Les Guides Abondance

HTTPS

Guide de passage de votre site en mode sécurisé

Par **Mathieu Chartier** (Internet-Formation.fr)

- Février 2015 -

Sommaire

Introduction

Depuis les premiers pas de Google en 1998, les créateurs du moteur de recherche ont toujours souhaité développer un outil à la pointe de la technologie. Si la politique interne fait parfois grincer des dents moult référenceurs et spécialistes du webmarketing, force est de constater que la firme tend toujours à maintenir sa ligne de conduite, quitte à déplaire aux fans inconditionnels de la marque.
L'histoire récente a démontré que Google cherchait à « purifier » coûte que coûte ses index pour proposer toujours plus de résultats naturels de qualité à ses visiteurs et clients. Les raz-de-marée provoqués par les filtres Google Panda et Penguin ont permis de nettoyer grandement le moteur, au risque de faire couler des entreprises et de toucher des innocents pour cause d'effets secondaires non maîtrisés ou imprévus.

Les vagues de pénalités ont dévasté la Toile et créé un sentiment de peur, au point que l'hégémonie de Google a divisé les internautes. Peu importe pour la firme, l'objectif est de garder le cap et désormais, Google s'attaque à l'une des tendances les plus fortes de sa génération : la sécurisation des données. Si cela n'a rien de pénalisant pour une fois, cela nous prouve que la devise de l'entreprise, « Don't be evil », n'a jamais été aussi pertinente... Ou pas...

Source de l'image : archive.org

La protection des données, de la vie privée ainsi que la sécurité sont ainsi des phénomènes qui prennent de plus en plus d'ampleur dans le cœur des internautes depuis des mois. Face au déploiement massif du web, du cloud et des réseaux sociaux, nombre de personnes se sont posé des questions au sujet de l'impact que pourrait avoir sur leur vie les informations qui traînent un peu partout sur la Toile. Cette question existentielle a relancé l'idée de la sécurisation des données et indirectement du rôle des protocoles SSL et HTTPS.

Dans les faits, la question de la sécurité et de la protection des données n'est pas une affaire récente. Nous nous sommes toujours interrogés sur l'influence du web sur nos vies privées et nos données personnelles. Quels risques courons-nous ? Devons-nous informer les sites gérant des renseignements privés ? N'existe-t-il pas des

moyens de détourner les informations stockées ? Toutes ces questions se sont multipliées avec l'essor d'Internet et du piratage, mais cet aspect s'est accentué à partir du moment où les boutiques en ligne ont fleuri sur la Toile et où les réseaux sociaux ont connu un franc succès. Dès lors, l'idée de la sécurisation des données a pris tout son sens afin de protéger notre intimité mais aussi nos comptes bancaires (qui restent le nerf de la guerre…).

Tout ce que nous allons développer dans ce guide spécialisé est axé sur cet idéal, c'est-à-dire protéger nos informations tout en améliorant la confiance des internautes envers nos sites web. Google a dévoilé récemment que le rôle de la sécurité pourrait impacter la position des pages web dans les résultats de recherche. Les passionnés que nous sommes ne peuvent donc pas passer outre et faire comme si de rien n'était…

Les changements ou ajouts de facteurs au sein de l'algorithme du moteur de recherche ne sont pas forcément fréquents. Certes, nous savons que Google effectue plusieurs centaines de changements par an (890 en 2013, par exemple) mais nous pouvons légitimement admettre que la grande majorité de ces mises à jour sont mineures (déploiement dans plusieurs pays, correction de codes...). Toutefois, nous ne sommes pas des devins et notre impuissance ne nous permet pas toujours d'affirmer que tels ou tels critères favorisent le positionnement des pages. Les spécialistes se réfèrent donc à des brevets, à des tests ou à des déclarations pour booster nos connaissances à ce sujet. Que dire de l'aubaine qui nous est présentée ici, puisque c'est Google qui l'a officiellement annoncée…

Ce guide a donc pour ambition de présenter le rôle de la sécurité pour les moteurs de recherche, mais aussi de maîtriser le rôle des protocoles SSL et HTTPS afin de mieux protéger nos sites web et nos données, que ce soit des boutiques en ligne ou tout autre type de support. Nous entrerons également dans l'historique de ces protocoles plus méconnus qu'il n'y paraît et dans le choix — ô combien complexe — des certificats, pour finir par des considérations plus techniques afin d'utiliser ces protocoles selon notre hébergeur ou en l'installant par nous-même.

