

SÉCURISATION DU RÉSEAU ET DU SITE WEB DE L'ENTREPRISE

GEORDY BALOU

BTS SIO SISSR

CFA INGETIS PARIS



SOMMAIRE

- Introduction
- Sécurisation du réseau
- Sécurisation du site web

INTRODUCTION

Un réseau d'entreprise désigne un ensemble interconnecté autorisant la circulation en mode continu ou discontinu de flux. Un réseau en informatique est un ensemble d'équipements reliés entre eux pour échanger des informations.

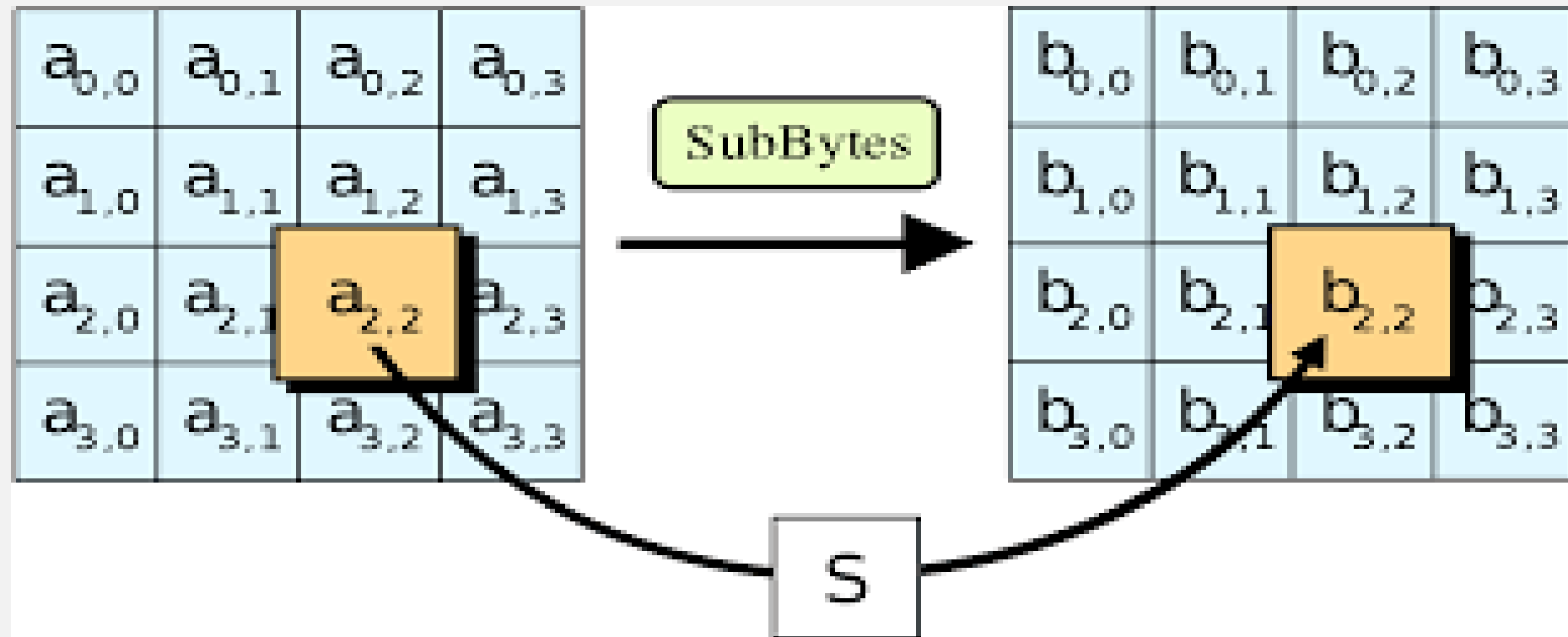
Afin de se protéger mais aussi de protéger son réseau de nombreux moyens peuvent être mis en place

