

MAINTENANCE & SÉCURITÉ WORDPRESS

Un site WordPress qu'on n'entretient plus est une porte qu'on laisse ouverte.

Comprendre pourquoi un site se dégrade, pannes techniques et piratage, ce qu'il faut surveiller, et comment le garder en bonne santé, mois après mois.

- ✓ Risques fréquents & plus rares
- ✓ Mécanisme du piratage
- ✓ Bonnes pratiques & FAQ

Piratage, panne : deux risques, pas toujours prévisibles.

Le plus souvent, cela commence par un oubli, ou un abandon, minuscule et presque invisible : une extension qu'on n'a pas mise à jour, un thème qu'on n'a pas remplacé, une version de PHP qu'on ne surveille plus. Rien ne se voit sur le site, et c'est bien le problème.



Des mises à jour de plugins ou extensions en retard

Chaque version corrige aussi des failles de sécurité déjà connues et rendues publiques.



Un plugin abandonné par son éditeur

Plus aucune mise à jour depuis longtemps : les failles découvertes après l'abandon ne seront jamais corrigées.



Une version de PHP obsolète

N'est plus corrigée au niveau sécurité : les failles découvertes après son abandon restent ouvertes, indépendamment du bon fonctionnement de vos extensions.



WordPress lui-même non mis à jour

Le cœur du site : une faille au niveau du cœur donne potentiellement accès à tout le reste.

PHP, c'est quoi ?

Le langage informatique qui fait fonctionner WordPress « sous le capot », un peu comme le moteur d'une voiture : invisible pour vous, mais indispensable. Comme toute technologie, il évolue avec le temps et doit être mis à jour régulièrement pour rester performant et sécurisé.

Chacun de ces oublis n'est pas un détail esthétique : c'est une porte laissée entrouverte. Elle peut mener à une simple panne, ou à un piratage. Voici, concrètement, ce que ça donne dans les deux cas.

Les risques les plus fréquents

Panne ou piratage : voici ce qui arrive le plus souvent à un site WordPress livré à lui-même, par ordre approximatif de fréquence.



Une mise à jour casse le site

Plugin, thème, constructeur de page (Elementor, Divi) ou WordPress incompatibles entre eux.



Plugin abandonné par son éditeur

Ses failles ne seront plus jamais corrigées.



Version PHP obsolète

Incompatible avec WordPress ou les extensions récentes.



Piratage via une faille connue

Injection de code, spam SEO, redirections, vol de données.



Sauvegarde absente ou trop ancienne

On le découvre souvent trop tard : le jour où on en a vraiment besoin.



Certificat SSL expiré

« Connexion non sécurisée » : la confiance chute d'un coup, et les données échangées ne sont plus chiffrées.



Site de plus en plus lent

Base de données surchargée, images non optimisées, pas de cache.



Formulaire de contact cassé

Des demandes perdues, en silence, sans que personne ne le sache.



Conflit entre deux extensions

La mise à jour de l'une casse le fonctionnement de l'autre.



Erreur humaine

Suppression accidentelle, mauvaise manipulation dans l'éditeur.

PLUS RARES, MAIS RÉELS



Ransomware

Le site est chiffré et rendu inaccessible, contre rançon.



Attaque DDoS (saturation)

Le site est submergé de requêtes et devient injoignable.



Nom de domaine expiré

Renouvellement oublié : le site et les emails disparaissent d'un coup.



Dépendance à un seul prestataire

Lui seul détient les accès : en cas d'indisponibilité, plus personne ne peut intervenir.

D'où vient vraiment le piratage, et qui a les clés

Deux angles morts fréquents, au-delà des mises à jour manquées : comment le piratage entre, et qui a encore accès au site.

COMMENT ÇA ENTRE



Thèmes et plugins « nulled » (piratés)

Des copies gratuites d'extensions premium, téléchargées hors du dépôt officiel. Elles embarquent très souvent un malware caché dès l'installation.



Licence premium expirée

Différent d'un plugin abandonné : l'éditeur corrige toujours les failles, mais sans licence renouvelée, votre copie ne reçoit plus ces correctifs.



Un hébergement partagé sans isolation

Chez un hébergeur sérieux, chaque compte est isolé des autres : ce risque reste rare. Il redevient réel quand plusieurs sites de clients différents tournent ensemble sous un seul compte, chez un freelance ou une agence, sans séparation entre eux.

QUI A ENCORE LES CLÉS



Des accès jamais révoqués

Un ancien prestataire ou une ancienne personne de l'équipe garde un accès administrateur ou hébergement, bien après la fin de la collaboration.