Que votre lecture soit bonne et instructive, c'est tout le mal que nous vous souhaitons !

Mathieu Chartier

CHAPITRE 1 : QU'EST-CE QUE LE SSL ?

Définition et présentation des protocoles courants

De la magie de l'Internet est née une forme de confusion contre laquelle lutte une grande majorité de spécialistes, à savoir la différence entre Internet et le web. Nous trouvons partout la mention de « site Internet », ce qui en soit n'est pas réellement juste. Nous devrions parler de « site web », et uniquement de cela, le Web étant l'un des services mis à disposition sur Internet. Pourquoi cette petite erreur peut-elle s'avérer dérangeante ? Tout simplement parce qu'elle entraîne par la même occasion des confusions à tous les niveaux, et notamment en ce qui concerne les protocoles qui vont nous intéresser tout au long de notre lecture…

Si nous parlons bien de site web, les protocoles sont quant à eux directement liés à Internet et peuvent être assez nombreux. Il convient donc de les présenter pour limiter les interprétations douteuses en ce qui les concerne. Nous n'entrerons pas dans les détails profonds et obscurs de ces protocoles, mais il est important de bien définir les principaux afin de mieux comprendre l'objectif de la sécurisation des données.

Le réseau Internet est composé d'un nombre incalculable de sous-réseaux qui réussissent à communiquer entre eux grâce à des protocoles. Partant de ce constat, nous pouvons déduire que les protocoles représentent une série d'étapes à suivre pour permettre la liaison des données entre plusieurs sous-réseaux ou machines. Les protocoles s'exécutent sur plusieurs couches de réseaux et n'ont pas tous les mêmes degrés de sécurisation ni même des objectifs identiques. Nous considérons qu'il existe deux grandes familles de protocoles, chacune n'apportant pas des garanties identiques en matière de protection ou de vérification des données :

- Orienté connexion : ces protocoles d'envoi ont l'avantage de vérifier la réception des données et d'envoyer un accusé de réception (une sorte de « ping » en retour).
- Non-orienté connexion : les données sont envoyées en blocs et ne sont pas vérifiées par la machine qui reçoit les informations, ce qui ne garantit pas une réception sûre mais présente l'avantage d'être souvent un peu plus rapide à l'exécution.

Les protocoles ne servent qu'à définir la manière de communiquer entre les

différentes machines. Nous pourrions presque les assimiler à différentes sortes de tuyaux dans lesquels passent des flux spécifiques. Nous définirons ici les principaux qui nous seront utiles lorsque nous évoquerons l'administration des serveurs web, ce qui ne s'avère pas toujours simple à comprendre pour les néophytes…

Parmi les protocoles les plus connus, nous pouvons proposer cette liste non exhaustive :

