Comment s’assurer d’être sur un site sécurisé et comment sécuriser son site ? Par Laurent.

La sécurité d’un site web est primordiale, que ce soit pour ses utilisateurs qui ne souhaitent pas perdre leurs données, ou pour ses propriétaires qui ne souhaitent pas subir les conséquences d’un vol de données.

Il est donc nécessaire d’avoir un site sécurisé. La majorité des utilisateurs et entrepreneurs pensent que le https est la preuve d’un tel site internet.

Seulement ce n’est pas forcément le cas pour deux raisons.

HTTPS ne montre que la sécurisation de l’échange de données.

En d'autres termes, le **stockage** sécurisé des données n'est absolument pas garanti par un site en HTTPS, seul leur échange l'est. Cela peut s'avérer problématique si le serveur est compromis. Et même les grandes entreprises ne sont pas à l'abri. Par exemple, en 2012, les données de 165 millions d'utilisateurs de LinkedIn ont été volées. Pire, comme à l'époque le chiffrement utilisé était SHA-1, qui n'est plus sécurisé, et que les mots de passe n'étaient pas salés, ces mots de passe ont rapidement été décryptés.

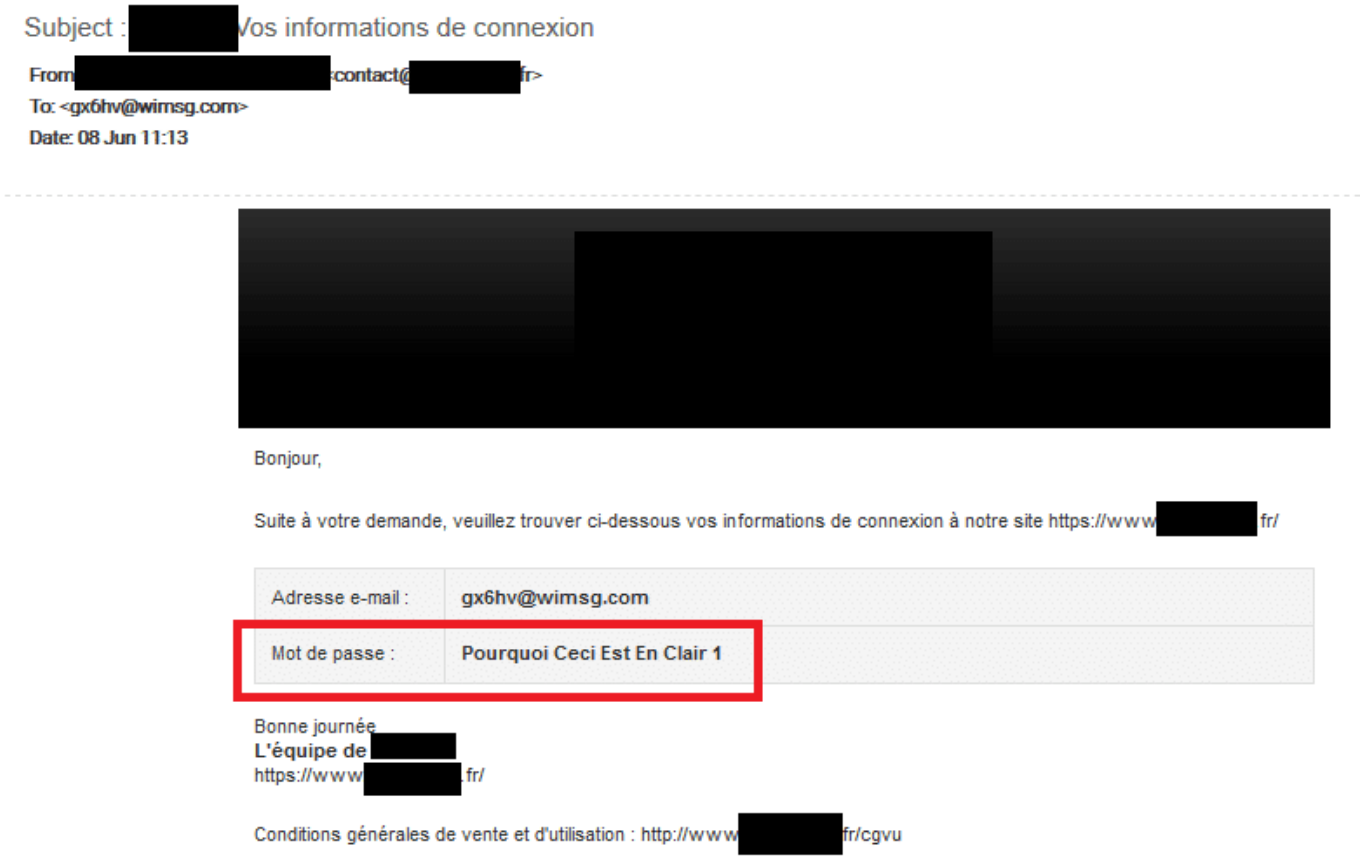
Si vous voulez découvrir si une brèche de données contient les vôtres, le site Have I Been Pwned est une excellente ressource. Il y a d'ailleurs déjà un article détaillant son utilisation sur Sospc. Par je ne sais quel miracle, ce n'a toujours pas été mon cas. Mais avec 5 milliards de comptes compromis selon le site, vous n'êtes pas forcément dans la même situation.

