



Marc Giraud - Webdesigner/Formateur - WordPress

## Le Guide Ultime



## Blindez votre WordPress en 30 minutes

Le manuel de survie pour les propriétaires de sites qui détestent le code.

Bienvenue dans votre nouvelle zone de confort

Félicitations ! En téléchargeant ce guide, vous venez de faire plus pour votre sécurité que 80% des utilisateurs de WordPress.

Vous vous demandez peut-être : "Pourquoi moi ? Mon site est petit, je n'ai rien à voler." C'est l'erreur numéro 1. Les pirates ne sont pas des humains tapis dans l'ombre qui vous visent personnellement. Ce sont des robots (bots) qui frappent à toutes les portes. Ce guide est là pour leur montrer que chez vous, les verrous sont en acier trempé.

Prêt à devenir le garde du corps de votre propre business ? C'est parti !

## CHAPITRE 1 : La Stratégie de la "Terre Brûlée" Sauvegardes



Pourquoi est-ce vital ? Parce que le risque zéro n'existe pas. Votre serveur peut brûler, une mise à jour peut tout casser, ou vous pouvez faire une fausse manipulation. La Checklist de votre filet de sécurité :

**Externalisation** : Ne stockez jamais vos sauvegardes sur le même serveur que votre site. Si le serveur coule, le canot de sauvetage coule avec lui.

**Redondance** : Gardez toujours les 3 dernières versions de votre site.

**Test de restauration** : Une sauvegarde qui ne fonctionne pas au moment de la restauration ne sert à rien. Testez-la une fois par an !

**L'astuce de pro** : Utilisez UpdraftPlus. Configurez-le pour envoyer une copie sur votre Google Drive ou Dropbox chaque semaine automatiquement.

## CHAPITRE 2 : La Forteresse des Accès (Mots de passe et Connexion)



Le saviez-vous ? La majorité des piratages réussis passent par la "force brute" ( deviner votre mot de passe).

Comment rendre leur tâche impossible ?

**Tuez "Admin"** : Si votre identifiant est "admin", vous avez déjà donné 50% de la solution aux pirates. Créez un nouvel utilisateur avec un nom complexe, donnez-lui les droits d'administrateur, et supprimez l'ancien compte "admin".

**La Double Authentification (2FA)** : C'est l'arme absolue. Même avec votre mot de passe, personne ne rentre sans le code unique sur votre téléphone (utilisez l' application Google Authenticator).

**Masquez l'entrée** : Par défaut, l'entrée de votre site est votre-site.com/wp-admin. Utilisez l'extension WPS Hide Login pour la changer en quelque chose d'unique, comme /ma-porte-secrete.

## CHAPITRE 3 : Le Bouclier Actif (Sécurité par extension)



Installer une extension de sécurité, c'est comme engager un vigile qui ne dort jamais  
[Le duel des champions](#) :Wordfence vs Solid Securit

[Wordfence \(Le Scanner\)](#) : Il vérifie chaque fichier de votre site pour voir si un code malveillant s'y cache. Son pare-feu bloque les IP suspectes en temps réel.

[Solid Security \(Le Verrouilleur\)](#) : Il est excellent pour durcir WordPress (interdire l' édition de fichiers, bannir les utilisateurs trop insistants).

[Ma recommandation](#) : Commencez par Wordfence. La version gratuite est déjà extrêmement puissante pour un non-développeur.

## CHAPITRE 4 : L'Hygiène Numérique :Mises à jour

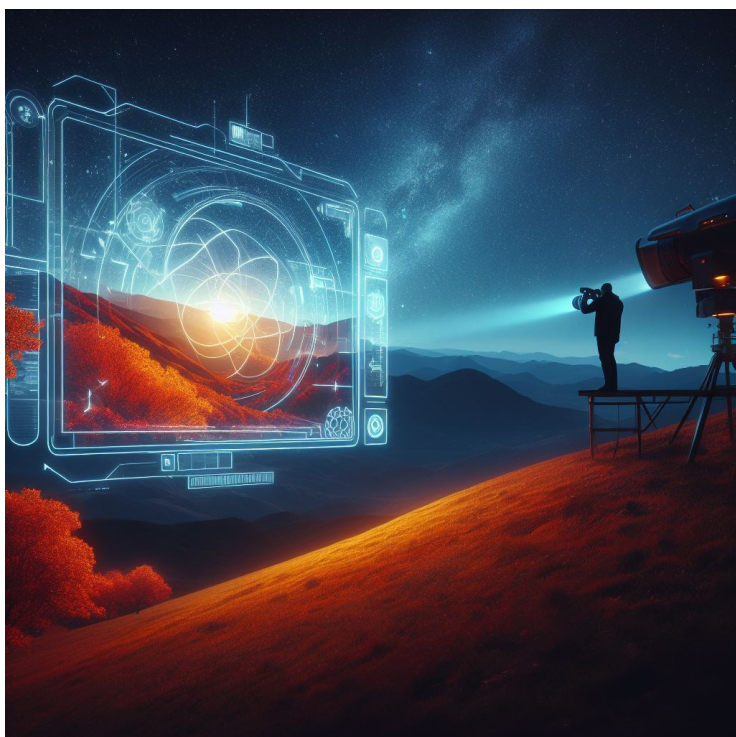
Un site à jour est un site difficile à hacker.  
Votre routine mensuelle de 5 minutes :

[Mettre à jour WordPress \(Cœur\)](#) : Pour les correctifs de sécurité critiques.

