

# Microsoft renforce l'utilisation du HTTPS au sein d'Internet Explorer

Le support du **HTTP Strict Transport Security** (HSTS) fait son entrée dans la version d'Internet Explorer proposée au sein de la mouture de test de Windows 10.

Ce système **renforce la sécurité des communications** entre l'internaute et les serveurs web. Il permet de s'assurer que la connexion est sécurisée. Si le certificat de chiffrement n'est pas correct, la connexion au site ne sera pas possible. De plus, le mélange de contenus sécurisés et en clair au sein d'une même page web n'est pas permis par le HSTS.

Une liste de sites web **devant utiliser le HTTPS par défaut** est fournie avec Internet Explorer. Elle s'appuie sur celle créée pour le projet Chromium. Des mécanismes spécifiques permettent également de s'assurer que l'internaute ne basculera pas en HTTP lorsqu'il a débuté sa visite sur un site en HTTPS.

L'objectif est de s'assurer que la séance de surf sur un site web **s'effectue de bout en bout de façon sécurisée**, en HTTPS, c'est-à-dire de manière chiffrée.

## Il était temps...

Les mauvaises langues remarqueront que Microsoft a pris son temps. Le HSTS est en effet pris en compte depuis les versions 4 de **Firefox, Chrome et Chromium**, soit depuis plusieurs années déjà.

Les serveurs web open source les plus populaires (Apache, Nginx, etc.) sont aujourd'hui compatibles avec ce protocole de sécurité. L'offre IIS de Microsoft peut également être configurée pour prendre en compte le HSTS.

### À lire aussi :

[Internet Explorer soigne sa sécurité](#)

[Chrome va stigmatiser les sites non HTTPS](#)

[Firefox HTTPS Everywhere, une extension pour naviguer en toute sécurité](#)