PROGRAMME DE FORMATION

La Cybersécurité en Entreprise
Sur une demi-journée

www.afcp-formations.fr

Service Commercial - Tel. 07 88 23 64 37 – mail : contact.afcp.formations@gmail.com
Service administratif - contact@afcp-formations.fr

OBJECTIFS PEDAGOGIQUES

Mesurer les enjeux de la cybersécurité pour protéger les organisations des cyberattaques.

Identifier les menaces potentielles, leurs impacts, et les stratégies adaptées pour les prévenir.

Développer des compétences pratiques pour anticiper et réagir efficacement aux incidents

Publics concernés
Toutes personnes pouvant être confrontées à ces situations.

Contenu de la formation
Connaissances théoriques et pratiques

Pré requis
Aucun

Compétences formateurs
Formateur Spécialisé en Cybersécurité

Durée de la formation
3 heures/40 en présentiel

Effectif
12 personnes maximum/session

Maintien des connaissances
Recyclage à prévoir tous les ans en raison de l'évolution des actes de malveillance.

Méthode et moyens pédagogiques
Une salle de cours
Paperboard à mettre à disposition par le client.
Vidéoprojecteur ou écran tactile.
Anticiper les risques et les menaces et réagir face à une attaque.

Moyen d'évaluation
Interaction avec le formateur.thématique
Quizz.
Une attestation de fin de formation permettant de valider les compétences acquises.

Modalités, délais d'accès et contact
Pour bénéficier de cette formation, vous devez vous inscrire auprès de
contact.afcp.formations@gmail.com
Tel. 0686404247
Tarif intra : **sur devis**
Délais d'accès 15 jours à partir de la date de prise de contact.

Modules - Contenu - Durée

Accueil - 30 minutes
- Présentation générale de la formation et ses objectifs

2 – Concepts de la cybersécurité - 30 minutes
- Définition des menaces principales (phishing, ransomware, DDoS)
- Importance de la sensibilisation au sein des entreprises
- Identification des impacts potentiels : pertes financières, atteinte à la réputation, risques légaux

3 – Scénarios malveillants - 40 minutes
- Etudes de cas : phishing, cyberattaques internes.
- Analyse des techniques de cyberattaques et ingénierie sociale.
- Comparaison des impacts sur des entreprises protégées et non protégées

4 – Stratégies de protection - 40 minutes
Approches de prévention : règles de sécurité, gestion des accès, sauvegardes.
- Exercices collaboratifs : identification des menaces et élaboration de solutions

5 – Gestion des incidents - 30 minutes
- Cas pratiques : intrusions, fuites de données, espionnage économique.
- Préparation à une réponse adaptée : plan d'urgence et actions corrective.

6 - Bilan de la formation (25 minutes)
Quizz
Fiche de satisfaction

Accessibilité : nous étudions au cas par cas toutes les situations de handicap afin d'envisager une intégration dans la formation. Dans le cas contraire, nous prévoyons une orientation vers des organismes appropriés. Il appartient aux clients en INTRA, de s'assurer que les locaux de formation soient accessibles aux personnes en situation de handicap.