CYBERSÉCURITÉ – DIRECTION ET GESTIONNAIRE

PROTÉGEZ L'AVENIR NUMÉRIQUE DE VOTRE ORGANISATION

Durée : 3 heures

Prérequis :

- Aucune connaissance préalable en cybersécurité requise.
- Avoir accès à un ordinateur avec une connexion Internet.

Moyens pédagogiques :

- Formation en ligne, en mode asynchrone
- Supports de formation inclus

Compétences acquises à l'issue de la formation :

- Élaborer des politiques internes robustes de cybersécurité
- Encadrer la gestion des accès, des sauvegardes et des appareils
- Créer un plan d'action pour la gestion des incidents

Attestation : oui

DESCRIPTION

Cette formation, spécialement conçue pour l'équipe de direction, met l'accent sur l'importance de mettre en place des politiques internes robustes de cybersécurité. Vous découvrirez que posséder des connaissances en cybersécurité et adopter de bonnes pratiques en ligne est essentiel, mais insuffisant si ces pratiques ne sont pas partagées et adoptées par l'ensemble de vos équipes. Si vous souhaitez comprendre les risques associés aux cyberattaques, mais surtout les anticiper et les neutraliser efficacement grâce à des politiques claires et des protocoles rigoureux, vous êtes au bon endroit. Savoir, c'est pouvoir, mais partager ce savoir, c'est sécuriser sur le long terme votre organisation.

PROGRAMME :

Objectif général

- Sécuriser de manière proactive l'accès à vos données et pérenniser les bonnes habitudes en ligne au sein de vos équipes.

Objectifs spécifiques

- Développer un calendrier d'entretien régulier pour tous les appareils.
- Assurer une mise à jour régulière des droits d'accès en fonction des changements de rôles.
- Adopter de bonnes pratiques de sauvegardes.
- Mettre en place des critères de création de mots de passe robustes.
- Assurer la bonne gestion des courriels envoyés et reçus.
- Maintenir des connexions sécurisées, notamment en télétravail.
- Encadrer l'usage des outils d'intelligence artificielle en interne.
- Définir des directives claires pour l'utilisation des appareils personnels dans un cadre professionnel.
- Assurer une gestion sécurisée en cas de départ d'un membre de l'équipe.
- Créer un plan d'action clair et pratique pour la gestion des incidents de cybersécurité.

QUESTIONS/RÉPONSES