Problème avec les mails de Li P’ti Fouineu ! 2e épisode !

Bonsoir le Monde !

décidément, les mails que j’envoie aux abonnés quand j’ai publié un nouvel article m’auront causé bien du tracas !

Dernier problème en date signalé par Sophie (merci Sophie): lorsque vous cliquez sur un lien dans mon mail (newsletter), certains d’entre vous, mais pas tout le monde, reçoivent une “**Erreur due à un contenu corrompu**” avec Firefox et quelque chose de proche ou encore “**Ce site est inaccessible**” avec d’autres navigateurs et ne réussissent pas à afficher mon article !!!! Cela arrive encore plus facilement si vous avez des extensions de navigateur anti-popup et/ou anti-publicitaires qui appliquent en général des règles plus strictes.

Je pense avoir réussi à corriger le problème et c'est la raison pourquoi je publie ce nouvel article pour que vous receviez la newsletter corrigée annonçant ce nouvel article et puissiez tester si le clic sur un lien du mail fonctionne à nouveau !

Qu'est-ce qu'il a dit le monsieur ? Rien pigé !

Je demande aux abonnés d'ouvrir mon prochain mail et de cliquer sur un des liens qu'il contiendra et surtout de me prévenir si cela ne devait pas marcher !
(Il suffira de répondre au mail…)

Merci d'avance pour votre aide !

L'explication pour les geeks mais pas que:

La newsletter (le mail que vous recevez à chaque nouvel article) est fabriquée automatiquement par un plugin de WordPress et ce plugin remplace les liens de l'article par d'autres pointant sur une page de passage intermédiaire spéciale qui sert à collecter des statistiques. Je ne sais malheureusement pas changer ça …

Jusque-là, pas trop de problème…

Si vous vous souvenez, j'ai déjà dû changer de système d'envoi de la newsletter car mon mail privé que j'utilisais jusque-là refusait soudainement que j'envoie un mail à plus de 20 destinataires alors que mon blog a un peu plus de 100 abonnés. Cela m'a pris quelques semaines de recherche et de tests avant que je choisisse **SendGrid** comme service gratuit d'envoi de mail "en masse".

SendGrid fait la même chose que le plugin WordPress, il remplace les liens dans le mail par d'autres pointant sur une page de passage intermédiaire spéciale qui sert à collecter des statistiques !

Ce faisant, quand vous cliquez sur un lien dans ma newsletter, vous être redirigé de façon invisible une première fois vers SendGrid, puis une deuxième fois, toujours de façon invisible, vers le plugin WordPress et enfin vers la page de l'article, la page d'accueil ou le lien pour se désabonner.

Vous n'êtes pas sans savoir qu'une minorité d'emmerdeurs finis (les hackers black hat) emmerdent l'écrasante majorité des gens "gentils" comme vous et moi de

sorte qu'on est obligé d'installer antivirus, anti-malware, anti-pub et j'en passe pour se protéger !

Les navigateurs Internet comme Firefox, Google Chrome et les autres essaient aussi de vous protéger au maximum et c'est de là que vient mon nouveau problème !

En effet, quand le navigateur (ou une de ses extensions) voit un lien qui est redirigé trop de fois, il considère cela comme un problème de sécurité et affiche une erreur à la place du site final qu'il considère maintenant comme étant trop à risque !
Le message d'erreur est évidemment incompréhensible pour le commun des mortels (et même faux dans mon cas).

Et voilà comment des milliers de sites absolument innocents faits par des amateurs sont exclus d'Internet et disparaissent réduisant ainsi la richesse d'Internet comme peau de chagrin car il ne restera que les gros sites commerciaux ayant les moyens d'avoir un webmaster en permanence sur le pont avec des compétences suffisamment pointues pour faire face à la complexité grandissante de la gestion d'un site web !

C'est la même raison de sécurité très complexe à gérer qui fait disparaître les offres gratuites de service Internet ! **C'en est déjà fini de l'Internet pour tous !**
Pour combattre ça, suivez par exemple mes conseils pour publier votre propre site web gratuitement ! Commencez par l'épisode 1.

Si ça continue comme cela, **il faut s'attendre à ce que Internet devienne impraticable** un jour ou l'autre ! Demandez-vous ce que vous ferez alors … Moi je sais déjà, payer betalen payare !!!!!

SendGrid, qui a été racheté par Twilio, me permet actuellement d'envoyer gratuitement 100 mails par jour; il y a déjà plus de 100 abonnés pour le blog et je ne peux donc déjà plus écrire un article par jour (qui a dit "heureusement" ?)… si le nombre de mails par jour est encore diminué ou si le blog gagne des abonnés, Il n'est pas impossible que je doive changer de service d'envoi de mails d'ici quelque temps… MailJet permet 200 mails par jour…

La solution que j'ai pu appliquer est de supprimer les statistiques de SendGrid

qui font double-emploi et ne me servent à rien. Heureusement, il y a un réglage qui permet cela chez SendGrid; un tel réglage n'existe pas sur le plugin WordPress.
Avec ces nouveaux réglages, les liens cliquables de ma newsletter ne seront plus redirigés qu'une seule fois au lieu de deux et j'espère que cela va régler le problème !