- IP (pour « Internet Protocol ») : c'est le premier protocole à avoir été défini (bien avant l'arrivée du Web, d'ailleurs) et il gère les transferts de paquets dans le réseau. Il permet de donner une adresse « fixe » à une machine afin de pouvoir la repérer dans le réseau et donc de communiquer avec elle. Une adresse IP est inclue dans un système d'informations, un peu à l'image des ISBN pour les livres par exemple, chaque IP correspondant à des réseaux, sous-réseaux et machines précises.
- TCP (pour « Transmission Control Protocol ») : c'est le protocole de transmission des données associé en général aux adresses IP, il est à l'origine de toutes les connexions entre les machines et sert de base à d'autres protocoles.
- DNS (« Domain Name System ») : il s'agit d'une méthode, créée en 1983, qui permet d'attribuer des alias aux adresses IP grâce à un système de correspondance entre DNS et IP. Son objectif est de faciliter la compréhension et la mémorisation des adresses en faisant correspondre des noms de domaine intelligibles aux diverses adresses IP. Il faut avouer qu'il est plus agréable de retenir « www.site.com » que 213.168.1.15, par exemple…
- FTP (« File Transfer Protocol ») : protocole de transfert de données par flux en masse. Il est un peu plus lent que d'autres protocoles de transfert mais plus performant pour les envois multiples. C'est pour cette raison qu'il garde la préférence sur Internet.
- HTTP (pour « HyperText Transfer Protocol ») : c'est le principal canal de diffusion des informations sur lequel s'appuie le web. Il a été créé par Tim Berners Lee en 1990 pour développer le web que nous connaissons à l'aide de fichiers HTML et d'autres méthodes d'envoi de données (POST, GET, PUT…).
- HTTPS : c'est le pendant sécurisé du protocole HTTP qui s'appuie sur les protocoles SSL ou TLS que nous allons présenter par la suite.

- SMTP, POP et IMAP : ces trois pro-

Figure 1.1 – Protocoles Internet (source : http://www.formatiques.com/les-protocoles-internet.html)

tocoles sont utilisés pour les transferts de courriers électroniques (e-mails). SMTP permet d'envoyer les données. POP et IMAP servent à recevoir des emails.

Le sujet de notre guide est axé sur la sécurité des données, c'est pourquoi nous ne pouvons pas clôturer cette présentation des protocoles sans évoquer ceux qui vont nous être utiles au cours de nos pérégrinations :

- SSL (« Secure Socket Layer ») ou TLS (« Transport Layer Security ») : ce sont deux versions de protocoles destinés à sécuriser les données et surtout les échanges sur Internet grâce à des systèmes de chiffrement et des vérifications avancées gérées à partir de clés publiques et privées.
- SSH (« Secure SHell ») : il est à la fois un programme et un protocole de connexion. Ses principales différences avec SSL est que SSH requiert une authentification côté serveur et qu'il peut être utilisé ailleurs que sur le Web au sein d'autres services d'Internet comme Telnet, les courriers électroniques, FTP…

Ce premier tour d'horizon des protocoles Internet aura eu le mérite de nous rappeler ou de nous mettre en tête le fonctionnement complexe qui règne derrière chacune de nos connexions. Nous allons désormais présenter plus en détails SSL et HTTPS pour mesurer leur rôle réel sur la Toile et leur impact éventuel sur le référencement web.

Description avancée du protocole SSL

Fonctionnement général

… (voir page suivante)…

Le nom actuel des certificats de sécurité est TLS mais l'ancienne version créée par Netscape, appelée SSL, s'est imposée à nous et le sigle est resté dans nos esprits. En réalité, nous pourrions presque considérer que SSL et TLS sont identiques mais le second est plus récent et utilisé de nos jours grâce à des systèmes plus évolués. Mais nous utilisons encore à tort le terme SSL, comme nous le ferons dans ce guide afin de ne perdre personne.

Ceci est un extrait du guide Abondance "HTTPS - Guide de passage de votre site en mode sécurisé"

Achetez ce guide complet en ligne à l'adresse :

http://www.boutique-abondance.com/

Conclusion

Nous avons tenté dans ce guide de vous donner un large aperçu de ce que sont les protocoles HTTPS et SSL/TLS sur Internet, mais aussi de déterminer les tenants et aboutissants qui vous permettent d'en tirer profit au mieux.

