 du navigateur le plus utilisé dans le monde, une sortie attendue pour octobre prochain.

	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

Dans un [billet de blog](#), Emily Schechter, de l'équipe de sécurité de Chrome, explique que les pages HTTP demandant des informations personnelles à l'internaute et les sites HTTP visités alors que le navigateur est configuré en navigation privée seront à leur tour marqués comme non sécurisés. « *Les mots de passe et les cartes de crédit ne sont pas les seuls types de données qui devraient être privés, écrit Emily Schechter. Tout type de données que les utilisateurs saisissent sur les sites Web ne devrait pas être accessible à d'autres sur le réseau.* »

« N'attendez pas pour migrer vers HTTPS »

Avec cette décision, et du fait de son poids sur le marché des navigateurs, Google espère pousser un peu plus l'adoption du HTTPS par les éditeurs de sites. Selon la firme, depuis les premières mesures adoptées dans Chrome 56, on a assisté, sur desktop, à une baisse de 23 % des pages HTTP demandant un mot de passe ou un numéro de carte de crédit.

Et Google envisage déjà d'aller plus loin. Dans son billet de blog, Mountain View évoque la possibilité de généraliser l'avertissement sur toutes les pages HTTP, y compris en dehors de la navigation privée. Sans toutefois indiquer une échéance pour cette nouvelle étape. « *Nous publierons de nouvelles informations à mesure qu'approchera la sortie des futures versions, mais n'attendez pas pour entamer la migration vers HTTPS* », lance Emily Schechter aux webmasters.

HTTPS : déjà plus d'une page sur deux

Début février, pour la première fois, le HTTPS a dépassé le seuil des 50 % des pages Web chargées sur deux semaines consécutives, selon les données de télémétrie de Mozilla. Une tendance qui s'est confirmée depuis (on est désormais au-dessus de 54 %). Le protocole Hypertext Transfer Protocol Secure (HTTPS) fournit une authentification des sites et serveurs Web associés. Le chiffrement bidirectionnel des données du navigateur réduit aussi considérablement la menace d'une attaque de type Man-in-the-middle.

Poussée par les révélations de Snowden sur la surveillance généralisée mise en place par la NSA, l'adoption du HTTPS doit beaucoup aux éditeurs de navigateur, qui multiplient les messages d'alerte pour les utilisateurs, à des sociétés comme Let's Encrypt, qui fournit gratuitement les certificats, ou encore Google, qui a annoncé qu'il allait favoriser le ranking des sites HTTPS sur son moteur de recherche.

A lire aussi :

[Le phishing aussi migre vers le HTTPS, grâce à Let's Encrypt](#)

[Pour pousser le HTTPS, Google devient une autorité de certification racine](#)

[50 % du trafic Web est protégé par HTTPS](#)

Crédit Photo : Pavel Ignatov – Shutterstock