C’est la hantise de tous les possesseurs de site internet : le hacking. Cela signifie que votre site a été piraté, et que par conséquent, il est désormais inexploitable, ou, dans le meilleur des cas, que la sécurité des données qu’il contient a été compromise.
Voilà comment réagir si cela vous arrivait et comment vous prémunir d’éventuelles attaques.

Quoi faire après un piratage informatique ?

Vous venez de vous rendre compte que votre site web est complètement hors service…
Pas de panique. Vous devez tout d’abord agir avec méthode et sans précipitation afin de limiter la perte de données.

Quelles sont les conséquences possibles d’un site hacké ?

Il existe plusieurs manières de pirater un site web. Vous pouvez tout d’abord constater la présence inopportune de liens vers d’autres sites douteux.
Ou bien, plus flagrant, votre site a complètement changé d’apparence…
Mais quelles sont les conséquences d’un tel hacking ?

- Vol de coordonnées personnelles ou bancaires
- Modification ou perte de données
- Usurpation d’identité
- Perte financière
- Perte de confiance de vos clients
- Implantation de malware
- Impact direct sur le SEO

Comment réagir après avoir constaté une cyberattaque?

Le premier bon réflexe à avoir est d’identifier d’où provient la faille de sécurité qui a mené à cette attaque.

> **« Ce qui est sécurisé à 99 % n’est pas sécurisé » – Le blog du hacker**

Vous pouvez pour cela examiner les « logs », autrement dit, les fichiers qui tiennent le journal de tout ce qui se passe sur votre site.
Observez alors les fichiers qui ont subi des modifications, et plus particulièrement durant les dernières 24 h avant d’avoir constaté le piratage.
Remettre sur pied un site qui a été piraté
Voilà le moment où vous serez heureux d’avoir fait une sauvegarde de votre site en préventif… Car celle-ci va servir !

- Supprimez ou corrigez tout d’abord les fichiers que vous avez identifié comme potentiellement vulnérables, puis procédez à la restauration du site en lui-même, à partir d’une sauvegarde fonctionnelle.
- Changez ensuite tous les mots de passe du site, et effectuez toutes les mises à jour demandées.
- Installez ensuite éventuellement un outil de détection d’intrusion, afin de prévenir une nouvelle attaque.

Agissez avec méthode et au besoin, faites-vous aider
Si vous ne vous sentez pas capable de réaliser ces actions sereinement, n’hésitez pas à faire appel à un expert.
Il vaut mieux solliciter quelqu’un de compétent, plutôt que de risquer de perdre définitivement vos données.

La prévention pour anticiper de futures attaques

Mettre en place une routine de sauvegarde efficace doit être votre priorité.
Comme nous venons de le voir, une sauvegarde régulière de votre base de données assure une remise en service rapide et simple.

Si vous vous apercevez que votre site est trop vulnérable, et que vous ne savez pas comment faire pour pallier au problème, nous vous conseillons de procéder à une refonte complète de celui-ci.

Envisagez une refonte pour prévenir les vulnérabilités

Le défaut de mises à jour ou l'emploi de technologies datées contribuent largement à faire de votre site une proie facile pour les hackers.

C'est alors peut-être l'occasion de prévoir une refonte complète, et de renforcer sa sécurité.

Confiez la réalisation de votre site à des professionnels

L'équipe de développeurs et de webmasters Expertisme se tient à votre disposition pour organiser une refonte complète de votre site web, en prenant en compte les aspects de sécurisation nécessaires.

Vous bénéficierez alors :

- De notre expérience sur diverses plateformes (WordPress, PrestaShop, Drupal, Joomla, …)
- De conseils personnalisés
- D'un accompagnement complet pour un site performant et sécurisé

L'avis de l'Expert en développement Web

Trop de sites web deviennent vulnérables avec le temps.

C'est pourquoi il faut régulièrement penser à organiser une refonte de son site web, avec des outils au goût du jour et au fait des dernières recommandations en termes de sécurité.

N'hésitez pas à nous contacter pour nous faire part de votre besoin.