SÉCURISATION DU RÉSEAU

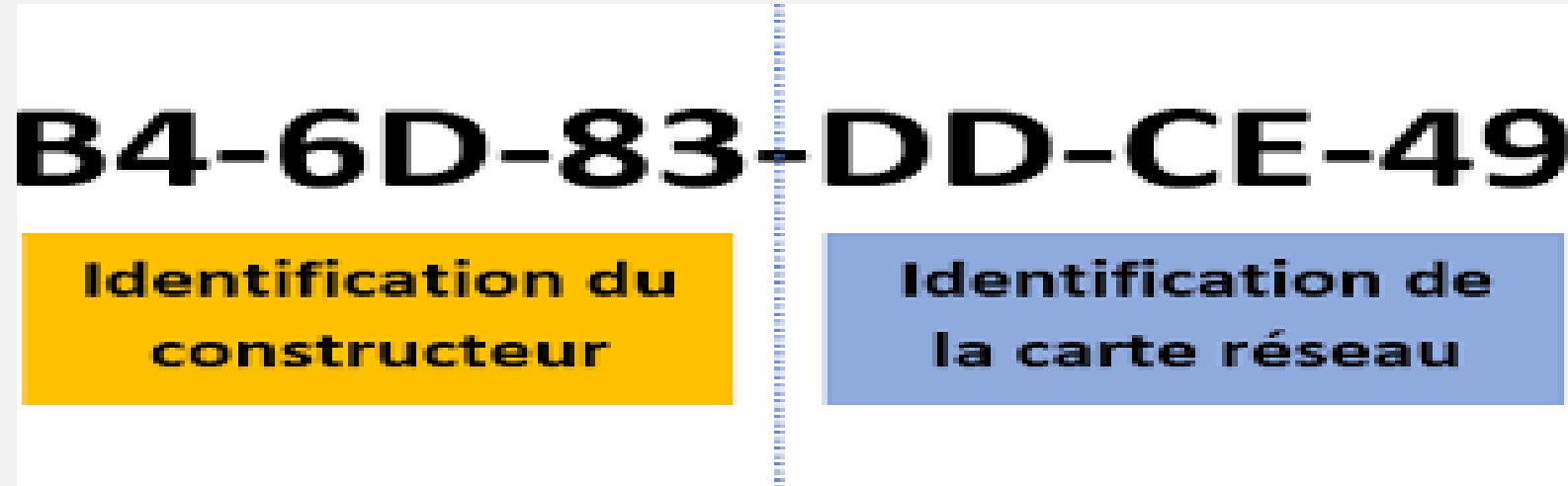
- La première option est de créer un mot de passe fort en effet ce mot de passe doit comporter au moins 8 caractères, il ne doit pas contenir aucun nom d'utilisateur, de famille ou de l'entreprise
- Il ne faut pas utiliser des mots entiers il est également recommandé de combiner des lettres minuscules majuscules, des chiffres des caractères spéciaux (par exemple : , ? ; . / § % u) mais aussi des lettres accentuées
- L'introduction délibérée de fautes d'orthographe est également un bon moyen.
- Nous devons renouveler régulièrement les mots de passe qui protègent des contenus ou accès les plus sensibles
- Ne pas utiliser les mêmes mots de passe Toujours se déconnecter d'un service ou d'un ordinateur avant de le quitter, surtout s'il se trouve dans un lieu public



- On recommande de chiffrer son réseau wifi, notamment contre les renifleurs de réseau comme Wireshark par exemple qui peut obtenir des informations en reniflant le réseau quand des données personnelles sont utilisées dans des sites non sécurisés
- Le chiffrement permet donc de rendre illisibles ces données même si elles sont interceptées, pour cela il faut mettre en place le protocole WPA2 qui utilise AES (algorithme de chiffrement) et surtout pas le protocole WEP



- On peut faire du filtrage par adresse mac
- Une adresse Mac est une adresse stockée dans une carte réseau qui est unique au monde



- Une connexion VPN (Réseau Privé Virtuel) crée un tunnel de données entre votre appareil et internet en passant par un serveur tiers cela peut aider à masquer vos identités ou faire croire qu'on se connecte depuis un autre endroit permet de changer l'adresse IP.
- Il faudrait utiliser un bon vpn connu comme nordVPN

- Le service de NordVPN est l'un des plus fiables du marché. Comme en témoignent les tests réalisés à l'aide de l'outil de mesure des VPN de référence Speed Test sur une connexion ADSL, ses serveurs sont dans l'ensemble stables et rapides que cela soit en France, en Angleterre, aux États-Unis, à Taïwan ou en Australie.

