CYBERSÉCURITÉ - SENSIBILISATION AUX MENACES ET BONNES PRATIQUES

1 jours (7 heures en présentiel ou 7 heures à distance en classe virtuelle)

Compétences visées

À l'issue de la formation, les participants seront capables d'identifier les menaces liées à la cybercriminalité, de détecter les intrusions courantes, et d'adopter des comportements sécurisés. Ils sauront hiérarchiser les données sensibles à protéger, mettre en œuvre des mesures de sécurité (gestion des mots de passe, mises à jour, sauvegardes) et élaborer une charte informatique adaptée à leur structure.

Objectifs pédagogiques

Cette formation vise à sensibiliser les participants aux risques majeurs en matière de cybersécurité et à leur fournir les clés pour y faire face. Les stagiaires apprendront à reconnaître les types d'attaques les plus fréquentes, à adopter des pratiques responsables et à structurer leur environnement numérique de manière plus résiliente. Une attention particulière sera portée à la mise en place d'une charte informatique, outil essentiel pour formaliser les règles de sécurité au sein de l'entreprise.

Population visée

Toute personne travaillant en environnement numérique, tous secteurs confondus : collaborateurs, responsables d'équipe, fonctions support, indépendants.

Pré-requis

Aucun prérequis technique n'est nécessaire. Il est recommandé d'être utilisateur régulier d'outils numériques (mail, bureautique, web…).

Procédures de positionnement et d'évaluation des acquis à l'entrée de la prestation

Audit téléphonique d'un conseil-formation pour s'assurer des pré-requis et des besoins de l'apprenant, complété d'un audit de niveau via un formulaire à remplir, soumis à l'analyse du formateur-référent.

Méthodes pédagogiques

8 participants maximum, un poste par stagiaire et un support de cours est envoyé en fin de stage (vidéos tutorielles et/ou support spécifique). La formation est constituée d'apports théoriques, de démonstrations et de mises en pratique basées sur des exercices applicatifs et/ou ateliers.

Formateur

Formateur expert dans le domaine de la protection des données.

Modalités de validation des acquis

Évaluation continue via des exercices applicatifs et/ou des ateliers de mise en pratique.
Évaluation en fin de stage par la complétion d'un questionnaire et/ou d'une certification officielle issue du Répertoire Spécifique.

Contenu

Introduction à la cybersécurité

- Définition et typologie des menaces : virus, phishing, ransomware, etc.
- Exemples récents d'attaques et conséquences

Adopter les bonnes pratiques pour sécuriser son environnement

- Mots de passe : unicité, complexité, gestion
- Mises à jour, antivirus, sauvegardes : pourquoi et comment
- Identification des données sensibles à protéger

Détecter les menaces et réagir efficacement

- Signes d'une attaque ou d'une intrusion
- Réactions à adopter en cas de suspicion
- Rôle de chacun dans la chaîne de sécurité

Élaborer une charte informatique interne

- Définir les règles internes via une charte informatique
- Modèle de charte à adapter selon les contextes
- Communication et diffusion de la charte auprès des équipes

CYBERSÉCURITÉ - SENSIBILISATION AUX MENACES ET BONNES PRATIQUES

Émargement quotidien d'une feuille de présence (en présentiel ou en ligne).
Complétion par le formateur/la formatrice d'un suivi d'acquisition des objectifs pédagogiques.
Remise d'une attestation individuelle de réalisation.