PROGRAMME DE FORMATION

Cybersécurité débutant

DURÉE : 1 jours I 7 heures

MODALITÉ D'ORGANISATION : Mixte

Informations

PUBLIC VISÉ

Responsables RSE, DPO, juristes, responsables informatiques et dirigeants chargés d'encadrer les usages de l'IA.

OBJECTIFS PÉDAGOGIQUES

Identifier les principales menaces de cybersécurité et leurs impacts sur l'entreprise.

Mettre en œuvre des mesures de protection simples (sauvegardes, mots de passe, antivirus).

Adopter les bonnes pratiques pour sécuriser ses usages numériques.

Construire une charte informatique adaptée à son organisation.

Détecter les signaux d'intrusion et adopter les bons réflexes en cas d'attaque.

PRÉREQUIS

Avoir des connaissances de base de l'environnement informatique.

ACCESSIBILITÉ

Si vous êtes en situation de handicap, merci de nous contacter afin que nous puissions vous accompagner et vous orienter au mieux dans votre demande et vos démarches.

Modalités pédagogiques

MODALITÉS

Formation dispensée en présentiel ou à distance (sur demande) par un formateur expert dans ce domaine : apports théoriques, exercices de mise en situation professionnelle.

MOYENS ET SUPPORTS PÉDAGOGIQUES

Programme, supports et fiches pratiques remis aux stagiaires. Supports pédagogiques utilisés : vidéos, documents PDF, PowerPoint et quiz.

MODALITÉS D'ÉVALUATION ET DE SUIVI

Avant la formation : audit des besoins et du niveau

En cours de formation : Évaluation en continu de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur lors de mises en situation et cas pratiques.

À la fin de la formation : évaluation de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur, évaluation des acquis : Quiz/QCM de fin de module.

Formation qualifiante : certificat de réalisation en fin de formation

Contenu pédagogique

01 - Introduction et tour de table

- Présentation des étapes et thématiques abordées : sommaire du module/parcours de formation.
- Validation des objectifs avec chaque apprenant.
- Tour de table guidé : échanges et positionnement des acquis et des besoins de chacun.

02 - Introduction à la cybersécurité et typologie des menaces en cybercriminalité

- Définition et enjeux de la cybersécurité : contexte réglementaire et obligations légales.
- Impact des cyberattaques sur les entreprises.
- Les principales attaques : phishing, ransomware, ingénierie sociale, études de cas et exemples concrets.
- Comment identifier une menace, méthodes d'identification des attaques.

03 - Bonnes pratiques en sécurité informatique au quotidien

- Gestion des mots de passe et authentification sécurisée : sécurisation des accès aux applications, aux données, usage des réseaux et appareils.
- Sensibilisation aux comportements à risque (emails, téléchargements, réseaux Wi-Fi...).
- Identifier les signes d'une cyberattaque : les bonnes pratiques en cas de suspicion d'intrusion, Protocoles internes et réflexes à adopter.
- Présentation d'outils de surveillance et d'alerte.

04 - Mise en oeuvre des mesures de protection

- Mise à jour et gestion des antivirus et pares-feux.
- Stratégies de sauvegarde et protection des données.
- Gestion des accès et rôles des utilisateurs.
- Objectifs et contenu d'une charte informatique : rédaction et diffusion de la charte en entreprise.
- Étude de cas, mise en place d'une politique de sécurité.

05 - Valider les acquis et clôturer la formation

- Bilan et évaluation finale de la formation.
- Enquête de satisfaction à chaud.

Modalités d'évaluation

Avant la formation : audit des besoins et du niveau

En cours de formation : Évaluation en continu de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur lors de mises en situation et cas pratiques.

À la fin de la formation : évaluation de la compréhension et de l'assimilation des savoirs et savoir-faire par le formateur, évaluation des acquis : Quiz/QCM de fin de module.

Formation qualifiante : certificat de réalisation en fin de formation