3 étapes pour sécuriser WordPress pas à pas

Etape 1 : Sauvegardez votre site régulièrement

- **Installez et activez le plugin Backwpup**
- **BackWPup → Ajouter une nouvelle opération**
  - Dans l'onglet général : entrez un nom et choisissez un emplacement de sauvegarde
  - Dans l'onglet programmation : sélectionnez « avec le cron wordpress » puis réglez la fréquence
- **BackWPup →Opérations**
  - Lancez une sauvegarde manuellement « Lancer maintenant »
  - Téléchargez votre sauvegarde en retournant dans le menu « Opérations »

Remarque : Vos sauvegardes automatiques seront par défaut dans le répertoire …/wp-content/uploads/

Etape 2 : Sécurisez votre interface d'administration

- Maintenez L'ensemble de votre système à jour (WordPress, plugins, thèmes)
- Supprimez les extensions non utilisées ou inutiles
- Créez un nouvel utilisateur avec les droits administrateurs et supprimer ensuite le compte admin d'origine
- Créez un nouvel utilisateur avec les droits « Editeur » qui servira à publier vos articles
- Réattribuez tous les anciens articles à ce nouvel utilisateur
- Pour tous vos utilisateurs, choisissez un mot de passe avec au moins 10 caractères et mélangez lettres/chiffres/symboles
- Limitez le nombre de tentatives de connexion à votre interface d'administration
  - Installez le plugin WP Cerber
  - Dans l'onglet général du plugin décochez la case « Utilisateurs inexistants »

Etape 3 : Sécurisez vos fichiers et vos dossiers

- **Modification du fichier .htaccess (à la racine de votre installation WordPress)**

⇨ **Avant toute chose, sauvegardez votre fichier .htaccess**

En rouge, les lignes à ajouter :

```
# BEGIN WordPress
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L] RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]

# Enlever l'accès direct aux utilisateurs par leur identifiant
#Attention cette partie doit bien se trouver entre les balises <IfModule mod_rewrite.c>
et </IfModule>
RewriteCond %{QUERY_STRING} ^author=([0-9]*)
RewriteRule .* - [F]
</IfModule>
# END WordPress

# Désactiver l'affichage du contenu des répertoires
Options All -Indexes
# Protéger le fichier wp-config.php
<files wp-config.php>
order allow,deny
deny from all
</files>
# Protéger les fichiers .htaccess et .htpasswds
<Files ~ "^.*\.([Hh][Tt][AaPp])">
order allow,deny
deny from all
satisfy all
</Files>
```

- **Modification du fichier functions.php (à la racine de votre thème enfant)**

⇨ **Avant toute chose, sauvegardez votre fichier functions.php (si vous n'avez pas de fichier functions.php, créez-le)**

Contenu à insérer à la fin du fichier :

```
<?php
// 1) masque la version de votre WordPress
remove_action("wp_head", "wp_generator");
// 2) empêche l'édition de vos fichiers directement depuis wordpress
define('DISALLOW_FILE_EDIT',true);
// 3) Masquez les erreurs de connexion
add_filter('login_errors',create_function('$a', "return 'Erreur';"));
?>
```

- **Supprimez le fichier readme.html présent à la racine de votre WordPress**

Votre site WordPress est maintenant sécurisé !

L'article complet est disponible à cette adresse : http://naturedigitale.fr/securiser-wordpress/