Trop de comptes administrateur

Chaque compte « administrateur » est une porte potentielle. La plupart n'ont besoin que d'un accès limité à leur usage réel.



Pas de politique de mots de passe

Un mot de passe faible ou réutilisé ailleurs, sans double authentification (2FA), reste l'une des façons les plus simples d'entrer : pas besoin de faille technique si la porte est mal verrouillée.

En clair : une faille corrigée ne sert à rien si quelqu'un garde un accès qu'il ne devrait plus avoir.

Anatomie d'un piratage WordPress

Une faille non corrigée ne se traduit pas immédiatement par un site visiblement piraté. Voici, étape par étape, ce qui se passe entre les deux.

**La mise à jour n'est pas une question d'esthétique.
C'est une question de sécurité.**

1

Une faille reste ouverte

Extension, thème, PHP ou WordPress non mis à jour : la vulnérabilité est connue et publiée dans des bases de failles accessibles à tous.

2

Injection silencieuse

La faille est exploitée pour injecter du code malveillant. Rien ne change visuellement sur le site, ni pour vous, ni pour vos visiteurs.

3

Un kit de piratage s'installe, invisible

Il se loge hors du dossier « Extensions » : vous ne le verrez pas en consultant la liste des plugins depuis le tableau de bord.

4

Il se multiplie pour résister au nettoyage

Le kit crée plusieurs copies dans différents dossiers WordPress. Supprimez-en une, une autre la réinstalle automatiquement.

5

Un compte administrateur fantôme apparaît

Le kit peut créer un compte admin invisible dans la liste des utilisateurs, donnant un accès total et permanent au site.

6

Le site est exploité

Vol de données personnelles, ou publication de centaines d'articles pour profiter de votre référencement et rediriger vers d'autres sites.

Conséquence fréquente : un site qui publie du spam se retrouve **sur la liste noire de Google**. Le retour dans les résultats de recherche prend souvent des semaines, même après nettoyage.

Ce que ça coûte réellement

Un piratage n'est jamais qu'un problème technique. Il se traduit vite en pertes concrètes, parfois durables.



Indisponibilité

Commandes et demandes perdues : pendant l'indisponibilité, votre site n'existe tout simplement pas pour les visiteurs, qui ne reviennent pas toujours ensuite.



Perte de données

Comptes clients, commandes, articles ou commentaires enregistrés depuis la dernière sauvegarde peuvent disparaître.



Référencement (SEO)

Un site utilisé pour publier du spam peut être mis sur liste noire par Google. Il faut souvent plusieurs semaines pour revenir, même après nettoyage.



Responsabilité légale (RGPD)

Un vol de données clients oblige à prévenir la CNIL sous 72h, et les clients concernés si le risque est élevé. Des sanctions sont possibles.



Image de marque

Un site à l'abandon (visuellement daté, erreurs affichées) inspire moins confiance, même sans incident avéré.



Communication coupée, sans le savoir

Un formulaire cassé ou un serveur piraté qui envoie du spam : vos vrais emails professionnels (devis, factures) finissent bloqués ou en spam chez vos clients.

Bilan : une maintenance mensuelle coûte presque toujours moins cher que quelques heures de dépannage en urgence.

Bonnes pratiques : ce qu'il faut faire, régulièrement

Rien de sophistiqué : des habitudes simples, tenues dans la durée, ferment la quasi-totalité des portes ouvertes par négligence.



Mettre à jour tous les plugins et extensions

Sans les laisser s'accumuler pendant des mois, en priorité quand la mise à jour corrige une faille de sécurité.

Hebdomadaire



Surveiller les plugins abandonnés

Aucune mise à jour depuis trop longtemps ? Prévoir son remplacement avant que ça devienne une faille.

Mensuel



Vérifier la version PHP

À jour et compatible avec la version de WordPress et des extensions installées.

Semestriel



Mettre à jour WordPress

Dès qu'une nouvelle version est publiée, cœur du site compris.

Dès parution



Vérifier le SSL et le nom de domaine

Un certificat expiré ou un domaine non renouvelé peuvent rendre le site inaccessible du jour au lendemain. Le certificat se vérifie plus souvent, le renouvellement du domaine reste lui annuel.

Trimestriel



N'installer que des extensions et thèmes officiels

Jamais de version « nulled » (piratée) téléchargée hors du dépôt officiel ou de l'éditeur : elle embarque souvent un malware dès l'installation.

À l'installation



Passer en revue les accès existants

Comptes utilisateurs, accès hébergement et FTP : révoquer ce qui n'est plus justifié, notamment après la fin d'une collaboration.

