STÉPHANIE VESTER

GUIDE PRATIQUE - WORDPRESS

CHECKLIST SÉCURITÉ WORDPRESS

10 étapes pour auditer et protéger votre site, à cocher au fil de vos vérifications.

10	35+	100%
étapes clés à vérifier	points de contrôle concrets	lié au guide complet en ligne

Chaque étape renvoie vers la section détaillée du guide complet sur mon site stephanie-vester.fr pour les explications, les portions de code et les recommandations de plugins.

Lors de la 1ère utilisation, je vous recommande d'utiliser l'article complet, plus détaillé.

POURQUOI CETTE CHECKLIST ?

Chaque jour, des milliers de sites WordPress sont piratés pour une seule raison : ils ne sont pas assez protégés. Au-delà du risque technique, sécuriser son site est aussi une obligation légale dès que vous stockez des données utilisateurs (conformité RGPD).

Cette checklist reprend, étape par étape, l'ensemble des vérifications du guide « Sécurité WordPress : le guide ultime en 10 étapes ». Cochez chaque point au fur et à mesure de votre audit, et cliquez sur les liens pour retrouver les explications détaillées, le code à copier-coller et les plugins recommandés.

> Comment l'utiliser : imprimez cette checklist ou gardez-la ouverte à côté de votre tableau de bord WordPress. Prévoyez 1 à 2 heures pour un premier passage complet, puis reprenez-la tous les 3 à 6 mois (étape 10).

1 CHOISIR L'HÉBERGEUR, LE THÈME ET LES PLUGINS

- [ ] Hébergeur fiable, avec support réactif et bonnes pratiques de sécurité (mutualisé, VPS, cloud ou dédié selon vos besoins et l'évolution de votre site depuis le dernier checkup sécurité)
- [ ] Thème actif, bien noté, mis à jour régulièrement et compatible avec la version de PHP de votre serveur
- [ ] Plugins peu nombreux (supprimez ceux inutiles), légers et activement maintenus par leur développeur
- [ ] Thème enfant utilisé pour toute personnalisation de code

Voir le détail de l'étape 1 →

2 BONNES PRATIQUES GÉNÉRALES DE SÉCURITÉ

- [ ] Nom d'utilisateur différent de « admin » et préfixe des tables de la base de données modifié
- [ ] Un compte par utilisateur, aucun identifiant ni mot de passe partagé
- [ ] Sauvegardes automatiques régulières (UpdraftPlus, Duplicator…) stockées sur un espace distant
- [ ] Sauvegarde manuelle systématique avant toute mise à jour ou modification risquée
- [ ] Mises à jour testées une par une (cœur, puis thème, puis plugins) avec vérification du site après chaque mise à jour
- [ ] Veille active sur les nouvelles failles de sécurité (newsletters officielles, médias spécialisés)

Voir le détail de l'étape 2 →

3 CHIFFREMENT DES DONNÉES (CERTIFICAT SSL)

- [ ] Certificat SSL installé (Let's Encrypt, gratuit, ou autre fournisseur de confiance)
- [ ] Trafic HTTPS forcé sur l'ensemble du site
- [ ] Mixed content corrigé : toutes les URL en http remplacées par des URL en https

Voir le détail de l'étape 3 →

4 INSTALLER UN PARE-FEU

- [ ] Pare-feu DNS et/ou applicatif (WAF) mis en place (Cloudflare, Wordfence, Sucuri, SecuPress…)
- [ ] Scan de malware programmé en analyse quotidienne
- [ ] Notifications par email activées en cas de menace détectée
- [ ] Protection contre les attaques par force brute et blocage des IP suspectes activés

Voir le détail de l'étape 4 →

5 PROTÉGER LE LOGIN & L'ADMINISTRATION

- [ ] Mots de passe forts et uniques pour tous les comptes
- [ ] Authentification à deux facteurs (2FA) activée
- [ ] Nom d'utilisateur masqué dans les pages auteur, les URL et le sitemap
- [ ] URL de connexion à l'administration déportée (hors /wp-admin par défaut)
- [ ] Nombre de tentatives de connexion limité

Voir le détail de l'étape 5 →

6 SÉCURISER LES FICHIERS SENSIBLES

- [ ] Accès au fichier wp-config.php bloqué via .htaccess
- [ ] Affichage du contenu des répertoires désactivé
- [ ] Permissions correctement réglées (dossiers en 755, fichiers en 644)
- [ ] Édition de fichiers depuis le tableau de bord WordPress désactivée (DISALLOW_FILE_EDIT)

Voir le détail de l'étape 6 →

7 AJOUTER LES HEADERS DE SÉCURITÉ

- [ ] Headers actuels vérifiés sur securityheaders.com
- [ ] Strict-Transport-Security (HSTS) ajouté
- [ ] X-Frame-Options et X-Content-Type-Options ajoutés
- [ ] Content-Security-Policy, Referrer-Policy et Permissions-Policy configurés

Voir le détail de l'étape 7 →

8 BLOQUER XML-RPC, PING ET L'API REST ANONYME

- [ ] Accès anonyme à l'API REST bloqué
- [ ] XML-RPC désactivé
- [ ] Pingbacks désactivés
- [ ] Blocages vérifiés en navigation privée (/wp-json/wp/v2/users)

Voir le détail de l'étape 8 →

9 SÉCURISER LES FORMULAIRES

- [ ] CAPTCHA actif sur chaque formulaire(reCAPTCHA, hCaptcha ou CAPTCHA mathématique)
- [ ] Entrées utilisateurs filtrées et validées (format email, longueur, balises HTML bloquées)
- [ ] Nombre de soumissions limité (anti-spam, délai minimum, blocage IP)
- [ ] Champs d'upload sécurisés (formats autorisés, taille limitée, stockage protégé)

Voir le détail de l'étape 9 →

10 SUIVRE CE GUIDE RÉGULIÈREMENT

- [ ] Checkup sécurité programmé tous les 3 à 6 mois dans votre agenda
- [ ] Pas de fausse sécurité : un certificat SSL seul ne suffit pas
- [ ] La sécurité traitée comme un processus continu, pas comme un état acquis

Voir le détail de l'étape 10 →

BESOIN D'AIDE POUR PASSER À L'ACTION ?

Si sécuriser votre site WordPress vous semble trop complexe ou si vous n'avez simplement pas le temps de vous en occuper, je peux m'en charger pour vous en prestation unique ou dans le cadre d'un contrat de maintenance.

Contactez-moi !

QUI SUIS-JE ?

Après 15 ans en tant que salariée en développement web full-stack, je suis devenue freelance développeuse web et consultante SEO en 2024.

J'accompagne les TPE & PME dans leur projet web, pour construire, maintenir, faire évoluer leur site et surtout, **bien le référencer**.
Plus qu'une simple vitrine, je fais en sorte qu'il devienne un véritable outil au service de votre marque, qui apporte des leads et des conversions.