En partenariat avec PYRAMYD

Programmes libres / CMS

WordPress - Sécuriser son site

Ref. WPRESS-SEC / WPRESSSEC25

1 jour (7h00) | ★★★★☆ 4,6/5 | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel

Tarif public inter-entreprises par personne : 970 € ht

Contenu mis à jour le 17/07/2026. Document téléchargé le 13/11/2026.

Public concerné

- Webmasters
- Webdesigners
- Chefs de projets
- Développeurs ou toute personne ayant besoin de sécuriser son site Internet réalisé avec WordPress

Prérequis

- Etre à l'aise avec l'environnement informatique (Mac, PC ou Linux) et avec les technologies du Web (hébergement et langages du Web).

Objectifs de formation

- 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

Programme de votre formation

M2i START

Contextualisation du projet de formation et prise en compte des besoins de chacun

- Positionnement initial de l'apprenant par rapport aux objectifs
- Définition des priorités et des objectifs personnels de l'apprenant
- Vidéos de mise en situation
- Accès au Chat interactif myM2i pour interagir avec les membres de son groupe

Programme

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

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

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

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

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

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

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

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

Outils de suivi

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

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

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

Exemples de travaux pratiques (à titre indicatif)

- *Atelier pratique*
  - *Choix de l'hébergement*
  - *Installation sécurisée de WordPress*
  - *Choix du template*
  - *Renseignement sur les plug-ins*
  - *Installation paramétrage iThemes Security*

M2i BOOST

Réactivation et approfondissement des acquis en situation de travail.

- 30 jours d'accompagnement personnalisé sur myM2i inclus [2]
- Ressources Boosters (Abonnement au M2i'Mag Soft Skills, formations offertes, invitations aux conférences d'actualité...)

Le contenu de ce programme peut faire l'objet d'adaptation selon les niveaux, prérequis et besoins des apprenants.

Modalités, méthodes et moyens pédagogiques

Équipe pédagogique :

Un consultant expert de la thématique et une équipe pédagogique en support du stagiaire pour toute question en lien avec son parcours de formation.

Techniques pédagogiques :

Pédagogie participative mettant l'apprenant au cœur de l'apprentissage. Utilisation de techniques ludo-pédagogiques pour une meilleure appropriation. Ancrage facilité par une évaluation continue des connaissances au moyen d'outils digitaux et/ou de cas pratiques.

Ressources pédagogiques :

Un support de formation présentant l'essentiel des points vus durant la formation et proposant des éléments d'approfondissement est téléchargeable sur notre plateforme.

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 M2I Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

Modalités d'évaluation des acquis

Modalités d'évaluation : évaluation en 3 phases :

Pendant la formation : un bilan journalier effectué par l'intervenant.
À chaud : à la fin de la formation, un bilan qualité pour mesurer l'atteinte des objectifs.
À froid : à J + 3 mois, une évaluation du transfert des acquis en situation professionnelle.

Accessibilité de la formation

Le groupe M2I s'engage pour faciliter l'accessibilité de ses formations. Toutes nos formations sont accessibles aux personnes en situation de handicap : les détails de l'accueil des personnes sont consultables sur la page Politique Handicap.

Modalités et délais d’accès à la formation

Les formations M2I sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 12 jours ouvrés.

1. Les actions et les outils présentés dans ce programme le sont à titre indicatif et peuvent faire l’objet d'adaptation selon les niveaux, prérequis et besoins des apprenants. Les compétences clés de ce programme sont traitées à raison d'une compétence par demi-journée de formation.
2. Sur myM2i, pendant 30 jours post-fin de formation, les apprenants disposent d’une messagerie sécurisée pour échanger, dans la limite de 4 sollicitations, avec leur formateur.

Scannez ce code pour consulter le programme en ligne et vous inscrire