PROGRAMME DE FORMATION DETAILLE
SÉCURISER SON SITE WORDPRESS

WordPress équipe plus de 40 % des sites internet dans le monde, ce qui en fait une cible privilégiée pour les attaques automatisées. Cette formation d'une journée vous guide dans les réflexes essentiels pour sécuriser durablement votre site : sauvegarde, mise à jour maîtrisée, durcissement des accès et réaction face à un incident. Le programme de formation est entièrement personnalisable en fonction de vos besoins.

Famille	Web / Digital	**Référence**	F298
Nb de jours	1 jour	**Nb d'heures**	7 heures
En présentiel	Oui	**À distance**	Oui (Zoom / Teams)
Éligible au CPF	Non		

Tarif :

INTER-ENTREPRISE 400€ HT / participant	**INTRA-ENTREPRISE** 450€ HT (+ 200€ HT / pers. supplémentaire)

INFORMATIONS PRATIQUES

1. Pour qui ?

Prérequis :

Aisance avec un environnement Windows ou Mac et un navigateur web. Disposer d'un accès administrateur à un site WordPress (hébergement personnel ou de démonstration) est recommandé pour la mise en pratique. Aucune compétence en développement n'est requise.

Public :

Gestionnaires de site internet, community managers, chefs d'entreprise de TPE/PME, indépendants, ainsi que toute personne responsable de la sécurité d'un site WordPress au sein de son organisation.

2. Objectifs, moyens, modalités, sanction, adaptation PSH

Objectifs :

Être en mesure d'identifier les principales menaces pesant sur un site WordPress et de mettre en œuvre les mesures essentielles pour le sécuriser : sauvegarde, mise à jour maîtrisée, durcissement des accès, mise en place d'extensions de protection, détection et réaction face à un incident de sécurité.

Moyens pédagogiques :

Un PC par personne, le formateur diffuse son écran sur un vidéo-projecteur ou télévision grand écran
Un groupe de maximum 5 personnes en inter-entreprise.
En distanciel : Utilisation de Zoom ou Teams avec partage d'écran, chat, audio et vidéo en temps réel.
Exposé théorique, suivi d'une mise en pratique.

Moyens pour suivre l'exécution de l'action :

- La présence du stagiaire est vérifiée par le formateur à l'aide d'une feuille de présence signée par demi-journées

Moyens pour en apprécier les résultats :

- A la fin de la formation, le stagiaire complète une évaluation à chaud (Permettant d'évaluer la qualité de la prestation)
- Puis, il complète avec le formateur une évaluation des acquis (Permettant de déterminer les points acquis, non acquis ou en cours d'acquisition)
- Quelques mois après la formation, le donneur d'ordre complète une évaluation à froid (Permettant de d'assurer que la formation a pu être mise en pratique)

Sanction de la formation :

- A la fin de la formation le stagiaire reçoit une attestation de formation reprenant l'intitulé de la formation, les dates et le nombre d'heures réalisées.

Délai d'accès :

En intra-entreprise : En fonction de vos disponibilités et celles de nos formateurs.
En inter-entreprise : En fonction des sessions que nous avons programmé, consultable en cliquant ici

Profil formateur :

Consultant expert en développement web et en sécurité des sites WordPress, intervenant en tant que consultant auprès des TPE/PME pour la protection et la sécurisation de leur présence en ligne.

Adaptation aux personnes en situation de handicap :

Nous nous engageons à favoriser l'accessibilité du public en situation de handicap, en fonction de leurs besoins et/ou difficultés, en adaptant la durée de la formation, le programme et son déroulement, les moyens pédagogiques et techniques, ainsi que les supports pédagogiques. Ces formations adaptées sont proposées en individuel ou en collectif (pour un public à besoins similaires). Afin de trouver la meilleure solution, nous nous appuyons sur des partenaires évoluant dans le domaine du handicap.

Personne à contacter / référent handicap :

Lambert Christophe
03 59 25 10 15
christophe.lambert@lc-formateur.com

3. Évaluation, avis...

Nouvelle formation : les indicateurs de satisfaction et d'évaluation seront disponibles après les premières sessions.

4. Comment financer ma formation ?

Vous êtes salarié, travailleur non salarié (TNS), commerçant, artisan, profession libérale. Identifier les dispositifs mobilisables (OPCO, plan de développement des compétences, autofinancement...) en cliquant ici.

5. Programme de formation détaillé

Personnalisation : le programme peut être modifié en fonction de vos besoins et de vos objectifs, sur le contenu, la durée, les modalités, les moyens pédagogiques et techniques.

Comprendre les menaces et enjeux de sécurité de WordPress ***Jour 1 - matin***

Architecture WordPress et surface d'attaque : noyau, thèmes, extensions et base de données

Panorama des menaces courantes

Failles de sécurité exploitées par des attaques automatisées (scans, brute force, injections)
Piratage, défacement du site et vol de données
Conséquences pour l'entreprise : blacklistage par Google, perte de référencement, atteinte à l'image

Adopter une culture de la vigilance et les bons réflexes de sécurité au quotidien

Sauvegarder son site pour pouvoir réagir ***Jour 1 - matin***

Stratégie de sauvegarde : fichiers et base de données, fréquence et durée de rétention
Solutions de sauvegarde : extension dédiée et sauvegarde côté hébergeur
Vérifier et tester une restauration de sauvegarde

Maintenir son site à jour, premier rempart de sécurité ***Jour 1 - matin***

Cycle de versions WordPress et procédure de mise à jour sécurisée : sauvegarde ? test ? production
Mise à jour des extensions et des thèmes : utilité, obsolescence, réputation de l'éditeur
Sources de téléchargement fiables et suppression des extensions et thèmes inutilisés

Durcir l'accès et l'administration du site ***Jour 1 - après-midi***

Renforcement des identifiants et authentification à deux facteurs
Limitation des tentatives de connexion et protection de la zone d'administration (wp-admin, wp-login.php)
Gestion des rôles et des permissions utilisateurs selon le principe du moindre privilège

Mettre en place des protections actives ***Jour 1 - après-midi***

Extensions de sécurité : pare-feu applicatif, scan de malwares et alertes
Certificat SSL (HTTPS) et choix d'un hébergeur fiable
Vigilance face au phishing et aux e-mails frauduleux ciblant les administrateurs de site
Cas pratique : diagnostiquer et sécuriser un site de démonstration après une tentative d'intrusion simulée

Détecter, réagir et organiser la sécurité dans la durée ***Jour 1 - après-midi***

Signaux d'un site compromis et premiers réflexes de diagnostic
Procédure de réaction face à un incident : isolement, restauration de sauvegarde, changement des identifiants
Élaboration d'une check-list de vigilance récurrente et sensibilisation des autres utilisateurs du site
Questions / réponses et synthèse de la formation

Formation ajoutée le 26/09/2026.

PROCHAINES DATES INTER-ENTREPRISE

Nous n'avons pas encore planifié de session inter-entreprise pour cette formation.
Elle est toutefois proposée en intra-entreprise.