Semestriel



Surveiller les vulnérabilités connues des extensions

Via un service de veille (type Patchstack ou WPScan) qui signale une faille dès sa publication, avant même la mise à jour du correctif.

Continu



Vérifier que les emails du site sont bien délivrés

Un envoi de test (formulaire de contact, commande) permet de s'assurer qu'ils n'atterrissent pas en spam ou nulle part.

Trimestriel

Se prémunir avant que ça arrive

Les bonnes pratiques réduisent le risque. Ces précautions limitent les dégâts le jour où, malgré tout, un problème survient.



Mettre en place des sauvegardes régulières

Idéalement quotidiennes, et stockées ailleurs que sur le serveur d'origine : si le site est piraté ou si le serveur tombe en panne, une sauvegarde conservée au même endroit peut être perdue ou inaccessible, juste au moment où vous en avez besoin.



Tester régulièrement le site

Pas seulement le mettre à jour : vérifier qu'il fonctionne toujours, pages clés comprises. Un exemple courant : deux extensions parfaitement saines chacune se mettent à jour, mais leur nouvelle combinaison provoque un petit bug d'affichage ou de fonctionnement que seul un vrai coup d'œil permet de repérer.



Activer la double authentification (2FA)

Et sécuriser l'accès à wp-admin : mots de passe robustes, limitation des tentatives de connexion. Protégez également la boîte mail liée à votre compte administrateur avec un mot de passe unique et la double vérification.



Surveiller les comptes utilisateurs

Repérer tout compte inconnu ou avec des droits administrateur que vous n'avez pas attribués.



Surveiller les comportements inhabituels

Nouveaux fichiers, ralentissements soudains, redirections ou pages inconnues qui apparaissent.

Trois pièges fréquents

La maintenance n'est pas qu'une question de sécurité contre le piratage : mal comprise, elle peut créer ses propres problèmes.

A Une mise à jour peut, elle-même, mettre le site hors ligne

Une mise à jour d'extension ou de WordPress peut provoquer une erreur fatale et rendre le site inaccessible. Vous n'êtes pas forcément averti : sans vérification régulière, un site tombé peut le rester longtemps, sans que vous vous en rendiez compte.

B Les mises à jour automatiques ne suffisent pas seules

Automatiser les mises à jour réduit la charge, mais en cas d'erreur fatale sans notification, le site devient indisponible sans qu'on sache quelle mise à jour est en cause, faute de suivi humain derrière l'automatisation.

C Restaurer via la sauvegarde ne récupère pas toujours tout

Une sauvegarde permet de restaurer le site après une erreur fatale. Mais toute donnée créée entre la sauvegarde et l'incident (nouveau compte client, commande, article, commentaire) sera perdue si l'on restaure purement et simplement. Selon les besoins du site, faire appel à un webmaster pour dépanner sans restaurer permet parfois de corriger le problème sans perdre ces données récentes.

Concrètement : un outil automatisé ne sait pas choisir entre restaurer, réparer, ou dépanner sans perdre de données. Un suivi humain, oui.

D'autres pièges à connaître

Moins évidents que les trois premiers, mais tout aussi coûteux quand on les découvre trop tard.

D Le plugin gratuit d'aujourd'hui n'est pas garanti demain

Beaucoup d'extensions gratuites existent pour attirer vers une version premium : l'éditeur peut réduire ou arrêter le support de la version gratuite du jour au lendemain.

E Nettoyer sans corriger la faille ne règle rien durablement

Si on supprime le code malveillant sans corriger la vulnérabilité d'origine, le site peut être réinfecté en quelques jours : le kit de piratage sait souvent se réinstaller.

F Toutes les sauvegardes ne se valent pas

Sauvegarder les fichiers sans la base de données (ou l'inverse) rend une restauration complète impossible.

G Le moins cher n'est pas toujours le plus sûr

Chez un hébergeur sérieux, les comptes sont correctement isolés les uns des autres : ce risque est rare. Il redevient réel lorsque plusieurs sites de clients différents sont hébergés ensemble sous un seul compte, sans séparation entre eux : une faille sur l'un peut alors, dans certains cas, atteindre les fichiers des autres. Un peu comme des voisins qui partageraient la même clé pour plusieurs appartements.

H Une mise à jour appliquée n'est pas synonyme de vérifiée

Même avec un outil qui automatise et confirme la mise à jour technique, personne ne remplace un vrai coup d'œil humain : l'outil sait que la mise à jour s'est installée, pas si le formulaire de contact ou le panier fonctionnent toujours pour un vrai visiteur.