NordVPN



Figure de proue des VPN, NordVPN continue d'évoluer à marche forcée. Ses performances sont montées d'un cran grâce notamment à l'implémentation du protocole VPN de dernière génération NordLynx. Outre des applications remarquables et désormais entièrement francisées, il se distingue par sa simplicité d'utilisation et son excellente stabilité. Un service que l'on ne peut que vous recommander, si vous cherchez un VPN sans prise de tête.

Les plus

- + Streaming et accès TV très efficace
- + Très grand nombre de serveurs
- + Protocole VPN NordLynx de dernière génération
- + Réactivité du support client

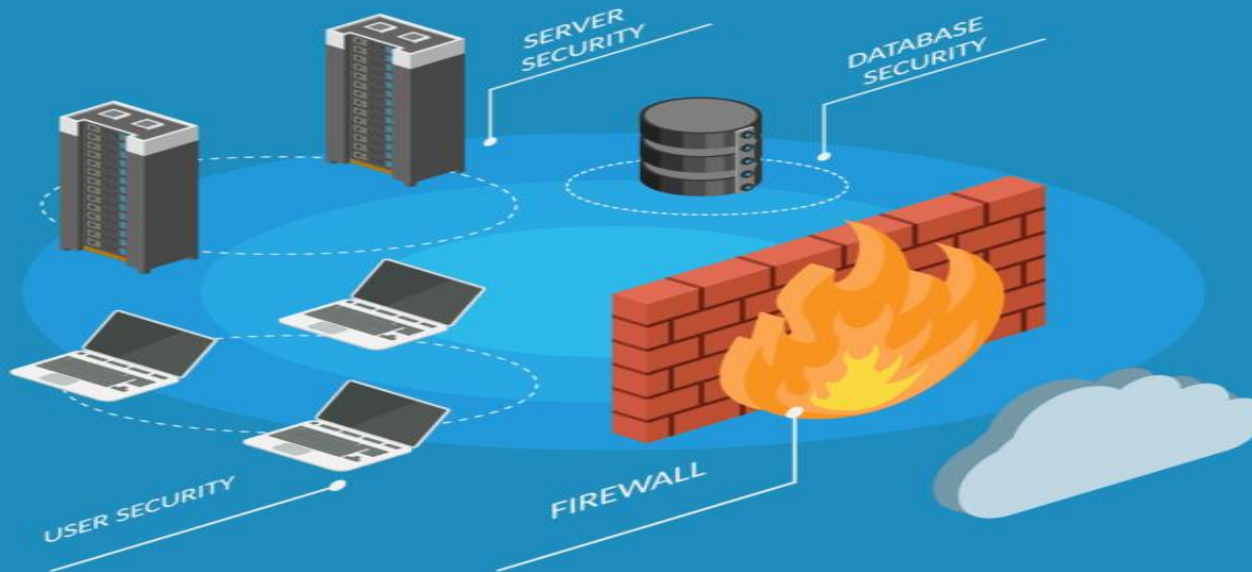
Les moins

- Couverture multiplateforme à améliorer
- Configuration routeur complexe

Performances  9

Nombre de Serveurs  10

- Activer le pare feu
- Le pare-feu est une passerelle filtrante qui protège un ordinateur ou un réseau des intrusions venues d'Internet. Il filtre en effet les [paquets](#) de données qui sont échangés. Il est parfois traduit comme [coupe-feu](#), barrière de sécurité ou garde-barrière. Il est doté au moins de deux interfaces, l'un destiné au réseau interne et l'autre au réseau externe.
- Affichez le Panneau de configuration (en cliquant sur le menu Démarrer) et cliquez sur Pare-feu Windows.
- Cliquez sur Activer ou désactiver le Pare-feu Windows et vérifiez que le pare-feu est bien activé, qu'il s'agisse des paramètres des emplacements réseau domestique ou d'entreprise (privés) ou des paramètres des emplacements réseau public.