Pour avoir ce réglage sur WordPress, je devrais installer une nouvelle version du plugin; j'ai essayé cela mais ça a cassé complètement mon site et m'a demandé à nouveau quelques heures de travail pour le remettre debout !
J'ai évidemment signalé cela aux auteurs du plugin en question mais pas de réponse jusqu'ici (et je dois avouer que je n'en attends pas…)

Voilà, vous savez tout !

Li P'ti Fouineu vous salue bien !

Mon adresse mail a-t-elle été compromise ?

Bonsoir le Monde !

On a tous une ou plusieurs adresses de messagerie qu'on a renseignées sur plein de sites où l'on s'est inscrit (= créé un compte) et dont on ne change quasi jamais le mot de passe et je parie aussi que plusieurs d'entre-vous ne connaissent même plus les mots de passe de ces sites !

Or une adresse de messagerie est une cible de choix pour les pirates qui peuvent utiliser celles qu'ils ont réussi à craquer pour envoyer des mails tous azimut en votre nom le plus souvent sans même que vous le remarquiez …
Nos mails contiennent aussi des tonnes d'informations aussi privées que précieuses pour un pirate !

Il y a un moyen de savoir si votre adresse mail a un jour été compromise en consultant une liste des compromissions connues.

Le plus facile est d'utiliser **Firefox Monitor** qui est en français et basé sur Have I Been Pwned (site en anglais) dont j'ai déjà parlé dans un article précédent !

Vous n'êtes pas obligé d'utiliser le navigateur Firefox pour utiliser Firefox Monitor qui est un site web et pas une extension du navigateur !

Il s'agit du site web **https://monitor.firefox.com** où vous renseignez votre adresse mail à vérifier et le site vous retourne la liste des fuites éventuelles connues pour votre mail !

Si aucune fuite ne vous est retournée, cela veut dire que votre mail n'a pas été compromis dans des piratages connus (tous les piratages ne sont évidemment pas connus publiquement).

Si une ou plusieurs fuites sont listées et que vous n'avez jamais changé le mot de passe du site ayant subi un piratage, il est impératif que vous changiez le mot de passe du compte compromis !!!!
Les fuites peuvent provenir de votre fournisseur de mail mais aussi d'autres site où vous avez renseigné votre adresse mail.

L'avantage d'utiliser Firefox Monitor est que si vous avez déjà un compte Firefox ou que vous en créez un, vous pouvez aussi être averti de toute nouvelle fuite découverte concernant votre adresse mail.

Comme exemple, mon adresse Gmail a été compromise dans 11 piratages connus (Dropbox, Tumblr, Avast, etc…) et mon adresse Hotmail dans 2 piratages connus…
Pour chaque fuite, le site renseigne quelles données ont été compromises comme l'adresse mail, l'adresse IP, le mot de passe, le numéro de téléphone, etc …
Mon adresse mail GMX, qui est maintenant mon adresse principale, n'a encore jamais été compromise.

Normalement, chaque site compromis devrait vous prévenir et vous demander d'actualiser votre mot de passe mais certains ne le font malheureusement pas ou le mail de notification peut avoir disparu dans vos spams…

Changer le mot de passe d'un compte est habituellement facile mais ce nouveau mot de passe peut éventuellement créer quelques surprises inattendues:

- si il s'agit d'un compte Google, ce changement va avoir un impact sur votre Smartphone et/ou tablette Android, Google Home, Drive et autres applications liées à votre compte Google (Agenda, etc…).
- si il s'agit d'un compte DropBox, il faudra appliquer le nouveau mot de passe sur tous vos appareils où DropBox est installé.
- et de même pour d'autres applications…

Ne vous inquiétez pas, ces applications vous redemanderons le nouveau mot de passe.

Si vous avez oublié le mot de passe d'un site, tous proposent un lien "Mot de passe oublié" à utiliser puisque pour changer un mot de passe d'un compte, il faut d'abord s'y connecter…

C’est aussi un bon moment pour réfléchir à la gestion de vos mots de passe:

- comment ne pas les oublier
- comment générer des mots de passe robustes
- etc…

Le site Have I Been Pwned qui fournit toutes ces informations sur les piratages est l’œuvre d’une seule personne qui a du mal à suivre pour mettre son site à jour et cette personne vient donc de mettre son site en vente afin d’essayer de le pérenniser au vu de son utilité publique… Espérons que ce service si utile perdure dans le temps.

Enfin, si vous n’utilisez pas encore Firefox, je ne peux que vous conseiller de l’installer et de l’utiliser comme navigateur principal ou au moins de secours car il est beaucoup plus sûr et ne vous piste pas, je dirais même ne pille pas vos informations, comme le fait Google Chrome.
De plus si vous êtes utilisateur de Facebook, il existe une extension nommée Facebook Container dont je vous ai bien évidemment déjà parlé aussi et qui limite ce que Facebook peut récupérer sur votre PC tout en permettant une utilisation normale de Facebook; un must !
Je vous déconseille fortement d’utiliser Google Chrome qui, si il est bien facile d’utilisation, est sans doute le pire navigateur Internet sur le marché pour son côté collecte d’information qui ne regarde normalement que vous.
De plus, Firefox est un navigateur Open source ce qui signifie que son code source (le programme) est public et que tous le monde y compris les firmes spécialisées en sécurité et détection de pistage peuvent vérifier que ce code ne contient ni faille de sécurité ni de code malicieux.

Li P’ti Fouineu vous salue bien !