La mise en place du nouveau facteur de positionnement de Google pour les sites sécurisés avec des certificats SSL a quelque peu chamboulé le web et les idées qui en émanent. À ce jour, vous savez que le phénomène est encore peu développé et que le critère manque de poids dans l'algorithme du moteur de recherche. Mais si les dires des officiels se confirment, HTTPS risque de devenir un facteur plus important dans les années à venir…

Dans les faits, nous avons vu qu'il n'est pas toujours simple de mettre en place ces services sécurisés pour des raisons logistiques, techniques et financières, car le passage d'HTTP à HTTPS ne se fait pas d'un seul coup. Il est nécessaire d'avoir quelques prérequis et de bonnes connaissances initiales en gestion de serveurs pour s'armer et installer SSL, hormis sur les hébergements mutualisés qui proposent ce service sans efforts particuliers mais souvent sous une forme dégradée.

L'autre problématique de l'HTTPS se pose autour du choix des certificats et de leur prix, car ces deux facteurs ont une forte tendance à bloquer les récalcitrants. De plus, nous avons vu que la présence d'une sécurité accrue est loin d'être toujours recommandée sur certains types de sites, ce qui ne justifie pas toujours les tarifs élevés de certains certificats de bonne qualité. Dans cette jungle d'autorités de certification, il faut bien avouer qu'il est difficile de trouver sa place et Google aura intérêt à mieux argumenter pour favoriser les sites sécurisés mais aussi pour donner envie aux webmasters de passer le cap. Concluons notre long discours en notant que l'HTTPS peut constituer un vrai plus pour une majorité de site web, au-delà même du positionnement dans les SERP qui nous a amené à rédiger ces pages, le fait que Google ait amorcé le phénomène nous oblige à envisager l'avenir autrement et à espérer que la sécurité progresse dans les années futures.

Si ce facteur ne révolutionnera pas la recherche mondiale ni même le fait de devoir avant tout rédiger de bons contenus, de qualité et à forte valeur ajoutée, vous pouvez désormais vous poser légitimement la question d'utiliser SSL et HTTPS pour vos sites web en attendant les évolutions du facteur SEO dans l'algorithme de Google…

Bon référencement !

Mathieu Chartier

Présentation de l'auteur

Mathieu Chartier est un jeune consultant, webmaster et formateur poitevin qui s'est spécialisé dès ses premières heures dans le référencement et la technique web.

Initialement archéologue, il a suivi un master en information et communication (spécialité web éditorial) à l'université de Poitiers en 2008, ce qui lui a donné le goût de l'écrit, du code et du web...

Il a développé son auto-entreprise basée sur les centres de formation et agences www.internet-formation.fr et www.evigeo.com, ce qui lui permet de dispenser des formations à travers le Poitou-Charentes et en France sans oublier son amour pour les prestations pures (référencement, créations de scripts, d'extensions WordPress, de sites web…).

Sa passion pour l'écriture s'est développée dès 2013 avec un premier essai consacré au SEO et titré Le guide du référencement web (éditions First) puis un second ouvrage intitulé Guide complet des réseaux sociaux (éditions First). Un troisième livre coécrit avec Alexandra Martin (www.miss-seo-girl.com) sur les techniques avancées de référencement a également été publié aux éditions Eyrolles le 1er janvier 2015, sous l'intitulé Techniques de référencement web : audit et suivi SEO.

Vous pouvez suivre ses actualités sur son site personnel www.mathieu-chartier.com ou tout simplement via son blog professionnel blog.internet-formation.fr sur lequel il partage sa passion, ses expériences et ses scripts.

Retrouvez Mathieu Chartier sur vos plates-formes préférées :

- Blog Internet-Formation : http://blog.internet-formation.fr
- Twitter : https://twitter.com/Formation_web
- Google+ : https://plus.google.com/+MathieuChartierSEO
- Viadeo : http://www.viadeo.com/fr/profile/mathieu.chartier4
- Linkedin : https://www.linkedin.com/in/chartiermathieu
- Instagram : http://instagram.com/mathieu_chartier

INTERNET FORMATION