



GUIDE GRATUIT

WordPress est-il sécurisé pour une entreprise ?

15 actions concrètes, les 5 failles les plus courantes et la procédure à suivre en cas de piratage — le guide complet pour protéger votre site professionnel.

Stéphane — SiteParSteph

Freelance WordPress en Alsace — Strasbourg · Haguenau · Kochersberg · Berstett

INTRODUCTION

Les statistiques qui font peur (et leur contexte)

La réponse courte : OUI, WordPress est sécurisé pour une entreprise — à condition d'être correctement maintenu. Les statistiques alarmistes existent, mais elles manquent cruellement de contexte.

LES CHIFFRES BRUTS

- ☐ Environ 30 000 sites sont piratés chaque jour dans le monde, tous CMS confondus (Source : Astra Security / Patchstack, 2026)
- ☐ 43 % de ces piratages ciblent des petites entreprises (Source : Astra Security, 2026)

LE CONTEXTE QUI CHANGE TOUT

- ☐ WordPress propulse 41,5 % du web mondial (Source : W3Techs, juillet 2026) → c'est une cible massive, pas une cible vulnérable
- ☐ **90 % des vulnérabilités WordPress viennent des plugins, 6 % des thèmes, 4 % seulement du cœur de WordPress** (Source : WPScan, 2026)
- ☐ Les sites piratés sont très majoritairement des sites négligés (aucune mise à jour depuis plusieurs mois)

C'est comme dire que les voitures sont dangereuses parce qu'il y a des accidents. La majorité des accidents sont liés à l'erreur humaine, pas à un défaut de fabrication.

Pourquoi WordPress est ciblé par les pirates

Volume : 41,5 % du web = retour sur investissement maximal pour les hackers. **Automatisation** : des bots scannent en masse les failles connues sur des millions de sites. **Plugins populaires** : une faille dans un plugin utilisé par 5 millions de sites = jackpot.

Négligence : beaucoup de sites sont « abandonnés » sans aucune maintenance.

Les 5 failles de sécurité les plus courantes

1 Plugins non mis à jour

Cause n°1 des piratages. Un plugin populaire non corrigé = une porte ouverte connue de tous les hackers. Solution : mises à jour hebdomadaires, suppression immédiate des plugins inutilisés.

2 Mots de passe faibles

« admin/admin123 » est encore trop fréquent. Un bot teste des milliers de combinaisons par heure. Solution : 12+ caractères, unique par compte, gestionnaire de mots de passe (Bitwarden, 1Password).

3 Hébergement bas de gamme

Un mutualisé surchargé sans isolation entre les sites : si un voisin se fait pirater, vous aussi. Solution : hébergeur professionnel avec isolation CloudLinux (O2Switch, OVH VPS).

4 Thèmes piratés (« nulled »)

Un thème premium téléchargé gratuitement = une backdoor incluse dans 90 % des cas. Économiser 50 € pour risquer 1 500 € de réparation. Solution : uniquement des sources officielles.

5 Pas de certificat SSL

Sans HTTPS, les données circulent en clair. Solution : HTTPS obligatoire, gratuit avec Let's Encrypt chez tous les bons hébergeurs.

15 actions pour sécuriser votre WordPress

La plupart sont configurables en 2 à 3 heures. Cochez au fur et à mesure.

- ☐ **1. Mises à jour hebdomadaires** — WordPress core + plugins + thème. Automatiser les mises à jour mineures.
- ☐ **2. Mots de passe forts** — 12+ caractères, majuscules, chiffres, symboles. Différent pour chaque compte.
- ☐ **3. Authentification 2FA** — Google Authenticator ou Authy. Plugin : WP 2FA.
- ☐ **4. Hébergement professionnel** — serveur en France, isolation entre comptes, support réactif.
- ☐ **5. Certificat SSL/HTTPS** — gratuit avec Let's Encrypt. Obligatoire en 2026.
- ☐ **6. Plugin de sécurité** — Wordfence (gratuit suffit pour 90 % des cas) ou iThemes Security.
- ☐ **7. Sauvegardes automatiques quotidiennes** — UpdraftPlus + stockage cloud externe.
- ☐ **8. Limitation des tentatives de connexion** — blocage après 3 à 5 échecs. Inclus dans Wordfence.