I La sécurité n'est jamais acquise une fois pour toutes

Un audit fait aujourd'hui décrit l'état du site aujourd'hui, pas dans six mois : un nouveau plugin installé entre-temps, ou une faille tout juste découverte sur une extension jusque-là saine, suffisent à rouvrir une porte. Comme un contrôle technique de voiture : valable au moment du contrôle, pas une garantie contre la panne future.

FAQ : ce qu'on me demande souvent

Q Mon hébergeur ne s'occupe-t-il pas déjà de la sécurité ?

Non : l'hébergeur sécurise le serveur, pas votre WordPress. Plugins, thème, comptes et contenu restent de votre ressort. Ce sont deux niveaux différents.

Q Puis-je faire les mises à jour moi-même ?

Oui, techniquement. La difficulté n'est pas la compétence, c'est la régularité : y penser chaque semaine, vérifier que rien n'est cassé, corriger si besoin.

Q Combien de temps pour remettre en état un site piraté ?

Ça dépend de la profondeur de l'infection et de la disponibilité d'une sauvegarde saine : de quelques heures à plusieurs jours si tout est à reconstruire. Cela dépend aussi de l'état d'entretien du site : si la dernière intervention remonte à plus de 5 ans, nettoyer le site peut coûter plus cher que reconstruire un site neuf.

Q Et si mon site est piraté malgré une maintenance en place ?

Le risque zéro n'existe pas. Mais un suivi régulier permet de détecter et corriger bien plus vite, avant que les dégâts ne s'aggravent.

Q Une sauvegarde suffit-elle à me protéger ?

Elle protège contre la perte de données, pas contre le piratage lui-même. Et surtout, si elle a été faite après l'infection, le kit de piratage peut déjà s'y trouver aussi : restaurer sans corriger la faille d'origine ne suffit pas. Il faut la prévention en plus : mises à jour, surveillance, protection active.

Q Mon site n'a pas été mis à jour depuis longtemps, par où commencer ?

Par un état des lieux : selon le cas, une remise à niveau pour le remettre à jour en sécurité, ou un audit complet. Ensuite, un suivi régulier.

Q Qu'est-ce qu'un plugin ou thème « nulled » (piraté) ?

Une copie piratée d'une extension premium, distribuée gratuitement hors des canaux officiels. Elle embarque très souvent un malware caché dès l'installation.

Q Panne ou piratage : comment faire la différence ?

Une panne suit en général une action identifiable (mise à jour, modification). Un piratage n'a souvent aucun déclencheur visible, mais s'accompagne de signes indirects : nouveaux comptes, redirections, ralentissement. Un premier diagnostic, gratuit, permet de trancher.

Une maintenance WordPress, sans y penser

Jorboo prend en charge tout ce qui précède, chaque mois : mises à jour, sauvegardes, surveillance et intervention en cas de pépin.

Maintenance Essentielle

Votre site tourne, à jour et protégé.

39€ HT / mois
sans engagement

- ✓ Mises à jour WordPress, thèmes et plugins
- ✓ Sauvegardes quotidiennes, hébergées à l'extérieur
- ✓ Surveillance et monitoring 24h/24
- ✓ Protection contre les vulnérabilités connues (Patchstack)
- ✓ Intervention en cas d'incident lié à une mise à jour
- ✓ Rapport mensuel détaillé

Maintenance Pro

LE PLUS CHOISI

La tranquillité, plus un coup de main chaque mois.

59€ HT / mois
sans engagement

- ✓ **Toute Essentielle** : mises à jour, sauvegardes, surveillance, protection, intervention, rapport
- ✓ Nettoyage et optimisation de la base de données
- ✓ 1h de support mensuelle : modifications, ajustements, corrections

Maintenance E-commerce

La sécurité maximale pour votre boutique en ligne.

79€ HT / mois
sans engagement

- ✓ **Tout Pro inclus** : mises à jour, surveillance, 1h de support
- ✓ Sauvegardes toutes les heures, pour limiter au maximum le risque de perte de commandes
- ✓ Vérification régulière du tunnel d'achat (panier, paiement)
- ✓ Formule pensée pour les sites WooCommerce

Les heures de support mensuelles incluses dans les formules Pro et E-commerce ne sont ni cumulables ni reportables sur le mois suivant.

Besoin d'un audit ponctuel, sans maintenance mensuelle ? Il démarre à 190 € HT. Écrivez-moi, on en parle.

Écrivez-moi votre situation

Réponse sous 24h ouvrées, 100 % par écrit, sans engagement.

contact@jorboo.fr

06 86 88 34 44

SMS / WhatsApp uniquement