Alors que faire ? Car les sites web ne dévoilent pas leurs politiques de sécurité pour des raisons évidentes. L'utilisateur doit donc dans la majorité des cas faire confiance au site lorsqu'il décide d'y entrer ses données.

Je tiens cependant à mentionner un cas particulier, où l'utilisateur peut tout de suite savoir que le site n'est pas sécurisé.

Si un site stocke votre mot de passe en clair, fuyez.

Impossible ! Nous sommes en 2018 ! Aucun site ne réaliserait cela !



Subject : [redacted]Vos informations de connexion

From [redacted]<contact@[redacted]fr>

To: <gx6hv@wimsg.com>

Date: 08 Jun 11:13

[redacted]

Bonjour,

Suite à votre demande, veuillez trouver ci-dessous vos informations de connexion à notre site https://www[redacted]fr/

Adresse e-mail :	gx6hv@wimsg.com
Mot de passe :	Pourquoi Ceci Est En Clair 1

Bonne journée,

L'équipe de [redacted]

https://www[redacted].fr/

Conditions générales de vente et d'utilisation : http://www[redacted]fr/cgvu

…Diantre, ils ont osé. Le 1 était nécessaire car le mot de passe requiert un chiffre, si vous vous posez la question.

D'après plaintextoffenders.com, qui regroupe des cas similaires (mais anglophones), 30% des sites web stockent leurs mots de passe en clair. Souvent il s'agit de sites peu connus, mais pas toujours. En effet, parmi les coupables, on trouve Le New York Times, Fedex, Adobe, ou AT&T (Télécom américain avec plus de 400 millions de clients) (Source).

Malheureusement, cela est difficile à éviter puisque vous apprendrez le problème après votre inscription… D'où l'utilité d'utiliser un mot de passe unique par site. Cela dit, puisque vous ne pouvez pas changer de données bancaires, il vaut mieux ne pas les donner à de tels sites.

HTTPS ne garantit votre sécurité que si l'infrastructure est à jour.

La bonne nouvelle, c'est que c'est généralement le cas.

La seconde bonne nouvelle, c'est que même lorsque ce n'est pas le cas, décrypter le trafic entre vous et un site en HTTPS devient possible en théorie, mais cela reste peu pratique.

Néanmoins, une mention semblait nécessaire. Surtout que même si le site que vous visitez est vulnérable à une faille, le cadenas sera toujours présent.

