digicert®

Votre guide de référence rapide HTTPS Everywhere

Qui mieux que le leader des certificats SSL, DigiCert, peut vous faire découvrir tous les avantages de l'utilisation du HTTPS sur l'ensemble de votre site et vous aider à le mettre en oeuvre !

https:// Qu'est-ce que le HTTPS Everywhere ?

HTTPS Everywhere est une mesure de sécurité figurant parmi les meilleures pratiques pour les sites Web, qui garantit la protection des internautes tout au long de leur visite d'un site. Ce terme désigne simplement l'utilisation du HTTPS – le protocole Web sécurisé avec les protocoles SSL/TLS – sur l'ensemble de votre site Web et non de manière sélective.

HTTPS authentifie l'identité de votre site Web, la connexion et l'intégrité des données et crypte toutes les informations échangées entre le site et les internautes (y compris les cookies). Il protège ainsi vos informations contre toute visualisation, modification ou utilisation non autorisée. Sécuriser la connexion pendant toute une session de navigation est indispensable pour protéger les internautes d'attaques de type usurpation d'identité, par injection et hôte interposé.

Les navigateurs et la volonté de promouvoir le HTTPS

Il n'est plus acceptable de ne sécuriser qu'une partie des connexions de vos utilisateurs. Quand vous utilisez le HTTPS de façon intermittente sur votre site Web, seules quelques pages sont protégées par cryptage et authentification SSL. Les autres restent vulnérables au vol de données, à l'injection/la modification de contenu et à la violation de la confidentialité du fait de la surveillance Internet.

Le déploiement du SSL de manière intermittente ne satisfait pas aux attentes et aux droits des utilisateurs. Cela ne répond pas non plus aux attentes des navigateurs et des plateformes des systèmes d'exploitation. Dans le cadre d'une campagne de plusieurs années pour encourager l'adoption du HTTPS, les principaux fournisseurs de navigateurs, notamment Google, Mozilla et Apple, ont petit à petit modifié l'interface de ces navigateurs pour renforcer le caractère négatif du HTTP et mettre en avant de façon positive le HTTPS sécurisé.

Qu'avez-vous à y gagner ?

La confiance est le fondement de l'économie sur Internet. Pour gagner cette confiance, il vous faut une sécurisation de bout en bout qui protège chaque page Web visitée, pas seulement les pages de connexion et de paiement. Les modifications récentes des normes Internet et des navigateurs Web offrent également un avantage aux sites Web qui utilisent le HTTPS et punissent les sites non sécurisés qui continuent à employer le protocole HTTP.

Google, par exemple, confère un rang plus élevé aux pages protégées par HTTPS depuis 2014. Une notification « Sécurisé » est également affichée dans la barre d'adresse des pages HTTPS. En juillet 2018, Google commencera aussi à afficher un avertissement « non sécurisé » sur chaque page HTTP. Chrome a été le premier navigateur à venir

placer un avertissement aux internautes sur toutes les pages se basant sur le protocole HTTP. Les autres navigateurs lui emboîteront le pas au fur et à mesure du passage d'Internet à une norme de « sécurisation par défaut ».

En outre, de nombreuses nouvelles technologies Web et fonctionnalités de navigateur exigeront l'utilisation du HTTPS. Cela comprend le HTTP/2, une amélioration fondamentale du protocole de communication Web qui améliorera énormément les performances des sites, ainsi que des fonctions comme la géolocalisation, notifications, Service Workers, norme mobile AMP de Google, nouvelles méthodes de compression et bien davantage. En bref, sans HTTPS, votre site Web sera piégé dans le passé.

3 Les trois principales astuces pour une transition vers le HTTPS Everywhere

1. Veillez à ce que tous les services tiers dont vous dépendez, comme les services de publicité ou d'analyse exécutés sur votre site, soient disponibles sur HTTPS pour éviter les problèmes de « contenu mixte ».
2. Achetez des certificats SSL supplémentaires si différentes parties de votre site Web sont exécutées sur différents serveurs ou domaines.
3. Redirigez toutes les pages de votre site vers leur nouvel équivalent HTTPS. N'oubliez pas non plus de mettre à jour vos outils Google Webmaster. Quand vous passez à l'extension HTTPS Everywhere, il y a des répercussions au niveau du référencement Web. Google et d'autres moteurs de recherche considèrent cela comme un déplacement de site semblable à un nouveau nom de domaine.

digicert®

Conclusion

- En mettant en oeuvre HTTPS Everywhere, vous sécurisez les données des internautes et de votre entreprise sur toutes les pages de votre site – du début à la fin.
- L'utilisation intermittente du cryptage SSL ne suffit plus pour protéger les internautes et empêcher la violation des données.
- L'interface utilisateur du navigateur commencera à afficher des indicateurs négatifs « non sécurisé » et cette tendance ne fera que se poursuivre avec l'augmentation des attentes en matière de sécurisation.
- Passez à un rang de référencement plus élevé sur Google avec HTTPS Everywhere, une amélioration qui viendra probablement encore plus se renforcer à l'avenir.
- HTTPS Everywhere est facile à mettre en oeuvre sur votre site Web et n'exige pas de matériel supplémentaire.
- Sécurisez votre site avec des certificats SSL pour renforcer votre marque et votre réputation en illustrant votre engagement envers la sécurité en ligne.
- L'augmentation de la confiance des utilisateurs diminue les taux de rebond et les abandons de panier. Vous augmenterez ainsi vos transactions et taux de conversion.