Sécurité, Maintenance

Site WordPress en 2026 Les risques d'un site non maintenu

Un site qui s'affiche correctement n'est pas forcément un site sain. Extensions vulnérables, PHP dépassé, sauvegardes jamais testées, accès oubliés : voici ce qui se passe en coulisses.

Publié le 8 mai 2026

Ce qu'il faut retenir de ce dossier

Un site WordPress non maintenu peut continuer à s'afficher correctement tout en accumulant des risques invisibles : extensions vulnérables, thème obsolète, version PHP en fin de vie, sauvegardes non testées, formulaires défaillants, lenteurs, erreurs SEO ou incompatibilités avec WooCommerce.

L'enjeu n'est pas de mettre à jour "pour mettre à jour", mais de conserver un site fiable, restaurable et exploitable. Pour une PME, le bon repère est simple : si personne ne sait répondre précisément à la date de la dernière sauvegarde testée, aux extensions critiques utilisées, aux comptes administrateurs actifs et à la version PHP en production, le site n'est probablement pas correctement maintenu.

Les chiffres 2025-2026 confirment l'urgence : 11 334 nouvelles vulnérabilités ont été découvertes dans l'écosystème WordPress en 2025 (+42 % en un an), et le délai médian entre la publication d'une faille et son exploitation massive par des robots automatisés est désormais de seulement 5 heures.

Un site qui fonctionne n'est pas forcément un site sain

Un site peut sembler parfaitement normal côté visiteur tout en étant fragile côté administration. C'est même l'une des difficultés principales avec WordPress : l'absence de panne visible donne souvent l'impression que tout va bien.

En réalité, un site non maintenu accumule des écarts techniques au fil du temps : versions anciennes, extensions abandonnées par leur développeur, thème non suivi, base de données encombrée par des révisions, formulaires qui ne délivrent plus les emails, sauvegardes jamais testées, dépendances PHP incompatibles, comptes utilisateurs oubliés.

Un actif numérique, pas un simple outil

Pour une PME, le site web est souvent le premier point de contact commercial. Une indisponibilité, une compromission ou une perte de données peut avoir des conséquences directes sur le chiffre d'affaires, la relation client et la réputation de l'entreprise.

Trois questions pour commencer

- Qui est responsable de la maintenance de votre site aujourd'hui ?
- Quelle est la date de la dernière sauvegarde testée et restaurée avec succès ?
- Combien de temps votre activité peut-elle fonctionner sans site ni messagerie ?

Les failles de sécurité et le problème des 5 heures

WordPress propulse plus de 43 % de l'ensemble des sites web mondiaux en 2026. Cette popularité en fait la cible numéro un des attaques automatisées : des robots parcourent en permanence Internet à la recherche de signatures connues de versions vulnérables.

Le rapport annuel Patchstack 2026 dresse un constat sans appel sur l'état de la sécurité WordPress.

Ce dernier chiffre est particulièrement important : le délai médian de 5 heures signifie que l'attente de la prochaine maintenance mensuelle pour appliquer une mise à jour critique n'est plus une stratégie viable. Pour les vulnérabilités les plus ciblées, 45 % sont exploitées dans les 24 premières heures suivant leur divulgation publique.

Par ailleurs, 46 % des vulnérabilités n'avaient pas de correctif disponible au moment de leur publication. Le développeur de l'extension n'avait tout simplement pas livré de mise à jour. Dans ce cas, aucune mise à jour ne peut être appliquée.

Ce que les attaquants laissent derrière eux :

après compromission, les attaques laissent fréquemment des fichiers malveillants, des portes dérobées et du spam SEO injecté. Ces traces peuvent rester actives après un nettoyage partiel et provoquer une réinfection ou une dégradation de la visibilité du site.

Visuel de contenu à créer : image-site-wordpress-2026-risques-securite.webp

Infographie recommandée : timeline "De la faille à l'exploitation" avec les étapes 0h (divulgation), 5h (exploitation médiane), 24h (45 % des sites ciblés), 30j (maintenance mensuelle habituelle).

Les extensions abandonnées ou trop nombreuses

Une extension ajoute une fonctionnalité, mais aussi une dépendance. Plus un site contient d'extensions, plus il faut suivre de mises à jour, de compatibilités, de conflits possibles et de risques de sécurité. L'installation WordPress moyenne tourne avec entre 20 et 30 extensions actives.

Le danger n'est pas uniquement le nombre d'extensions. Il faut surtout distinguer plusieurs catégories à risque :

?Extensions désactivées mais présentes

Un plugin désactivé mais toujours présent dans le dossier wp-content/plugins peut toujours être exploité directement via une requête HTTP. Le bon réflexe est de le supprimer totalement.