Si vous souhaitez tester la sécurité de votre propre certificat SSL, Le test est disponible en cliquant ici. SSL Pulse note que sur les 150 000 sites les plus populaires, 60% sont sécurisés, et donc que 29% ont un niveau de sécurité

insatisfaisant, et 11% sont vulnérables.

Enfin, sachez qu'il n'y a aucun moyen pour Internet Explorer 6 de communiquer de manière sécurisée. Si vous utilisez encore IE6, reprenez votre vie en main et changez de navigateur. Il n'est plus supporté depuis 2010…

Que faire pour avoir un site sécurisé ?

Stockage des données.

Heureusement, les CMS comme WordPress implémentent dans leur grande majorité des mesures de sécurité en hashant les mots de passe et données sensibles. Cependant, si vous réalisez votre site sans ces outils, il ne faudra pas oublier d'implémenter ces mesures de sécurité. Pour rappel :

- Salez les mots de passe (en rajoutant une phrase avant ceux-ci)
- Utilisez un algorithme de hash fort (Bcrypt, pas MD5 ni SHA1)

L'attrait du mot de passe en clair lors du développement d'un site est de simplifier le processus de récupération du mot de passe. En effet, si le mot de passe est hashé, pas moyen de le renvoyer à l'utilisateur. Tant pis, prendre l'effort d'implanter une bonne procédure de récupération vaut le coup.

Vérifier son implémentation d'HTTPS.

Comme mentionné précédemment, vous pouvez tester la sécurité de votre site ici. La meilleure option est de prier pour que le résultat soit satisfaisant ; sinon, pour améliorer votre note, il faudra mettre les mains dans le cambouis. Je vous recommanderais plutôt de prendre contact avec votre hébergeur

à moins de vraiment savoir ce que vous faites. Mais si c'est le cas et que votre hébergeur vous laisse plein contrôle sur votre serveur, sachez qu'utiliser la dernière version de OpenSSL vous donnera une note suffisante.

L'avis de Laurent Brault.

La sécurité d'un site Internet est primordiale, surtout dans le cas de site ayant beaucoup de données personnelles. Cette sécurité doit être analysée tant du point de vue du Web-Master que de celui de l'Internaute.

Les consignes de sécurité de base sont assez simple.

Vue du WebMaster.

- Le site doit être https
- Il ne doit pas avoir de version http
- Les mots de passe doivent être chiffrés avec un protocole sécurisé. Ils ne doivent JAMAIS être en clair, et encore moins transmis en clair dans un email.
- Les données personnelles doivent être chiffrées et leur gestion doit respecter le RGPD (consultable et modifiable par le « propriétaire », effaçable à sa demande).

En respectant ces 4 règles vous obtiendrez un site avec un bon niveau de sécurité. Mais soyez vigilent, les hackers ne dorment que d'un œil.

Vue de l'Internaute.

- Eviter les sites qui ne sont pas https. En cours de navigation assurez-vous que le site ne repasse pas en http … C'est le signe d'un piratage en cours.

- Les mots de passe ne doivent JAMAIS être en clair. Si après inscription le site vous transmets un bel email avec votre identifiant et votre mot de passe. Fuyez ce site.
- La gestion de vos Données Personnelles doit respecter le RGPD. Vous devez trouver facilement la description de leur utilisation, la procédure pour les obtenir, les modifier et éventuellement les effacer.

Ces quelques conseils ne vous garantissent pas contre un piratage ou une utilisation abusive de vos données mais vous aurez fait votre possible pour les éviter.

Si vous êtes concernés par la sécurité numérique, faites une visite sur le site de **MDK Solutions**, qui a rédigé cet article. Cette société Rémoise est spécialisée dans la gestion sécurisée des données numériques pour usage nomade.

*Vous avez envie comme **Laurent** de publier sur Sospc sur un sujet qui vous passionne ?*

*Je vous propose de **vous rendre ICI** pour en savoir plus si vous êtes intéressé.*

Christophe, Administrateur.