[Mettre à jour les Extensions](#) : Ne gardez que le strict nécessaire. Une extension inactive est une porte dérobée potentielle.

[Mettre à jour PHP](#) : Dans l'onglet "Santé du site" de WordPress, vérifiez que vous utilisez une version récente de PHP (le langage de votre site). C'est plus rapide et plus sûr !

Plan d'action immédiat (Votre To-Do List)



- J'ai installé un certificat SSL (HTTPS).
- J'ai fait une sauvegarde complète et je l'ai téléchargée sur mon PC.
- J'ai changé mon identifiant "admin" pour quelque chose d'unique.
- J'ai installé Wordfence et lancé mon premier scan.
- J'ai supprimé toutes les extensions que je n'utilise pas.

## Foire Aux Questions (FAQ)

**Q : Est-ce que mon site va devenir lent avec tout ça ?**

R : Non ! Une bonne extension de sécurité comme Wordfence est optimisée. Ce qui ralentit vraiment un site, ce sont les images trop lourdes ou un hébergement de mauvaise qualité.

**Q : Que faire si je reçois un mail disant que quelqu'un a essayé de se connecter ?**

R : Souriez ! Cela signifie que votre système de sécurité fait son travail et a bloqué l'intrus. Pas besoin d'agir si l'accès a été refusé.

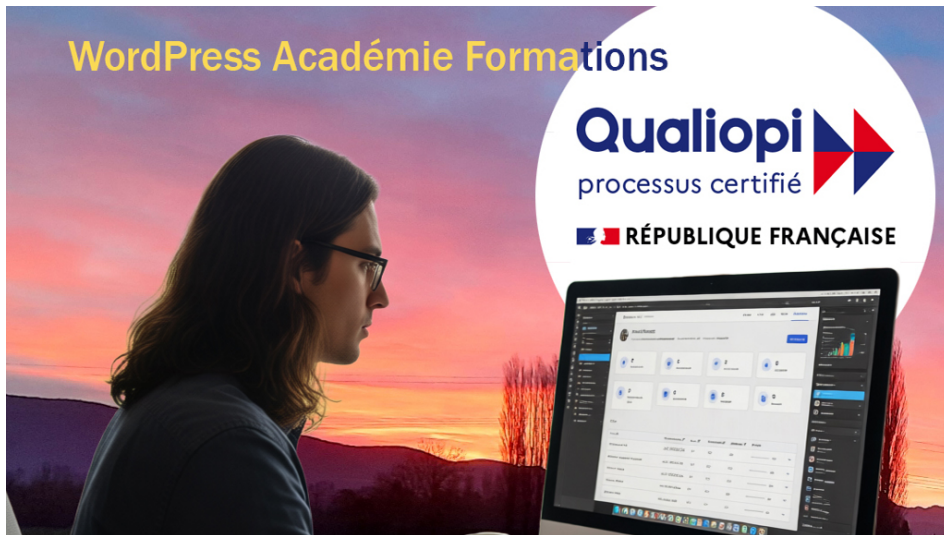
**Q : La sécurité totale existe-t-elle ?**

R : Non, mais le but est d'être plus difficile à hacker que votre voisin. Les pirates cherchent des cibles faciles. Avec ce guide, vous n'en êtes plus une.

## Le mot de la fin

Vous l'avez fait ! Votre site est désormais une forteresse. La sécurité n'est pas une destination, c'est un voyage. Restez curieux, gardez vos outils à jour, et votre business en ligne prospérera en toute sérénité.

Vous avez un doute ? Une question ? N'hésitez pas à me contacter sur webdesigner @marc-giraud.fr ou à rejoindre notre communauté pour plus de conseils !



### Prêt à passer au niveau supérieur ?

Vous venez de franchir une étape cruciale : votre site est désormais protégé contre 99% des menaces courantes. C'est un excellent début, mais la sécurité n'est que la fondation de votre empire numérique.

Voulez-vous arrêter de "bricoler" et commencer à maîtriser WordPress comme un véritable pro ? Que ce soit pour booster votre SEO, créer une boutique en ligne qui cartonne ou personnaliser votre design sans jamais toucher à une ligne de code, j'ai ce qu'il vous faut.

Transformez votre site en machine à résultats

Sur ma plateforme de formation, je vous accompagne pas à pas pour dompter le web, avec des méthodes simples, concrètes et garanties sans jargon technique.

[ 💎💎 Découvrir mes Formations WordPress: <https://www.formateurwordpress.marc-giraud.fr/>