

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.



Objectifs pédagogiques

Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques



Pré-requis

Une réelle connaissance informatique est nécessaire



Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.



Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

Responsable, technicien, correspondant informatique

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales...



Programme de formation

Accueil et introduction

- Accueil des participants
- Présentation de l'objectif du cours
- Brève introduction à la cybersécurité

Les menaces en ligne pour les TPE et PME

- Les principales menaces en ligne : phishing, ransomware, malware, etc
- Les menaces venant de l'intérieur : virus, vol de données, destruction de données...
- Exemples de cas réels de cyberattaques contre les petites entreprises
- Les conséquences financières et de réputation des cyberattaques

Contacts



Notre centre à **Mérignac**

14 rue Euler
33700 MERIGNAC

☎ 05 57 92 22 00

✉ contact@afib.fr



Notre centre à **Périgueux**

371 Boulevard des Saveurs,
24660 COULOUNIEUX CHAMIERES

☎ 05 64 31 02 15

✉ contact@afib.fr

Bonnes pratiques en cybersécurité

- .. Utilisation de mots de passe forts et uniques
- .. Cryptages de fichiers
- .. Mises à jour régulières des logiciels
- .. Sensibilisation à l'email et aux pièces jointes suspectes
- .. Sensibilisation aux bonnes pratiques : échanges de documents, gestion des comptes...
- .. Travail à distance et prestataires extérieurs
- .. Accès au réseau en interne, Wi-Fi...

Comment sécuriser mon environnement Windows et Microsoft ?

- .. Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11...)
- .. Conseils pour sécuriser mon domaine et Active Directory
- .. Outils et conseils pour sécuriser mon serveur de fichiers
- .. Conseils pour la gestion du réseau et des serveurs applicatifs