SÉCURISATION DU SITE WEB

- Pour que le site soit sécurisé, il va falloir mettre en place un certain nombre de principe car la sécurisation d'un site Internet se fait au travers de plusieurs actions.
- De plus, cela nécessite une attention régulière. Ce n'est clairement pas quelque chose qu'on fait une fois et puis qu'on peut oublier ensuite.

- [Installer un certificat SSL](#) (pour passer votre site en HTTPS)
 - Utiliser des mots de passe sécurisés
 - Mettre à jour votre site et ses plugins régulièrement
 - Configurer des sauvegardes journalières
 - Installer des plugins permettant de sécuriser votre site WordPress
 - Valider manuellement les commentaires
-
- Pour que vous compreniez mieux comment sécuriser un site Internet, nous allons détailler à la suite chacune des étapes listées.

❖ Installer un certificat SSL (pour passer votre site en HTTPS)

- Un site sécurisé est un site qui utilise le protocole HTTPS. Pour y arriver il faudra tout simplement installer un certificat SSL.
- Si vous ne faites pas ça, votre site Internet ne sera pas en mesure de fournir une connexion sécurisée aux visiteurs.



- Vous ne vous en rendez peut être pas compte mais en 2022, pratiquement tous les sites web utilisent un certificat SSL afin de chiffrer la connexion avec leur plateforme.

- Nous n'allons pas nous attarder sur les détails techniques d'un certificat SSL et d'une connexion HTTPS. Retenez simplement que sans ça, les données qui vont transiter vers votre site ne seront pas protégées. Vous allez ainsi risquer de compromettre la sécurité de vos visiteurs.
- De plus d'un point de vue SEO (classement sur Google), c'est très mal vu de ne pas proposer de connexion sécurisée.
- Pour installer un certificat SSL sur votre site Internet, il y a plusieurs possibilités qui vont s'offrir à vous :
- Choisissez un hébergeur web qui propose gratuitement avec son hébergement des certificats SSL. C'est par exemple le cas d'[Hostinger qui met à disposition gratuitement des certificats SSL Let's Encrypt](#).
- Optez pour un créateur de site qui inclut dans son abonnement un certificat SSL gratuit. Nous vous invitons à lire notre [comparatif des meilleurs logiciels de création de site](#) pour de plus amples informations.
- Comme dit, **un certificat SSL Let's Encrypt fera amplement l'affaire.**
- Mais si vous voulez un niveau de sécurité encore plus élevé pour votre site, vous pourrez toujours acheter un certificat SSL avancé. L'hébergeur Hostinger en propose à la vente.

❖ Utilisation de mots de passe sécurisés

- Dès qu'on parle de sécurité en ligne, on en vient forcément au sujet des mots de passe.
- Afin de sécuriser votre site Internet, **veillez à utiliser des mots de passe complexes**. Cela vaut aussi bien pour le mot de passe que vous utilisez afin d'accéder à votre espace d'hébergement, ou celui vous permettant d'accéder au panneau d'administration de votre site WordPress.
- Qu'est-ce qu'un mot de passe complexe au juste ? À quoi cela ressemble ?
- Déjà, si votre mot de passe ne comprend que des chiffres ou des lettres, il va falloir changer tout ça ! Aussi, évitez à tout prix d'utiliser le même mot de passe sur toutes les plateformes en lien avec votre site Internet.
- Cela évitera que si un hacker trouve votre mot de passe, il puisse accéder à absolument tout.

