Protéger son site contre les attaques

Vous trouverez dans cet article, une série de **conseils pour vous aider à protéger votre sit**e. Nous nous basons sur un site réalisé avec le CMS WORDPRESS, mais ces règles s'appliquent aux autres CMS.

Nous ne mentionnons dans cet article que les opérations les plus simples à réaliser afin que le plus grand nombre puisse en bénéficier.

-  **Sauvegardez !**

  C'est évidemment la première étape et la seule totalement indispensable pour remettre votre site WordPress en activité après un piratage.

Les plugins de sauvegardes sont nombreux et efficaces et permettent très simplement de sauvegarder votre site de manière régulière et automatique :

– backwpup

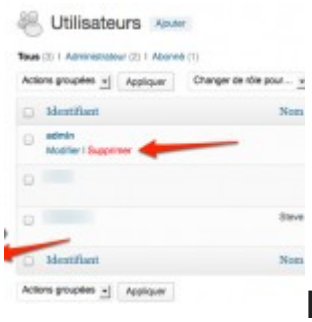
– updraftplus

Il vous appartient de télécharger régulièrement les sauvegardes et de les conserver sur un support externe. La fréquence des sauvegardes dépend de la fréquence de vos mises

à jour, vous pouvez par exemple faire une sauvegarde par mois ou par semaine.

Pour restaurer votre site il vous faudra un peu plus de compétences : maîtriser l'utilisation d'un logiciel ftp (filezilla) ainsi que de certaines procédures propres à votre hébergeur (par exemple chez l'hébergeur OVH : suivre le guide de procédure et fermeture pour hack OVH).

Quelles que soient vos compétences l'important est de sauvegarder, vous trouverez toujours quelqu'un avec les qualifications nécessaires à la remise en ligne de votre site.

- 

  Le compte admin

  Modifiez l'identifiant de votre compte qui permet l'accès à la gestion de votre site. Il est hors de question de laisser "Admin" comme identifiant et de faciliter la vie aux pirates. Choisissez un vrai mot de passe : des chiffres, des lettres, majuscules, minuscules, caractères spéciaux au moins 8 caractères.

- **Mettez votre wordpress ainsi que les plugins à jour.**

La plupart des sites qui se font hackés sont des sites qui n’ont pas été mis à jour depuis des mois, voire des années. Concernant les plugins, supprimez ceux dont vous ne vous servez plus de manière définitive, ne vous contentez pas de les désactiver.

- **Installer des plugins de sécurité.**

– restreindre les tentatives de connexion.
Par défaut, il est possible de tester autant de couples identifiant / mot de passe qu’on le souhaite. Le plugin “Limit Login Attempts” permet de restreindre le nombre de tentatives infructueuses de connexion et de bloquer l’utilisateur.

– Installez un antivirus
Wordfence est un plugin gratuit (avec une version payante premium) qui vous permet de protéger votre WordPress. La version gratuite comporte un firewall, un analyseur de virus et cheval de Troie.

- **Ajoutez un captcha à votre formulaire de contact**

  en plus d’éviter de recevoir des spams, le captcha renforce la protection contre certains types d’attaque.

- **Attention à ce que vous installez !**

  Les thèmes et plugin sont légion sur le net, préférez pour les plugins une installation à partir de wordpress et lors d’achat de plugin ou de thème payant bien lire les commentaires et les éventuels avis sur les problèmes rencontrés par les autres utilisateurs.

La protection de votre site WordPress est une démarche qui peut nécessiter du temps et qui peut aussi devenir complexe.

Les conseils donnés dans cet article vont vous aider à sécuriser à minima votre site, et de manière rapide et simple.

D’autres actions plus complexes peuvent également être envisagées pour renforcer encore cette protection (protéger des répertoires, le htaccess, …). Faites alors appel à votre agence web préférée !

Auteur: Renaud TAUPENAS