Plan d'Action de Formation

Centre de formation · N° 82 38 02069 38 · Inscrit auprès du Préfet de la région Rhône-Alpes

Bureautique – Sensibilisation cybersécurité

Niveau 1

1 Objectifs pédagogiques

- Comprendre les menaces en ligne
- Savoir identifier les pratiques de sécurité de base
- Reconnaître les signaux d'alerte d'une cyberattaque
- Comprendre l'importance de la protection des données
- Savoir réagir en cas d'incident de sécurité

2 Prérequis, public concerné

- Connaissance générale de l'informatique : Compréhension de base de l'utilisation des ordinateurs, des réseaux et d'Internet

3 Durée

- Entre 1 et 4 jours : adaptable selon le niveau et le périmètre, définie avec le client

4 Tarif

- À partir de 820 € HT par jour de formation, en intra jusqu'à 6 participants — devis personnalisé sur demande

5 Moyens pédagogiques

- (Formation INTRA ENTREPRISE 6 participants maximum)
- Présentations interactives / dynamiques
- Exercices de simulation : Organisez des exercices de simulation où les participants doivent réagir à des scénarios d'attaques informatiques pour tester leurs connaissances et leurs compétences en matière de sécurité
- Débats et discussions
- Ressources en ligne(vidéos éducatives et des guides pratiques pour approfondir leur compréhension de la cybersécurité.)

6 Méthode pédagogique

- Pédagogie active et participative
- La formation consiste à dérouler de manière détaillée le programme de formation en effectuant des manipulations et des exemples

7 Évaluation de la formation

- L'évaluation des connaissances se fait de façon continue, tout au long de la formation. En effet, dans cette partie du stage, il est demandé aux stagiaires d'appliquer pratiquement les connaissances théoriques apprises précédemment en utilisant les options des programmes qui ont été présentées. Les stagiaires, sous le contrôle du formateur, sont mis en situation de travail avec les programmes. Mise à disposition d'une assistance téléphonique
- Délivrance d'une attestation de stage

8 Délais d'intervention

- 4 Semaines selon disponibilité

9 Accessibilité aux personnes en situation de handicap

- Nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation

★ Programme détaillé de la formation

Introduction à la cybersécurité :

- Sensibilisation aux menaces et aux attaques courantes
- Compréhension des enjeux de sécurité informatique pour l'entreprise
- Rôle de chaque employé dans la protection des données et des systèmes

Formation sur la gestion des mots de passe :

- Bonnes pratiques pour la création et la gestion des mots de passe forts
- Utilisation de gestionnaires de mots de passe sécurisés
- Risques liés à la réutilisation de mots de passe et aux mots de passe faibles

Formation sur la protection contre les logiciels malveillants :

- Identification des types de logiciels malveillants (virus, ransomware, etc.)
- Techniques pour éviter les logiciels malveillants, comme la prudence lors du téléchargement de fichiers et la mise à jour régulière des logiciels

Formation sur la sécurité des e-mails :

- Reconnaissance des e-mails de phishing et des techniques d'ingénierie sociale
- Protocoles de sécurité pour les e-mails, tels que la vérification des expéditeurs et des pièces jointes

Formation sur la sécurité des appareils mobiles :

- Bonnes pratiques pour sécuriser les appareils mobiles utilisés pour le travail
- Utilisation de mots de passe, de chiffrement et de solutions de gestion des appareils mobiles

Formation sur la sécurité des réseaux :

- Utilisation sécurisée des réseaux Wi-Fi publics et privés
- Sécurisation des réseaux d'entreprise, y compris l'utilisation de VPN et de pare-feu

Formation sur la conformité et la protection des données :

- Connaissance des réglementations en matière de protection des données, telles que le RGPD
- Protocoles de sécurité pour la collecte, le stockage et le partage de données sensibles

Formation sur les réponses aux incidents de sécurité :

- Procédures à suivre en cas de suspicion de violation de sécurité
- Signalement des incidents de sécurité et collaboration avec l'équipe informatique pour résoudre les problèmes

Accessibilité Handicap : Cliquez ICI

Règlement intérieur à l'intention des participants : Cliquez ICI