Pour sécuriser au mieux votre site, voici quelques règles que vos mots de passe vont devoir respecter :

- Doit comprendre 16 caractères ou plus
- Utilisation de caractères spéciaux (\$!%@), des chiffres, ainsi que des majuscules
- Utilisation de ces caractères à des endroits aléatoires dans votre mot de passe
- N'introduisez aucun renseignement personnel

Il faudra aussi penser à changer régulièrement votre mot de passe (3 à 4 fois par an). Nous savons que c'est plus que contraignant mais c'est vraiment nécessaire afin d'améliorer la sécurité de votre site Internet.

- Imaginez les dégâts qui pourraient être causés par le hack de votre compte d'hébergement ? Et si c'était votre compte d'administration de WordPress ?
- Pour vous éviter le moindre tracas, utiliser des mots de passe sécurisés est quelque chose de très facile à mettre en place. Ne vous en privez donc pas. Si vous manquez d'inspiration au moment de changer vos mots de passe, sachez qu'il existe pas mal de sites qui peuvent vous assister :



Générateur de mot de passe sécurisé

Longueur du mot de passe:

16

Inclure des symboles:

☒ (par exemple, @\$%)

Inclure des nombres:

☒ (par exemple, 123456)

Inclure des caractères minuscules:

☒ (par exemple, abcdefgh)

Inclure des caractères majuscules:

☒ (par exemple, ABCDEFGH)

Exclure les caractères similaires:

☒ (par exemple, l, I, 1, L, o, 0, O)

Exclure les caractères ambigus:

☐ ({ } [] () \ ' " ~ , . : ; < >)

Générer sur votre appareil:

☒ (NE PAS envoyer sur Internet)

Sélection automatique:

☐ (sélectionner le mot de passe automatiquement)

Enregistrer ma préférence:

☐ (enregistrer tous les paramètres ci-dessus pour une utilisation ultérieure)

Charger mes paramètres n'importe où:

URL pour charger rapidement mes paramètres sur d'autres ordinateurs

Créer un mot de passe

Copie

Votre nouveau mot de passe:

Votre nouveau mot de passe apparaîtra ici.

Souvenez-vous de votre mot de passe:

Souvenez-vous de votre mot de passe avec le premier caractère de chaque mot de cette phrase.

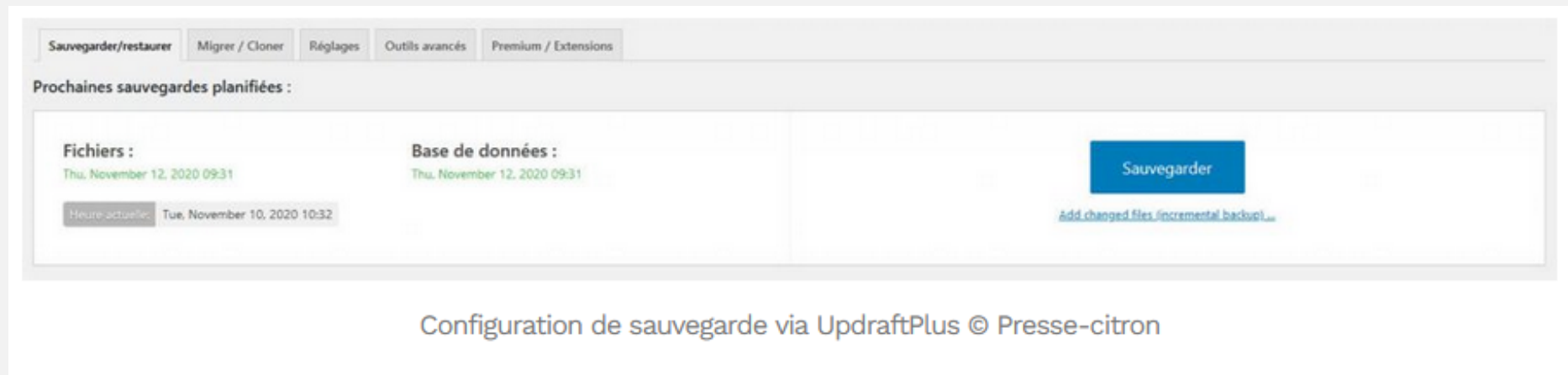
Générateur de mot de passe © Passwordsgenerator.net

