WordPress piraté: pages spam/phishing et redirections

Site piraté · https://academy.drgeek.com/docs/wordpress/site-pirate/wordpress-pirate-pages-spam-phishing-et-redirections/

Votre site WordPress affiche des pages inconnues dans Google ou redirige vers des contenus suspects? Même si tout semble normal en apparence, il est possible que votre site ait été piraté. Ce type de problème est fréquent et nécessite une intervention rapide pour éviter que la situation ne s’aggrave.

En bref

- un site peut être piraté sans que cela soit visible immédiatement
- des pages spam peuvent être injectées dans Google
- des fichiers malveillants peuvent se réinstaller automatiquement
- un nettoyage complet ou une réinitialisation est souvent nécessaire

Reconnaître un site WordPress piraté

Certains signes doivent vous alerter rapidement:

- des pages inconnues apparaissent dans les résultats Google
- des liens redirigent vers des sites de vente ou des contenus sans rapport
- des fichiers étranges sont présents dans votre hébergement ou votre FTP
- des fichiers supprimés réapparaissent
- le site semble normal, mais son comportement est inhabituel

Ce type de piratage est souvent utilisé pour injecter du contenu SEO (montres, casino, produits, etc.) afin d’exploiter la visibilité de votre site.

Pourquoi cela arrive ?

Dans la majorité des cas, le problème vient d’une faille de sécurité.

- WordPress non mis à jour
- extensions ou thème obsolètes
- mot de passe trop faible
- faille exploitée permettant d’injecter du code

Une fois le site compromis, des scripts malveillants peuvent être installés pour maintenir l’accès au site.

Pourquoi les fichiers reviennent

Supprimer des fichiers suspects peut sembler résoudre le problème, mais ce n’est généralement pas suffisant.
Si les fichiers réapparaissent, cela signifie qu’un accès pirate ou un script est encore actif.

Point important

- si des fichiers reviennent, le site est toujours infecté
- supprimer manuellement ne suffit pas
- une backdoor est probablement encore présente

Les solutions possibles

Nettoyer le site

Cette solution permet de conserver le site existant.

- analyse des fichiers infectés
- suppression des scripts malveillants
- vérification de la base de données
- mise à jour complète du site
- renforcement de la sécurité

Réinitialiser le site

Cette option consiste à repartir sur une base saine.

- suppression de l’installation actuelle

- réinstallation propre de WordPress
- remise en ligne du contenu sain
- mise en place d’une configuration sécurisée

Que faire en priorité

1. faire une sauvegarde du site (même infecté)
2. changer tous les mots de passe
3. éviter de supprimer des fichiers au hasard
4. faire analyser le site en profondeur
5. mettre à jour WordPress, le thème et les extensions

Impact sur Google

Un site piraté peut être utilisé pour créer des pages spam indexées dans Google.

Après nettoyage, il est important de:

- vérifier les pages indexées
- identifier les URL indésirables
- demander leur suppression
- relancer l’indexation du site

Astuce utile

Utilisez Google pour rechercher votre site avec la commande site:votresite.com. Cela permet de repérer rapidement les pages suspectes indexées.

Quand demander de l’aide?

Une intervention est recommandée si vous observez l’un des cas suivants:

- des fichiers réapparaissent après suppression
- des redirections inexpliquées
- des pages inconnues dans Google
- vous ne savez pas identifier les fichiers infectés

Pour conclure

Un site WordPress piraté peut continuer à fonctionner normalement en apparence, tout en étant exploité en arrière-plan. Pour éviter que le problème ne s’aggrave, il est important d’agir rapidement avec une solution adaptée : nettoyage complet ou réinitialisation.