GUIDE 12 SÉCURITÉ ET CONFORMITÉ

Site piraté : le guide de reprise en main

Les gestes à poser immédiatement si votre site web a été piraté ou infecté, dans l'ordre, avec ce qui aide vraiment et ce qui ne sert à rien.

M

Mario
Expert senior · GXN

Plus de vingt ans
En implantation technologique

31 juillet 2026
Mis à jour

SÉCURITÉ ET CONFORMITÉ

Site piraté : le guide de reprise en main

TL;DR

La réponse en une minute

Si votre site a été piraté, restez calme, c'est plus courant que vous pensez et ça se corrige presque toujours. Les premiers gestes sont de changer immédiatement tous les mots de passe liés au site, de faire une copie de l'état actuel avant de toucher à quoi que ce soit d'autre, d'identifier l'ampleur visible du problème, puis de procéder au nettoyage et à la fermeture de la porte d'entrée qui a permis l'incident. Après le nettoyage, l'étape que presque tout le monde oublie est de durcir la sécurité pour empêcher que ça se reproduise.

01 · GUIDE DE FOND

D'abord, respirez

Un site piraté fait peur, mais dans la grande majorité des cas, ce n'est pas catastrophique et ça se règle. Les attaques automatisées qui touchent la plupart des petits et moyens sites ne sont généralement pas dirigées personnellement contre vous. Elles ciblent des vulnérabilités connues, à grande échelle, sur des milliers de sites en même temps. Vous n'êtes probablement pas une cible spécifique, vous êtes une porte laissée entrouverte que quelqu'un a trouvée.

02 · GUIDE DE FOND

Les gestes immédiats, dans l'ordre

Changez tous les mots de passe liés au site. Hébergement, administration du site, courriel associé, tout ce qui pourrait avoir été compromis en même temps.

- Faites une copie de l'état actuel avant de nettoyer quoi que ce soit. Même infecté, ça peut servir à comprendre ce qui s'est passé.

- Regardez ce qui est visible. Le site affiche t il du contenu étrange, redirige t il vers un autre site, un navigateur affiche t il un avertissement de sécurité. Cette observation aide à cerner l'ampleur du problème.

- Vérifiez si votre hébergeur a suspendu le site de son propre chef, ce qui arrive parfois automatiquement en cas de détection de contenu malveillant.

- Ne paniquez pas et ne supprimez pas tout dans l'urgence. Une suppression précipitée peut détruire des preuves utiles pour comprendre la porte d'entrée exacte de l'attaque.

CARTE DE DÉCISION

Les quatre angles à garder ensemble

01

D'abord, respirez

02

Les gestes immédiats, dans l'ordre

03

Ce qui se fait ensuite, le nettoyage proprement dit

04

L'étape que tout le monde saute

GRILLE DE LECTURE DU GUIDE

Angle	Dimension à examiner	Usage dans la décision
01	D'abord, respirez	Établir le contexte
02	Les gestes immédiats, dans l'ordre	Identifier les dépendances
03	Ce qui se fait ensuite, le nettoyage proprement dit	Comparer les options
04	L'étape que tout le monde saute	Préparer la prochaine étape

03 · GUIDE DE FOND

Ce qui se fait ensuite, le nettoyage proprement dit

Identifier la porte d'entrée. Presque toujours, c'est un logiciel non mis à jour, un mot de passe faible, ou un compte oublié avec encore des accès actifs.

- Retirer le contenu malveillant injecté dans les fichiers ou la base de données du site.

- Fermer la porte d'entrée identifiée. Ça ne sert à rien de nettoyer si la faille reste ouverte pour la prochaine attaque.

- Restaurer à partir d'une sauvegarde saine si le nettoyage manuel s'avère trop complexe ou incomplet.

- Demander la révision auprès de Google ou des autres services si des avertissements de sécurité ont été affichés publiquement.

OUTIL INTERACTIF

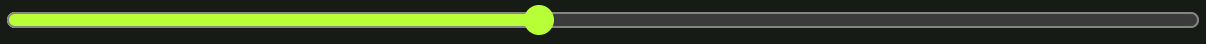
Situez votre décision

Sélectionnez les dimensions qui décrivent votre situation. Le résultat sert à organiser la prochaine conversation, pas à remplacer une analyse.