❖ Mise à jour régulière de votre site web et ses plugins

- Le fait de ne pas mettre régulièrement à jour votre site Internet peut vous porter préjudice.
- On entend par là qu'il va falloir mettre à jour régulièrement votre CMS (que vous utilisiez WordPress, [Magento](#), Drupal, [PrestaShop](#), etc). En effet sans cela vous allez exposer votre site à des bugs, ou encore à des failles de sécurité.
- Cette remarque vaut aussi pour tout ce qui est plugins. Même si vous utilisez [les meilleurs plugins WordPress](#) sur le marché, il faut veiller à les mettre à jour régulièrement.
- On ne vous demande pas de les mettre à jour dans les 2 heures qui suivent la mise à disposition d'une nouvelle version. Loin de là car c'est clairement contre productif et vous vous exposez à de possibles bugs. Pour autant, veillez à faire les mises à jour sous quelques semaines.
- Pour les mises à jour de WordPress, vous allez pouvoir configurer l'ensemble afin qu'elles se fassent toutes seules. À vous de voir ce que vous préférez.

❖ Configuration des sauvegardes pour votre site

- Qui dit sécuriser un site WordPress (ou autre), dit forcément sauvegardes. Si vous ne pouvez pas stopper une attaque ou un hack, il faut que vous ayez des sauvegardes solides de votre plateforme.
- De cette manière vous aurez toujours l'esprit tranquille.
- Pour sauvegarder votre site, plusieurs options vont s'offrir à vous :
- **Choix d'un hébergeur web qui propose un système de sauvegardes journalières** : [Hostinger](#) et [PlanetHoster](#), qui sont d'ailleurs parmi les meilleurs hébergeurs de 2022, proposent tous les deux cela.
- **Utilisation d'un plugin de backup** : si c'est quelque chose qui vous tente, on vous conseille vivement d'opter pour le plugin WordPress UpdraftPlus afin de sauvegarder et surtout sécurisé votre site. Lisez [notre tutoriel expliquant comment sauvegarder un site WordPress](#) pour mieux comprendre les étapes de configuration du plugin.



- Une fois la méthode et l'outil de sauvegarde choisis, il va falloir déterminer la fréquence de vos sauvegardes ainsi que l'emplacement de stockage.
- Ce sont des sujets à ne surtout pas négliger. En effet, vous vous doutez bien que faire une sauvegarde tous les six mois n'est pas efficace. Pareil pour les sauvegardes enregistrées directement sur votre espace d'hébergement.
- Pour ce cas de figure, envisagez vraiment des sauvegardes externalisées.

❖ **Installation de plugins pour sécuriser votre site (ainsi qu'un anti-malware côté hébergement)**

- Afin de sécuriser au mieux votre site Internet, il peut aussi être intéressant d'envisager l'utilisation de plugins permettant une sécurisation accrue.
- On pense à des plugins comme iThemes Security, Wordfence et bien d'autres.



Wordfence Security – Firewall & Malware Scan

Sécurisez votre site web avec l'extension de sécurité la plus compréhensible. Pare-feu, scanner de logiciel malveillant, blocage, trafic en temps réel, sécurité de connexion et bien d'autres.

Par *Wordfence*

★★★★★ (3 610)
3 millions et + installations actives

Dernière mise à jour : il y a 3 semaines

✓ Compatible avec votre version de WordPress

[Installer maintenant](#)

[Plus de détails](#)



iThemes Security (anciennement Better WP Security)

iThemes Security est l'extension WordPress n°1 de sécurité

Par *iThemes*

★★★★★ (3 836)
1 million et + installations actives

Dernière mise à jour : il y a 4 semaines

✓ Compatible avec votre version de WordPress

[Actif](#)

[Plus de détails](#)

