WORDPRESS SÉCURISER SON SITE

Public	Webmasters, webdesigners, chefs de projets, développeurs ou toute personne ayant besoin de sécuriser son site Internet réalisé avec WordPress.
Durée	1 journée - 7 heures
Pré-requis	Etre à l'aise avec l'environnement informatique (Mac, PC ou Linux) et avec les technologies du Web (hébergement et langages du Web).
Objectifs	Décrire les différents points de fragilité d'un site Web et d'un hébergement au niveau de la sécurité Mesurer les implications juridiques et d'exploitation Installer WordPress avec les règles de sécurité de base Installer et paramétrer des plug-ins complémentaires gratuits et payants à WordPress afin de le sécuriser Mettre en place une politique de sauvegarde de l'hébergement et des éléments WordPress Adapter le niveau de sécurisation du site en fonction des données qui y sont stockées et qui y transitent.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. CONTEXTE DE LA CYBERSÉCURITÉ

- Qu'est-ce que la cybersécurité d'un site Web ?
- De la gêne occasionnée à la perte de données
- De la perte de données au vol de données
- Niveaux de maturité de la cybersécurité
- Hébergement sécurisé
- Attaques les plus courantes
- Etre pris pour cible intentionnellement
- Automation, bots et dénis de service
- RGPD et législation des données privées

2. CHECK-UP SÉCURITÉ

- Ecosystème d'un site WordPress
- Vérification des versions logiciels pour l'hébergement
- Vérification des versions du WordPress et de ses éléments
- Complexité des mises à jour
- Audit de sécurité avec Sucuri

3. CÔTÉ HÉBERGEUR

- Risques des installations automatisées
- Fichiers .htaccess ou web.config
- Nom de domaine et certificat SSL
- Version PHP et MySQL
- Protocoles FTP
- Emails et certificats d'e-réputation
- Qu'est-ce qu'être blacklisté ?
- Créer des mots de passe forts
- Vérification des logs
- Hébergeurs "coffre-fort"
- Hébergeurs spécialisés WordPress

4. POINTS FAIBLES DE WORDPRESS

- Au moment de l'installation
- Types de mise à jour
- 5 points faibles WordPress
- Fragilisation par le template
- Les plug-ins les plus attaqués

5. POLITIQUE DE SAUVEGARDE

- Savoir revenir en arrière
- Les fichiers critiques
- Sauvegarde au niveau de l'hébergement
- Sauvegarde des fichiers du WordPress
- Sauvegarde du contenu du WordPress
- Sauvegardes manuelles et automatisées
- Sauvegardes locales et distantes
- Restauration
- Les bonnes pratiques
- Plug-ins et services de backup WordPress

6. SÉCURISATION RAPIDE

- Cacher votre WordPress
- Sécurisation des commentaires avec Akismet
- Plug-in Wordfence : version gratuite et payante
- Ce que protège vraiment Wordfence
- Avantages de la version payante de Wordfence
- Installation et paramétrage
- Suivi de la sécurité

7. SÉCURISATION MAXIMALE

- Présentation d'iThemes Security
- Installation et paramétrage
- Paramétrages initiaux de sécurisation
- Les 3 niveaux de priorité
- Mode avancé
- Changement des répertoires initiaux
- Pages 404
- Horaires d'ouverture de l'admin
- Bannissement
- Attaques de type "brute force"
- Détection des malwares
- Détection de modification de fichiers
- Sécurisation ultime de WordPress (Tweaks)
- Management des emails de notification
- Installer un plug-in antivirus
- Augmenter le niveau d'authentification

8. SOLUTIONS EN CAS D'URGENCE

- Test séquentiel des plug-ins installés
- Plug-in de maintenance
- Mettre le site en quarantaine
- Installer une version WordPress en sous-répertoire
- Exportation et réimportation du contenu .xml

9. OUTILS DE SUIVI

- Webmaster tools - Google Search Console
- Site en quarantaine
- Dialoguer avec Google après vaccination
- Erreurs d'exploitation

10. SÉCURISATION SPÉCIFIQUE AU E-COMMERCE

- Données critiques dans le e-commerce
- Fragilité des sites avec abonnements
- Que faire contre le scraping ?
- Eléments de réassurance client

11. CRÉER SON ESPACE LABORATOIRE

- Qu'est-ce qu'un site "draft" ?
- Installer un site de test en local
- Migrer un site manuellement
- Plug-in de migrations
- Script de nettoyage des URL via PHP et SQL

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation