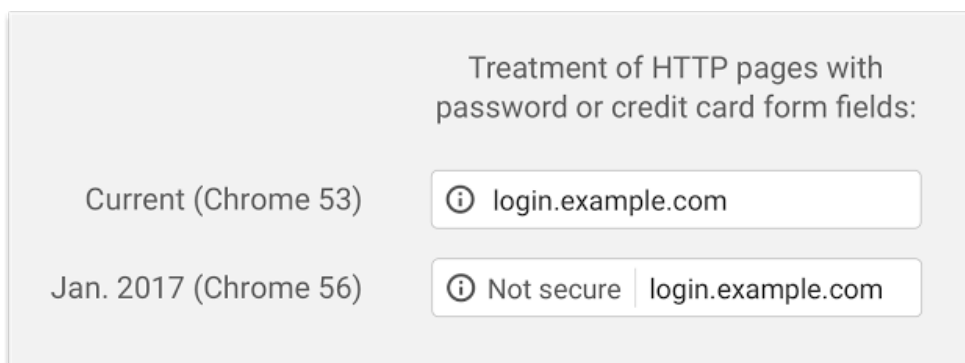


# Google Chrome poursuit sa croisade contre le Web non sécurisé

En début d'année, Google partait en croisade contre la navigation non sécurisée. Mountain View proposait d'introduire dans son navigateur Chrome des notifications visant à alerter l'utilisateur lorsqu'il se rendait sur un site qui ne chiffre pas les communications. Cela afin de faire prendre conscience que les données échangées pouvaient y être récupérées ou détournées. Depuis, une croix rouge devrait apparaître au niveau de la barre d'adresse d'ici la fin de l'année pour alerter des risques potentiels à poursuivre la navigation. Pour l'heure, nous ne constatons pas la présence de cette croix de signalisation sur les sites qui n'adoptent pas le protocole HTTPS, à commencer par celui que vous avez sous les yeux.

Google vient de renforcer cette politique. A partir de Chrome 56, attendu en janvier 2017, la version desktop du navigateur maison marquera explicitement comme non sécurisés les sites restés en HTTP sur lesquels s'échangent mots de passe ou numéros de carte bancaire. La mention « Non sécurisé » (*Not secure*) apparaîtra devant l'adresse du site dans la barre d'adresse du premier navigateur du marché (voir image ci-dessous).



## Les utilisateurs insensibles à l'absence de sécurité

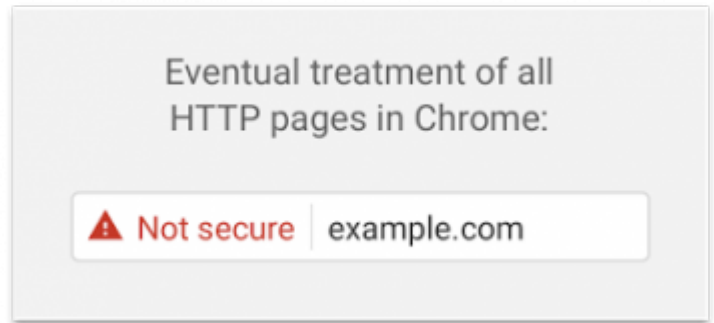
« Chrome indique actuellement les connexions HTTP avec un indicateur neutre (le « i » de information s'affichant dans le cercle en entête de l'URL, NDLR). Cela ne reflète pas le véritable manque de sécurité des connexions HTTP, [explique](#) Emily Schechter, membre de l'équipe de sécurité de Chrome. Lorsque vous chargez un site Web en HTTP, quelqu'un d'autre sur le réseau peut regarder ou modifier le site avant qu'il arrive à vous. » Selon des études pointées par Google, non seulement les utilisateurs ne s'alarment pas de l'absence d'icône de sécurité, mais ils deviennent aussi indifférents aux alertes trop fréquentes. D'où la volonté de l'éditeur de faire ressortir visuellement le danger potentiel aux yeux de l'utilisateur.

Et plus que se contenter d'alerter les internautes, la firme californienne espère pousser les éditeurs de sites à adopter les technologies de chiffrement de leurs pages. Une stratégie qui porte ses fruits. « Depuis que nous avons publié [notre rapport HTTPS](#) en février dernier, 12 nouveaux sites des 100 meilleurs sites Web ont basculé de HTTP vers HTTPS », assure la responsable. Qui assure que, désormais, plus de

la moitié des pages affichées dans Chrome le sont de manière chiffrée.

## Firefox et Edge en renfort contre le HTTP

Une tendance encourageant qui pousse Google à poursuivre sa politique d'avertissement. Dans un premier temps en pointant les pages non HTTPS lorsque l'utilisateur surfera en mode de navigation privé. Une mesure que l'entreprise pourrait ensuite généraliser à toutes les pages HTTP de manière plus voyante (voir image ci-contre). Les



utilisateurs fuiront-ils pour autant les sites non sécurisés? A voir. Toujours est-il que les éditeurs ont de moins en moins d'excuse pour ne pas adopter le chiffrement de leurs sites. « *Le HTTPS est plus facile et moins cher que jamais, et permet à la fois d'offrir de meilleures performances Web et de nouvelles fonctionnalités puissantes trop sensibles avec le HTTP* », soutient Emily Schechter.

Si Google part en croisade contre les sites non sécurisés, Chrome n'est pas le seul navigateur à privilégier les sites en HTTPS. Mozilla a de son côté commencé à [réserver les nouvelles fonctionnalités avancées de Firefox aux seules pages chiffrées](#). Et [Microsoft a adopté le HTTP Strict Transport Security \(HSTS\) pour Edge](#), le navigateur fourni avec Windows 10. De quoi réduire les chances de survie du web non sécurisé.

---

### Lire également

[Les certificats SSL gratuits Let's Encrypt reconnus par les navigateurs web](#)

[Un service signé Mozilla teste la sécurité de sites Web](#)

[Avec Certbot, l'EFF veut chiffrer le web](#)