Plug-ins WordPress pour améliorer la sécurité de votre site © Presse-citron

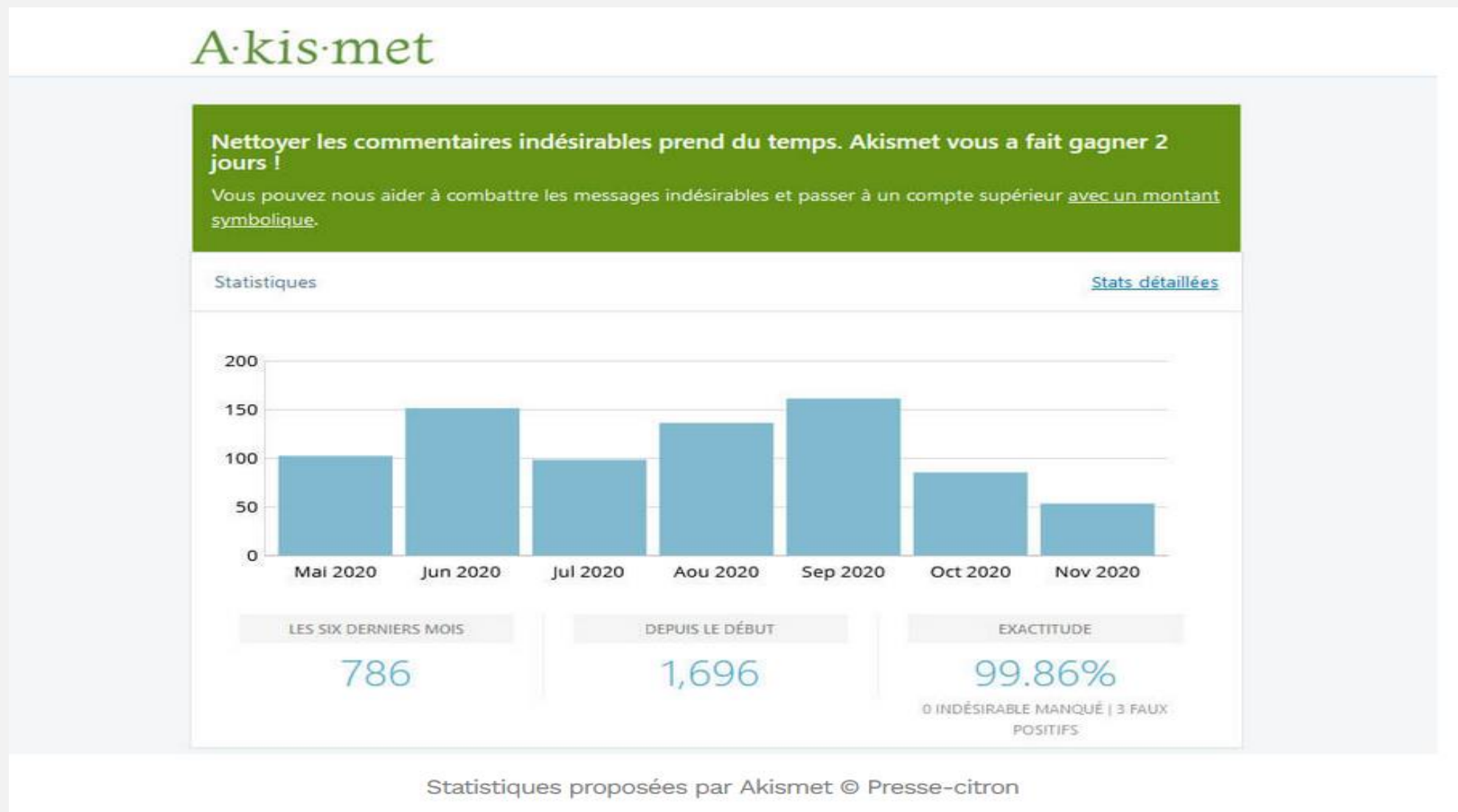
- Ces derniers vont vous permettre de bloquer les attaques brute force, de mettre en place un pare-feu supplémentaire, de scanner les logiciels malveillants, ou encore de bloquer des IP malveillantes.
- Si vous optez pour un plugin de sécurité comme iThemes Security sur WordPress, il est possible (et vivement recommandé) de déplacer l'administration afin de ne pas avoir votresite.com/wp-admin/ pour vous y connecter mais votresite.com/cequevousvoulez/. Cela protégera considérablement votre site face aux attaques et tentatives de connexion de type brute force.

