PROGRAMME DE FORMATION
"CYBERSÉCURITÉ, SENSIBILISATION"

Objectifs de la formation :

- Comprendre les différents types de menaces en cybercriminalité
- S'acculturer aux bonnes pratiques (mot de passe unique par système…etc)
- Détecter les intrusions et réagir face aux malveillances et comprendre les risques et les enjeux de sécurité
- Déterminer les données importantes à protéger et comprendre les actions à mettre en œuvre pour protéger les données importantes (mise à jour, antivirus, gestion des accès, sauvegarde…)
- Mettre en œuvre une charte informatique à partager en interne (les pratiques)

PUBLIC CONCERNÉ :
Tout public salarié

PRÉ-REQUIS :
Aucun

POSITIONNEMENT :
Echanges par mails, téléphone ou rencontre physique.

MODALITÉS D'ORGANISATION :

Durée : 7 h en distanciel.

Horaires : 9 h 00 - 12 h 30 / 13 h 30 - 17 h 00.

Dates de la formation : à définir ensemble.

COÛT DE LA FORMATION :

1 200,00 € / personne.
2 800,00 € / H

Financement OPCO possible.

Trouvez le vôtre !

**Organisme non soumis à la TVA, Art. 261.4.4 a du Code général des Impôts*

Contenu :

1. Introduction à la cybercriminalité et aux menaces- 1,5 H

- Identifier les principaux types de cybermenaces (phishing, ransomwares, malwares…).
- Comprendre les enjeux et risques de sécurité pour une entreprise.
- Sensibilisation aux impacts des cyberattaques.

2. Bonnes pratiques et protection des données-1,5 H

- Adoption des bonnes pratiques (gestion des mots de passe, MFA, navigation sécurisée).
- Déterminer les données sensibles à protéger.
- Stratégies de protection : mises à jour, antivirus, gestion des accès.

3. Détection et réaction face aux menaces-2 H

- Identifier les signaux d'intrusion et comportements suspects.
- Réagir en cas d'attaque : premiers réflexes et procédures internes.
- Sauvegarde et récupération des données après une cyberattaque.

4. Mise en place d'une politique de cybersécurité interne-2 H

- Élaborer une charte informatique adaptée à l'entreprise.
- Sensibiliser et former les collaborateurs aux bonnes pratiques.
- Intégrer la cybersécurité dans les processus quotidiens.

Modalités pédagogiques :
- Distanciel synchrone
- Méthode interrogative afin que les participants soient acteurs de leur formation et assimilent en mettant en pratique de suite les enseignements.

Modalités d'assistance technique :
- Possibilité nous joindre par téléphone ou mail.

Modalités de positionnement :
- Positionnement en 2 étapes :
- Contact avec les entreprises pour connaitre le besoin des inscrits, leur poste, niveau de compétences. Tour de table en arrivant en formation.

Modalités d'évaluation :
- Évaluation des acquis via un questionnaire en amont de la formation *(via Digiforma)* dès l'inscription.
- Évaluation des acquis aussi lors de la définition des objectifs au démarrage de la formation.
- Évaluation finale via un questionnaire après chaque séquence et en fin de formation *(via Digiforma)*

Moyens techniques :
- Mise en situation, questionnaires, exercices pratiques, andragogie, adaptation au public, Paperboard, rétroprojecteur, exercice papier et sur ordinateur.

contact@formagestion.fr
06.23.55.48.78

Formagestion est déclaré sous le N° 32591153959
auprès de la DREETS de Lille - Siret : 903 645 711 00016