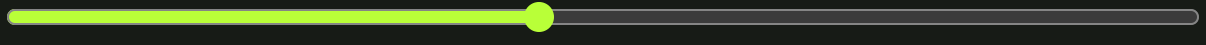
CE QUI VOUS CONCERNE MAINTENANT

- 01 **D'abord, respirez**
- 02 **Les gestes immédiats, dans l'ordre**
- 03 **Ce qui se fait ensuite, le nettoyage proprement dit**
- 04 **L'étape que tout le monde saute**

Urgence de la décision 5



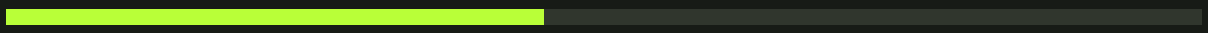
Niveau de contrôle actuel 5



ANALYSE RECOMMANDÉE

Plusieurs dimensions doivent être traitées ensemble

Évitez une décision isolée. Cartographiez les dépendances et convenez d’un ordre d’intervention.



45 / 100

L'étape que tout le monde saute

Une fois le site nettoyé et remis en ligne, le réflexe naturel est de tourner la page et de passer à autre chose. C'est exactement le moment où il faut durcir la sécurité, pas relâcher la vigilance. Mettre à jour tous les logiciels, revoir tous les comptes ayant accès, mettre en place une surveillance continue, et vérifier que les sauvegardes fonctionnent réellement, pas juste en théorie.

Sauter cette étape, c'est nettoyer une fois et attendre la prochaine attaque, qui viendra probablement par le même chemin.

05 · GUIDE DE FOND

Ce que nous pouvons faire, et ce que nous ne faisons pas

Nous faisons le nettoyage technique, l'identification de la porte d'entrée, le durcissement de la sécurité, et le rétablissement après incident. Nous ne faisons pas l'enquête judiciaire formelle destinée à des procédures légales, ni l'analyse d'intrusion certifiée pour des fins d'assurance. Si votre situation nécessite ce niveau d'investigation, nous vous le dirons franchement et vous orienterons vers les ressources appropriées.

06 · GUIDE DE FOND

Ce que je vois sur le terrain

Presque tous les sites piratés que j'ai nettoyés en vingt ans partageaient le même profil. Des mises à jour repoussées pendant des mois, parfois des années. Des comptes d'anciens employés ou d'anciens fournisseurs jamais désactivés. Aucune sauvegarde vérifiée, ou une sauvegarde qui existait en théorie mais n'avait jamais été testée.

L'attaque elle même n'était presque jamais sophistiquée. C'était la négligence accumulée qui avait ouvert la porte, pas un génie du crime informatique.

07 · GUIDE DE FOND

Quand ce guide ne suffit pas

Si des données personnelles de clients ont potentiellement été exposées, la situation dépasse le simple nettoyage technique et touche à des obligations de notification qui relèvent de votre conseiller juridique. Si vous soupçonnez une intention criminelle ciblée précisément contre votre entreprise, plutôt qu'une attaque automatisée générique, une consultation avec les autorités appropriées devient pertinente en complément du travail technique.

QUESTIONS ET RÉPONSES

Questions fréquentes

01 **Dois je payer une rançon si on me la demande.**

Généralement non, il n'y a aucune garantie que payer résout quoi que ce soit, et ça encourage la poursuite de ces pratiques. Une restauration à partir d'une sauvegarde saine est presque toujours préférable.

02 **Combien de temps prend un nettoyage complet.**

03 **Vais je perdre mon positionnement sur Google après un piratage.**

04 **Comment savoir si mon site est encore infecté après un nettoyage.**

MÉTHODE ÉDITORIALE

Guide de fond écrit par Mario pour GXN à partir de situations réelles d’entreprise. Les recommandations restent indépendantes des marques et des fournisseurs.

M

À PROPOS DE L'AUTEUR

Mario

Expert senior directement accessible, avec plus de vingt ans d'expérience en implantation technologique.

Voir le profil de Mario ↗

PROCHAINE ÉTAPE

Si c'est en cours actuellement, la section SOS numérique de notre site est conçue exactement pour cette urgence.

Sinon, l'évaluation gratuite vous donne une lecture honnête de votre situation de sécurité actuelle.

Pas d'appel obligatoire. Pas de séquence de vente.