- L'autre chose qu'il ne faut pas négliger, c'est la protection de votre hébergement et donc de votre site face aux malwares.
- Pour vous éviter des sueurs froides, privilégiez vraiment un hébergeur web qui propose avec ses hébergements un système anti-malware efficace.
- Si vous n'avez pas encore d'hébergement web, nous pouvons vous conseiller dans ce cadre Hostinger. Cet hébergeur réputé à travers le monde dispose d'un système anti-malware mais aussi d'un système anti-DDoS efficace afin de vous éviter des mauvaises surprises

❖ Validation manuelle des commentaires

- Cela ne coule pas forcément de source pour tout le monde mais le fait de valider manuellement les commentaires publiés sur les articles de votre site peut vous aider à améliorer la sécurité globale de votre site WordPress.
- Sécurité globale car faire cela ne va pas protéger votre hébergement web mais plutôt les visiteurs de votre site.
- Énormément de commentaires de spam et d'hameçonnage sont postés sur les sites Internets. Pour éviter que vos visiteurs tombent dans le panneau, essayez dans la mesure du possible de valider les commentaires avant qu'ils soient publiés. Cela évitera que des liens peu recommandables soient visibles et cliquables par tous.

- Pour vous assister dans cette tâche, nous pouvons aussi vous conseiller d'utiliser un plugin anti-spam. Il en existe pas mal sur WordPress (Akismet Anti-Spam étant certainement la référence).



- Grâce à un tel plugin, un premier tri sera fait automatiquement et vous n'aurez plus qu'à modérer les commentaires qui sont passés au travers du système anti-spam.

❖ **Quelles sont les menaces encourues par votre site web ?**

- Les menaces en lien avec la non sécurisation d'un site Internet sont nombreuses. C'est pour cette raison qu'il ne faut absolument pas lésiner sur les moyens et le temps passé à la sécurisation de votre site web.
- Voici une liste non-exhaustive des menaces auxquelles vous allez devoir faire attention :
- Attaque par déni de service (DDoS)
- Code malicieux / Injection SQL
- Virus
- Ransomware
- Hameçonnage
- En appliquant les conseils listés dans notre guide vous expliquant comment sécuriser un site, vous allez pouvoir contrecarrer l'ensemble de ces menaces.
- Mais comme dit, c'est un véritable travail de sape qui ne s'arrête jamais.

❖ Conclusion sur la sécurisation d'un site Internet

- Nous espérons qu'après avoir lu ce guide, vous savez à présent quoi faire afin d'améliorer la sécurité de votre site web.
- Dans la mesure du possible il va falloir considérer l'ensemble des aspects que nous avons pu détailler. Sans cela, votre site et ses visiteurs ne seront jamais en totale sécurité.
- Globalement la mise en place de nos différents conseils est assez simple. Nous tenons encore à vous préciser que notre liste est non-exhaustive.
- Il est tout à fait possible d'améliorer la sécurité de votre plateforme en ligne via d'autres moyens et méthodes. Pour autant, les principaux aspects sont couverts ici même.
- Et rappelez-vous, choisissez bien votre hébergeur web. C'est lui qui va être le premier garant de la sécurité de votre hébergement et de votre ou vos sites Internet. Il faut donc qu'il mette à disposition le nécessaire (protection anti-DDoS, anti-malwares), voire même plus si c'est possible. Notre recommandation à ce niveau est d'opter pour Hostinger.
- En plus de mettre à disposition tout le nécessaire afin de sécuriser votre site web, vous payerez votre hébergement à un prix plus que raisonnable. Et vous allez avoir le droit à 30 jours de garantie satisfait ou remboursé.
- Source : <https://www.presse-citron.net/hebergeur/faq/securiser-site/>