?Extensions abandonnées

Un plugin qui n'a pas reçu de mise à jour depuis plus d'un an et dont le développeur ne répond plus aux signalements de sécurité est une bombe à retardement.

?Extensions critiques non surveillées

Les extensions de paiement, de formulaires, de sécurité, de cache, de SEO et d'e-commerce doivent être suivies en priorité. Une faille sur WooCommerce Payments est bien plus critique qu'une faille sur un widget de réseaux sociaux.

?Extensions premium sur marketplaces

Les extensions payantes reçoivent moins de scrutin de la part des chercheurs en sécurité. En 2025, 76 % des vulnérabilités trouvées dans les composants premium étaient exploitables en conditions réelles.

Lien interne à prévoir

Ce sujet sera développé dans le dossier dédié : "Trop d'extensions WordPress : à partir de quand cela devient dangereux ?"

Les mises à jour faites sans méthode

Ne pas mettre à jour est dangereux, mais mettre à jour sans méthode peut aussi casser un site. WordPress recommande explicitement de sauvegarder le site avant toute mise à jour afin de pouvoir restaurer en cas de problème.

Les mises à jour mineures et de sécurité du cœur WordPress peuvent être automatisées (elles le sont par défaut depuis WordPress 3.7). En revanche, les mises à jour majeures, celles de WooCommerce, des constructeurs de pages (Elementor, Divi) ou des extensions critiques doivent être testées.

Un vrai processus de maintenance devrait comprendre les étapes suivantes :

- 1Sauvegarde complète avant interventionFichiers, base de données, médias et configurations. La sauvegarde doit être stockée hors du serveur de production.
- 2Vérification de compatibilitéContrôler la compatibilité entre la version de WordPress cible, la version PHP du serveur et les extensions critiques.
- 3Mise à jour et test visuelVérifier l'affichage des pages principales, du menu, du pied de page et des éléments dynamiques.
- 4Test des formulairesEnvoyer un message de test depuis chaque formulaire de contact, de devis ou d'inscription et vérifier la réception.
- 5Test du tunnel WooCommercePour les boutiques : tester le panier, le processus de commande, les emails transactionnels et les notifications.
- 6Procédure de retour arrière documentéeEn cas de problème, savoir exactement comment restaurer la sauvegarde en moins de 30 minutes.

Une version PHP dépassée : sécurité, compatibilité et performances

WordPress dépend du langage PHP pour fonctionner. Une version PHP ancienne pose trois problèmes simultanés : sécurité (absence de correctifs), compatibilité (extensions modernes qui refusent de fonctionner) et performance (les versions récentes de PHP sont significativement plus rapides).

Version PHP	Statut en juillet 2026	Recommandation
PHP 7.x et antérieur	Fin de vie depuis 2022	Migration urgente, aucun correctif de sécurité.
PHP 8.0	Fin de vie depuis nov. 2023	Migration urgente, aucun correctif de sécurité.
PHP 8.1	Fin de vie depuis déc. 2025	Migration nécessaire, plus de support officiel.
PHP 8.2	Supporté jusqu'à déc. 2026	Acceptable à court terme, planifier la migration.

PHP 8.3 | Supporté jusqu'à déc. 2027 | Version recommandée et stable pour WordPress.

PHP 8.4 | Supporté jusqu'à déc. 2028 | Version actuelle recommandée si le site, le thème et les extensions sont compatibles.

PHP 8.5 | Supporté jusqu'à déc. 2029 | À envisager uniquement après vérification de compatibilité WordPress, thème et extensions.

Pour une PME, cela signifie que la maintenance ne doit pas se limiter au tableau de bord WordPress. Elle doit inclure l'environnement d'hébergement : version PHP, base de données (MySQL/MariaDB), certificats SSL, permissions des fichiers, configuration du cache serveur et journaux d'erreurs.

Comment vérifier sa version PHP ?

Dans le tableau de bord WordPress, aller dans Outils -> Santé du site. La version PHP en production est affichée dans la section "Informations". Si elle est inférieure à 8.2, contacter l'hébergeur pour planifier la migration.

Les sauvegardes qui n'ont jamais été testées

Avoir une sauvegarde n'est pas suffisant. Il faut savoir si elle est complète, récente, accessible et surtout restaurable. L'ANSSI recommande les sauvegardes régulières comme une règle de base absolue de sécurité numérique, et précise qu'elles doivent être réalisées sur des supports distincts et testées.

