

Sensibilisation à la cybersécurité

Référence : **SECSENSIB**

Durée : **1 jour (7 heures)**

Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucun prérequis

PROFIL DES STAGIAIRES

- Tous les salariés d'une entreprise

OBJECTIFS

- Découvrir les bonnes pratiques pour limiter les risques juridiques et opérationnels
- Comprendre comment protéger les informations en adéquation avec les besoins métiers

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- Une pédagogie active et ancrée dans le réel : Alternance d'apports théoriques courts et d'activités pratiques ; Approche par la mise en action ; Ancrage métier ; Évaluation continue
- Formats et adaptation selon le contexte : Présentiel (inter Paris, Lyon, Nantes, Rennes, Toulouse, Pau/ intra partout en France) ; Distanciel synchrone (classe virtuelle) ; Distanciel asynchrone
- Une dimension innovante : Serious game Phishing Game ; Atelier Plan d'hygiène numérique ; Auto-diagnostic cybersécurité ; Continuité pédagogique
- Moyens pédagogiques et techniques mobilisés : Plateforme Internet pour héberger les supports, quiz et ressources complémentaires ; Supports de formation numériques (présentation, fiches pratiques, modèles de mots de passe, trames de plan d'hygiène numérique) ; Ordinateurs ou tablettes connectés pour les ateliers pratiques et simulations ; Accompagnement par un formateur expert en cybersécurité, garantissant un transfert de compétences concret et adapté aux TPE/PME
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

- Consultant-formateur expert Cybersécurité

MÉTHODES D'ÉVALUATION DES ACQUIS

- Avant la formation : test de positionnement ou de validation des prérequis
- Pendant la formation : les évaluations formatives sous plusieurs formes (exercices, quiz...)
- A la fin de la formation : Evaluation sommative sous forme de quiz général ou étude de cas qui permet de s'assurer de l'atteinte des objectifs de la formation ; Evaluation satisfaction remplie par chaque apprenant
- Après la formation : Evaluation à froid, un mois après la session de formation
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Comprendre les enjeux de la cybersécurité (1h30)

- Panorama des menaces actuelles (ransomware, phishing, fraude, fuite de données)
- Impacts sur l'activité : pertes financières, atteinte à l'image, arrêt de production
- Obligations légales et réglementaires (RGPD, confidentialité des données)
-  **Activités** : Étude de cas d'une cyberattaque en entreprise ; Échange interactif sur les risques propres au secteur des participants

2. Identifier les menaces et comportements à risque (2h)

- Ingénierie sociale et phishing : tactiques, indices visuels, exemples concrets
- Mots de passe faibles, absence de double authentification
- Mauvaises pratiques de navigation, d'usage des messageries et supports amovibles
-  **Activités** : Atelier « Phishing Game » : détection d'emails frauduleux ; Quiz interactif sur les comportements à risque

3. Adopter une hygiène numérique efficace (3h30)

- Gestion sécurisée des mots de passe (MFA, coffres-forts numériques)
- Sauvegardes et mises à jour régulières
- Bonnes pratiques sur postes de travail, mobiles et en télétravail
- Gestion sécurisée des données et de leur partage
- 💡 *Activités : Configuration MFA et création de mots de passe robustes ; Atelier Plan d'hygiène numérique : checklist personnalisée pour l'équipe*

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .