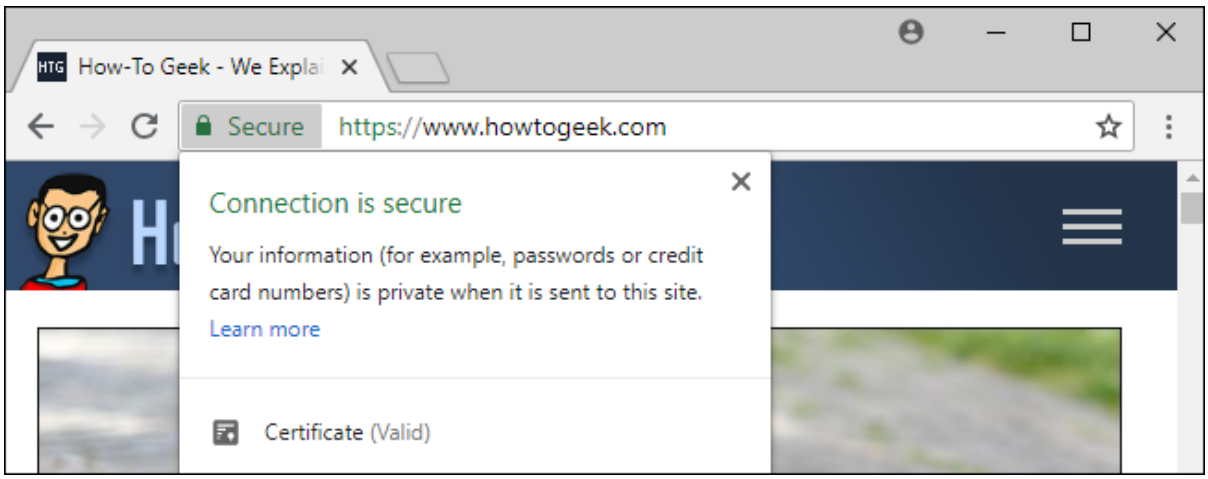
www.howtogeek.com /397043/https-is-almost-everywhere.-so-why-isnt-the-internet…

Explication:
HTTPS est presque partout. Alors, pourquoi Internet n'est-il pas sécurisé maintenant?

La plupart du trafic Web en ligne est maintenant envoyé sur une connexion HTTPS, ce qui le rend « sécurisé ».
En fait, Google avertit maintenant que les sites HTTP non cryptés ne sont pas sécurisés.

Alors pourquoi y a-t-il encore autant de logiciels malveillants, de demande de rançons et d’autres activités dangereuses en ligne ?

Les sites « sécurisés » ont simplement une connexion sécurisée



Chrome affichait le mot « Secure » et un cadenas vert dans la barre d'adresse lorsque vous visitiez un site Web à l'aide de HTTPS.
Les versions modernes de Chrome simple ont une petite icône de verrouillage gris ici, sans le mot « Sécurisé ».

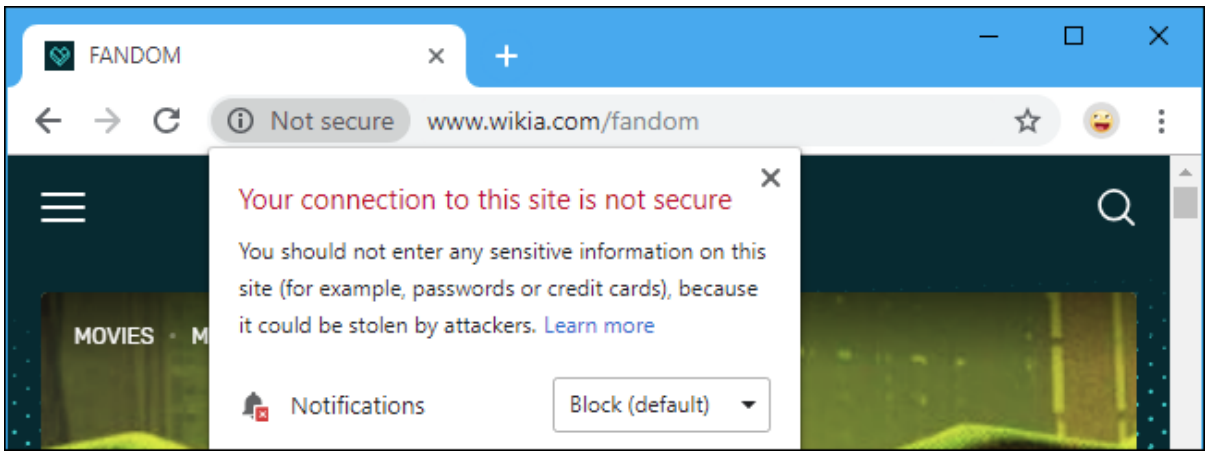
C'est en partie parce que HTTPS est maintenant considéré comme la nouvelle norme de référence.
Tout doit être sécurisé par défaut, donc Chrome ne vous avertit qu'une connexion n'est pas sécurisée lorsque vous accédez à un site sur une connexion HTTP.

Cependant, le mot « Secure » a également disparu parce qu'il était un peu trompeur.
Il semble que Chrome se porte garant du contenu du site comme si tout sur cette page est « sécurisé ».

Mais ce n'est pas vrai du tout.

Un site HTTPS « sécurisé » pourrait être rempli de logiciels malveillants ou être un faux site de phishing.

HTTPS arrête de fouiner et de trafiquer



HTTPS est super, mais il ne fait pas que tout sécuriser.

HTTPS signifie Hypertext Transfer Protocol Secure.
C'est comme le protocole HTTP standard pour se connecter à des sites Web, mais avec une couche de cryptage sécurisé.

Ce chiffrement empêche les gens de fouiner sur vos données en transit, et il arrête les attaques de l'homme au milieu qui peuvent modifier le site web tel qu'il vous est envoyé.
Par exemple, personne ne peut fouiner sur les détails de paiement que vous envoyez au site Web.

En bref, HTTPS s'assure que la connexion entre vous et ce site web particulier est sécurisée.
Personne ne peut l'écouter ou le trafiquer.
Voilà.

CONNEXES: ***Qu'est-ce que HTTPS, et pourquoi devrais-je m'en soucier?***

Cela ne signifie pas vraiment qu'un site est « sécurisé »

HTTPS est grand, et tous les sites Web devraient l'utiliser.
Toutefois, tout ce que cela signifie, c'est que vous utilisez une connexion sécurisée avec ce site Web particulier.
Le mot « Secure » ne dit rien sur le contenu de ce site.

Tout ce que cela signifie, c'est que l'opérateur du site web a acheté un certificat et mis en place le cryptage pour sécuriser la connexion.

Par exemple, un site web dangereux rempli de téléchargements malveillants peut être livré via HTTPS.
Tout cela signifie que le site Web et les fichiers que vous téléchargez sont envoyés sur une connexion sécurisée, mais ils pourraient ne pas être sécurisés.

De même, un criminel pourrait acheter un domaine comme «bankoamerica.com», obtenir un certificat de cryptage SSL pour celui-ci et imiter le vrai site Web de Bank of America. Ce serait un site de phishing avec le cadenas «sécurisé», mais cela signifie simplement que vous avez une connexion sécurisée à ce site de phishing.

HTTPS est toujours génial

Malgré les expressions que les navigateurs utilisent depuis des années, les sites HTTPS ne sont pas vraiment «sécurisés». Le passage des sites Web au HTTPS permet de résoudre certains problèmes, mais ne met pas fin au fléau des logiciels malveillants, du phishing , du spam, des attaques sur des sites vulnérables ou de diverses autres escroqueries en ligne.

Le passage aux HTTP est toujours formidable pour Internet! Selon les statistiques de Google , 80% des pages Web chargées dans Chrome sous Windows sont chargées via HTTPS. Et les utilisateurs de Chrome sous Windows passent 88% de leur temps de navigation sur les sites HTTPS.

Cette transition rend plus difficile pour les criminels d'écouter les données personnelles, en particulier sur le Wi-Fi public ou d'autres réseaux publics. Cela minimise également considérablement les chances que vous rencontriez une attaque d'intermédiaire sur le Wi-Fi public ou un autre réseau.

Par exemple, disons que vous téléchargez le fichier .exe d'un programme à partir d'un site Web alors que vous êtes connecté à

un réseau Wi-Fi public. Si vous êtes connecté avec HTTP, l'opérateur Wi-FI pourrait altérer le téléchargement et vous envoyer un autre fichier .exe malveillant. Si vous êtes connecté via HTTPS, la connexion est sécurisée et personne ne peut altérer le téléchargement de votre logiciel.

C'est une énorme victoire! Mais ce n'est pas une solution miracle. Vous devez toujours utiliser des pratiques de sécurité en ligne de base pour vous protéger contre les logiciels malveillants, détecter les sites de phishing et éviter d'autres problèmes en ligne.

Recherche et mise en page par:
Michel Cloutier
Pour le compte de CIVBDL
20210102