SENSIBILISATION CYBERSÉCURITÉ.

Grâce à cette formation, vous acquerrez une vision claire des enjeux de la cybersécurité et des compétences directement applicables dans votre quotidien professionnel : identification des menaces, adoption des bonnes pratiques d'hygiène numérique, gestion des incidents et protection des données sensibles.

Durée

7.00 heures (1.00 jour)

Profils des apprenants

Pour tout le monde.

Prérequis

Aucun prérequis.

Accessibilité et délais d'accès

Pour les personnes en situation de handicap, nous étudions les actions que nous pouvons mettre en place pour favoriser leur apprentissage à travers un questionnaire avant formation. Nous nous appuyons également sur un réseau de partenaires locaux.

Qualité et indicateurs de résultats

Taux de présence VS taux d'abandon, taux de satisfaction à chaud et à froid, taux de réussite à l'évaluation finale.

OBJECTIFS PÉDAGOGIQUES.

- Comprendre les enjeux de la cybersécurité pour les organisations.
- Identifier les principales menaces et vulnérabilités numériques.
- Adopter les bonnes pratiques d'hygiène informatique au quotidien.
- Savoir réagir face à une tentative d'attaque ou un incident.
- Contribuer activement à la mise en place d'une culture cybersécurité dans son organisation.

CONTENU DE LA FORMATION.

Module 1 : Introduction à la cybersécurité

- Définition et enjeux pour les entreprises
- Panorama des menaces numériques actuelles : Phishing ; Ransomwares ; Malwares ; Ingénierie sociale

Module 2 : Identifier les risques et vulnérabilité

- Exemples concrets d'attaques ciblant les entreprises
- Analyse des impacts potentiels pour une TPE/PME

Module 3 : Les bonnes pratiques d'hygiène informatique

- Sécurisation des postes de travail : mots de passe ; mises à jour ; sauvegardes
- Sécurité des emails et de la navigation web
- Bonnes pratiques en télétravail et mobilité

Module 4 : Réagir face à un incident

- Détection des signaux d'alerte.
- Gestes réflexes en cas d'attaque ou de suspicion.
- Communication interne et remontée des incidents.

Module 5 : Construire une culture cybersécurité

- Sensibiliser et impliquer l'ensemble des collaborateurs.
- Mettre en place des réflexes collectifs simples et efficaces.
- Valoriser la cybersécurité comme facteur de confiance et de pérennité.

ORGANISATION DE LA FORMATION.

Équipe pédagogique

Notre équipe pédagogique maîtrise l'ensemble des sujets proposés à la formation. Nous construisons nos programmes en identifiant les besoins en compétences des futurs apprenants et en collaboration avec nos experts métiers. Axio Formation repose sur une approche personnalisée pour chaque parcours professionnel.
Nous concevons des formations qualifiantes qui non seulement répondent à vos besoins spécifiques, mais vous préparent aussi à exceller dans votre domaine.

Pour tout besoin lié à la pédagogie, notre référente est Maud : maud.hoffmann@axio-formation.com
Pour tout besoin d'ordre administratif, notre référente est Emilie : emilie.vannieuwenborg@axio-formation.com

Moyens pédagogiques et techniques

- **En présentiel** : Accueil des participants dans une salle dédiée à la formation. Documents supports de formation projetés. Etudes de cas concrets. Quizz et activités collectives en salle; Mise à disposition en ligne de documents supports à la suite de la formation
- **En distanciel** : Classes virtuelles via l'interface Digiforma. Support de formation partagé. Activités d'entrainement en synchrone

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation.

- Feuilles d'émargement
- Autoévaluation de niveau en début de formation et fin de formation
- Evaluations d'entrainement tout au long de la formation
- Questionnaire de satisfaction à chaud et à froid.

FORMATION ÉLIGIBLE AU OPCO !