



crews
Where you belong

FORMATION

Cybersécurité

OBJECTIFS PÉDAGOGIQUES

- Comprendre les principaux risques et menaces liés à la cybersécurité
- Adopter les bonnes pratiques pour protéger ses données et ses outils
- Identifier et prévenir les principales tentatives de cyberattaque
- Mettre en place des mesures de sécurité adaptées à son environnement professionnel

DURÉE DE LA FORMATION

2 jours (14 heures)

PUBLIC VISÉ

Professionnels souhaitant renforcer la sécurité de leurs usages, données et outils numériques

PRÉ-REQUIS

Aucun

DÉLAIS D'ACCÈS

Admissibilité sur dossier et échange avec l'équipe Experience : réponse sous 48 heures

TARIF

- Formation inter-entreprise : 1 890 euros HT par personne
- Formation intra / sur mesure : sur devis



crews

Where you belong

PROGRAMME DÉTAILLÉ

- Comprendre les fondamentaux de la cybersécurité
 - Identifier les principaux enjeux de la sécurité numérique
 - Comprendre les différents types de cybermenaces
 - Identifier les vulnérabilités courantes dans un environnement professionnel
- Identifier les principales cyberattaques
 - Reconnaître les tentatives de phishing et d'ingénierie sociale
 - Comprendre les risques liés aux malwares et ransomwares
 - Identifier les comportements et situations à risque
- Sécuriser ses accès et ses outils
 - Créer et gérer efficacement ses mots de passe
 - Mettre en place l'authentification multifacteur
 - Sécuriser ses comptes, appareils et connexions
- Protéger ses données
 - Identifier les données sensibles de son organisation
 - Adopter les bonnes pratiques de stockage et de partage
 - Mettre en place des sauvegardes et limiter les risques de perte
- Sécuriser ses usages professionnels
 - Utiliser de manière sécurisée les emails et outils collaboratifs
 - Maîtriser les risques liés au télétravail et aux réseaux externes
 - Contrôler les accès et permissions accordés aux différents outils
- Réagir face à un incident de sécurité
 - Identifier les signes pouvant révéler une compromission
 - Adopter les premiers réflexes en cas d'incident
 - Comprendre les étapes de signalement et de gestion d'une cyberattaque
- Atelier de mise en pratique
 - Analyser les risques d'un environnement professionnel
 - Identifier les principales vulnérabilités et actions prioritaires
 - Construire un plan d'actions pour renforcer durablement sa cybersécurité

**crews**

Where you belong

DÉBOUCHÉS, PASSERELLES ET SUITES DE PARCOURS

À l'issue de la formation, les apprenants pourront identifier les principales cybermenaces, sécuriser leurs usages et données professionnels, adopter les bons réflexes face à une tentative d'attaque et mettre en œuvre des mesures permettant de réduire les risques numériques au sein de leur organisation.

MÉTHODES, MOYENS PÉDAGOGIQUES ET ENCADREMENT

- Animation des formations par des professionnels du digital activité
- Méthodes pédagogiques variées et dynamiques (études de cas, ateliers et travaux)
- Encadrement individuel par l'équipe Experience

MOYENS POUR SUIVRE LA FORMATION

- Suite d'outils technologiques performants : Google Workspace for Education, Edusign...
- Cas pratiques sur des situations réelles d'entreprises

MOYENS D'ÉVALUATIONS

- Évaluation des acquis en fin de formation via un quizz ou un rendu de projet

RÉSULTATS ET INDICATEURS DE PERFORMANCES

- Taux de satisfaction en fin de formation : NA
- Taux d'assiduité : NA

ACCESSIBILITÉ

Accessibilité des personnes en situation de handicap, RQTH, ou difficultés particulières, nous contacter pour organiser un entretien et vous proposer un programme adapté à vos besoins : handicap@crews-education.com

Accessibilité des publics internationaux, nous contacter : international@crews-education.com

CONTACTS

- Par téléphone : +33(0)4 80 81 94 50
- Par WhatsApp : +33(0)7 56 10 93 20
- Par email : contact@crews-education.com