Dans le cas d'un site WordPress, la sauvegarde doit impérativement couvrir l'ensemble des éléments suivants :

?Fichiers et médias

Le cœur WordPress, les thèmes, les extensions et le dossier wp-content/uploads contenant toutes les images et documents.

?Base de données

L'intégralité du contenu : articles, pages, réglages, utilisateurs, commandes WooCommerce et données de formulaires.

?Configurations spécifiques

Réglages du thème, configurations d'extensions, personnalisations CSS, fichiers .htaccess et wp-config.php.

?Données WooCommerce

Commandes, comptes clients, historique d'achats, stocks. Pour un e-commerce actif, la sauvegarde doit être quotidienne ou plus fréquente.

La règle des 3-2-1

Trois copies des données, sur deux supports différents, dont une copie hors site (cloud ou serveur distant). Une sauvegarde stockée uniquement sur le même serveur que le site sera perdue en même temps que le site en cas d'incident serveur.

Lien interne à prévoir

Ce sujet sera développé dans le dossier dédié : "Sauvegardes web : pourquoi une sauvegarde n'est utile que si elle est restaurable."

Les formulaires, emails et notifications qui ne fonctionnent plus

Un site peut rester visible tout en cessant de transformer. C'est l'un des problèmes les plus fréquents et les plus silencieux : les formulaires n'envoient plus correctement les emails, les notifications WooCommerce arrivent en spam ou disparaissent, un changement de serveur ou d'hébergeur a modifié la délivrabilité sans que personne ne s'en aperçoive.

Les causes sont souvent techniques : absence de configuration SMTP dédiée, enregistrements DNS (SPF, DKIM, DMARC) manquants ou mal configurés, adresse IP de l'hébergeur sur liste noire, ou extension de formulaire incompatible avec une mise à jour récente.

Les conséquences sont très concrètes pour le chiffre d'affaires : demandes de devis perdues, commandes non suivies, inscriptions non confirmées, messages clients invisibles pendant des semaines. La maintenance doit donc inclure des tests fonctionnels réguliers, pas seulement des mises à jour techniques.

Tests à effectuer régulièrement

- • Envoyer un message de test depuis chaque formulaire de contact et vérifier la réception dans la boîte mail de destination.
- • Passer une commande test sur WooCommerce et vérifier les emails de confirmation client et administrateur.
- • Vérifier que les emails ne tombent pas en spam (tester avec un outil comme Mail Tester).
- • Contrôler les journaux d'envoi d'emails si un plugin SMTP est utilisé.

Les performances qui se dégradent avec le temps

Un site WordPress peut devenir lent progressivement, sans qu'aucune alerte ne soit déclenchée : images trop lourdes non optimisées, base de données encombrée par des milliers de révisions d'articles, extensions ajoutées successivement sans audit, cache mal configuré, thème trop chargé, scripts tiers nombreux (publicités, trackers, widgets).

La lenteur n'est pas seulement un sujet de confort utilisateur. Elle a des conséquences mesurables sur trois plans :

?SEO et référencement

Google recommande fortement de bons scores Core Web Vitals, car ces signaux sont alignés avec l’expérience de page que ses systèmes de classement cherchent à récompenser. Un site lent peut donc fragiliser sa visibilité, en particulier si l’expérience mobile est dégradée.

?Conversion et ventes

Dans le e-commerce, la lenteur peut dégrader l’expérience utilisateur et réduire les conversions, en particulier sur mobile. L'impact peut devenir direct sur le chiffre d'affaires.

?Image de marque

Un site lent ou instable renvoie une image non professionnelle. Pour un visiteur, la qualité du site reflète la qualité de l'entreprise.

Repère pratique :

l'outil gratuit Google PageSpeed Insights permet de mesurer les performances d'un site et d'identifier les points d'amélioration prioritaires. Un score inférieur à 50 sur mobile est un signal d'alerte fort.

La perte de maîtrise des accès

Un site ancien accumule des comptes au fil des années : anciens prestataires, agences web précédentes, comptes administrateurs partagés entre plusieurs personnes, utilisateurs de test créés lors d'un développement, comptes d'anciens employés non supprimés, accès FTP transmis par email et jamais révoqués.

La documentation officielle WordPress recommande des mesures de durcissement (hardening) : limitation stricte des accès administrateurs, application du principe de moindre privilège (chaque utilisateur n'a que les droits nécessaires à sa mission), utilisation de mots de passe forts et de la double authentification (MFA).