15 actions (suite)

- ☐ 9. **Supprimer l'utilisateur « admin »** — créer un autre compte administrateur, supprimer celui par défaut.
- ☐ 10. **Permissions fichiers correctes** — 644 pour les fichiers, 755 pour les dossiers, 400 pour wp-config.php.
- ☐ 11. **Désactiver l'éditeur de fichiers** — `define( 'DISALLOW_FILE_EDIT', true );` dans wp-config.php.
- ☐ 12. **Masquer la version WordPress** — évite de révéler une version potentiellement vulnérable.
- ☐ 13. **Scan malware régulier** — hebdomadaire minimum. Wordfence le fait automatiquement.
- ☐ 14. **Monitoring uptime** — alerte immédiate si le site tombe. Outil gratuit : UptimeRobot.
- ☐ 15. **Plan de réponse incident** — savoir exactement quoi faire si le site est piraté (checklist prête, voir page suivante).

Conseil SiteParSteph : appliquer ces 15 mesures couvre l'essentiel des risques courants. Nous les appliquons systématiquement sur tous nos projets en Alsace.

Plugins de sécurité recommandés

PLUGIN	PRIX	POUR QUI
Wordfence	0 €	90 % des PME — firewall, scan malware, blocage IP
Wordfence Premium	149 \$/an	E-commerce, données sensibles — scan temps réel
iThemes / Solid Security Pro	99 \$/an	Alternative à Wordfence — 2FA intégré
Sucuri	199,99 \$/an	Sites critiques — CDN sécurité, nettoyage inclus

Sources : wordfence.com, solidwp.com, sucuri.net (2026).

Pour la grande majorité des PME : Wordfence gratuit suffit. Passez en Premium uniquement pour les sites e-commerce qui gèrent des données sensibles.

Que faire si votre site est piraté ?

Procédure en 6 étapes.

- 1 Isoler immédiatement**
Mode maintenance ou blocage d'accès via .htaccess. Éviter la propagation.
- 2 Contacter l'hébergeur**
Il dispose souvent d'outils de détection et de nettoyage côté serveur.
- 3 Restaurer une sauvegarde propre**
Choisir une date AVANT l'infection. D'où l'importance des sauvegardes quotidiennes.
- 4 Scanner avec Wordfence ou Sucuri**
Identifier tous les fichiers infectés si aucune sauvegarde propre n'est disponible.
- 5 Changer TOUS les mots de passe**
WordPress, FTP, hébergement, base de données. Sans exception.
- 6 Tout mettre à jour**
WordPress, plugins, thème. Puis rescanner pour confirmer le nettoyage.

Ce que je constate le plus souvent : un site piraté après plusieurs mois sans mise à jour coûte presque toujours plus cher à réparer (jours hors ligne, perte de clients, remise en état) qu'une année complète de maintenance préventive.

Sauvegardes : votre filet de sécurité ultime

Les règles d'or des sauvegardes.

- ☐ **Fréquence** : quotidienne minimum, temps réel pour les sites e-commerce
- ☐ **Stockage** : EXTERNE, jamais sur le même serveur (Google Drive, Dropbox, Amazon S3)
- ☐ **Rétention** : 30 jours minimum d'historique
- ☐ **Test de restauration** : une fois par trimestre, vérifier que ça fonctionne réellement

Plugin recommandé : **UpdraftPlus** (gratuit pour l'usage basique, 70 €/an en premium pour plus d'options et de destinations de stockage).

Conseil SiteParSteph : une sauvegarde non testée n'est pas une sauvegarde. Nous testons la restauration une fois par trimestre sur tous nos contrats de maintenance.

En résumé

WordPress EST sécurisé — quand il est maintenu. L'écrasante majorité des piratages viennent de la négligence (plugins et thèmes non mis à jour), pas de failles intrinsèques au CMS. Les 15 mesures de ce guide couvrent l'essentiel des risques courants.



Pas le temps de gérer la sécurité vous-même ?

C'est exactement pour ça que la maintenance professionnelle existe. Pour 30 à 80 €/mois, dormez tranquille.

siteparsteph.fr/contact

Stéphane — SiteParSteph

Freelance WordPress en Alsace — Création, refonte et maintenance de sites professionnels