Type d'accès	Risque principal	Action recommandée
Comptes administrateurs WordPress	Prise de contrôle totale du site	Inventaire, suppression des comptes inutilisés, MFA obligatoire.
Accès FTP / SFTP	Modification ou suppression de fichiers	Révoquer les accès des anciens prestataires, utiliser SFTP uniquement.
Accès hébergement (cPanel, Plesk)	Accès à toutes les données et sauvegardes	Mots de passe uniques et forts, MFA si disponible.
Accès registrar (nom de domaine)	Détournement du domaine, perte totale du site	Sécuriser avec MFA, vérifier les contacts administratifs.
Comptes éditeurs / auteurs	Publication de contenu non autorisé	Supprimer les comptes inactifs, vérifier les rôles attribués.

Checklist dirigeant : 8 questions à poser dès maintenant

Visuel de contenu à créer : image-site-wordpress-2026-checklist.webp

Checklist visuelle recommandée : 8 cases à cocher avec pictogrammes sobres et colonnes "Question" / "Ce qu'il faut savoir".

Question	Ce qu'il faut savoir
Qui maintient réellement le site ?	Nom du prestataire ou du responsable interne désigné. Si la réponse est floue, c'est un signal d'alerte.
Quelle est la date de la dernière sauvegarde testée ?	Pas seulement la date de sauvegarde automatique, mais la date du dernier test de restauration réel.
Les extensions critiques sont-elles identifiées ?	Paiement, formulaires, sécurité, SEO, cache. Ces extensions doivent être surveillées en priorité.
La version PHP est-elle compatible et maintenue ?	À vérifier dans Outils -> Santé du site. Minimum PHP 8.2, recommandé PHP 8.3 ou supérieur en 2026.
Les comptes administrateurs sont-ils maîtrisés ?	Suppression des anciens prestataires, comptes partagés et utilisateurs inactifs.
Les formulaires sont-ils testés régulièrement ?	Demandes de contact, devis, inscriptions. Un test mensuel minimum est recommandé.
WooCommerce est-il testé après chaque mise à jour ?	Tunnel d'achat complet : panier, paiement, emails de confirmation client et administrateur.
Existe-t-il une procédure de retour arrière documentée ?	Indispensable avant toute intervention importante. Le prestataire doit pouvoir restaurer en moins de 30 minutes.

Ce que les lecteurs demandent souvent

Un site WordPress non mis à jour est-il forcément piraté ?

Faut-il activer toutes les mises à jour automatiques ?

Un plugin désactivé est-il encore un risque de sécurité ?

Une maintenance mensuelle suffit-elle ?

Le prestataire doit-il fournir un rapport de maintenance ?

Comment savoir si mon site a déjà été compromis ?

Conclusion

Un site WordPress non maintenu n'est pas seulement un site ancien. C'est un système vivant qui dépend d'un CMS, d'un thème, d'extensions, d'un serveur, de comptes utilisateurs, de sauvegardes et de services externes. Chacun de ces éléments peut devenir un point de défaillance.

Pour une PME, la bonne approche consiste à sortir du flou : savoir ce qui est installé, qui intervient, ce qui est sauvegardé, ce qui est testé et ce qui se passe en cas de problème. La maintenance n'est pas une dépense invisible ; c'est l'assurance qui permet au site de rester disponible, sécurisé, performant et utile à l'activité de l'entreprise.

Un diagnostic court peut suffire à identifier les priorités : ce qui doit être corrigé immédiatement (PHP dépassé, extensions abandonnées, comptes non maîtrisés), ce qui peut être planifié (migration de version, audit des extensions), et ce qui relève d'une décision de direction (budget de maintenance, choix du prestataire).

Sources

• WordPress.org, Security : WordPress propulse plus de 43 % du web et seule la dernière version est officiellement supportée.

• Patchstack, State of WordPress Security in 2026 : 11 334 vulnérabilités en 2025, délai médian d'exploitation de 5 heures, 91 % des failles dans les plugins, 46 % sans correctif à la divulgation.

• PHP.net, Supported Versions : tableau officiel des versions PHP supportées et de leurs dates de fin de vie.

• ANSSI, 10 règles d'or en matière de sécurité numérique : recommandations sur les sauvegardes, les mises à jour et la gestion des accès.

• Google Search Central, Core Web Vitals : utilisation des Signaux Web Essentiels comme critère de classement SEO.

• WordPress.org, Hardening WordPress : guide officiel de durcissement de la sécurité WordPress.

• WordPress.org, Site Maintenance : recommandations officielles sur la maintenance et les mises à jour.