Laho
TERRE DE FORMATIONS
CCI HAUTS-DE-FRANCE

WEB ET DIGITAL

FORMATION CONTINUE

CYBERSÉCURITÉ
SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

A partir de 490€ nets de taxes.

100% présentiel

Public visé : Tout utilisateur régulier d'un ordinateur

Prérequis : Sans niveau spécifique

Accessibilité aux personnes handicapées
Contactez-nous pour une étude de vos besoins.

Prochaines sessions

AULNOY-LEZ-VALENCIENNES
SESSION 1 : 16 octobre

BEAUVAIS
SESSION 1 : 06/09/2024

LAON
SESSION 1 : 07/11/2024

LENS
SESSION 1 : 01/10/2024

ROUBAIX
SESSION 1 : 10/09/2024

98%
DE TAUX DE SATISFACTION

60
ANNÉES D'EXISTENCE ET D'EXPÉRIENCE

450
FORMATIONS DISPONIBLES

Objectifs

Prendre conscience des enjeux et des risques relatifs à la cyber sécurité dans une organisation
Connaître les acteurs et les ressources de la cyber sécurité
Identifier les menaces potentielles et savoir réagir
Mettre en œuvre les bonnes pratiques pour se prémunir des risques liés à la sécurité des systèmes d'information

Les + de la formation

- Formation pratique et applicable de suite
- Cette formation peut bénéficier d'un financement de la Région Hauts-de-France pour les PME à hauteur de 50% du coût estimé pour l'entreprise

BESOIN D'ÊTRE CONTACTÉ(E) POUR PLUS D'INFORMATIONS OU POUR UN DEVIS ?
APPELEZ NOTRE CONSEILLER pour un premier entretien GRATUIT et SANS ENGAGEMENT.
N° Vert 0 805 384 384 formationcontinue@laho-formation.fr

CYBERSÉCURITÉ
SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

Contenu de la formation

Découpage par demi-journée :

Beaucoup d'entreprises ont tendance à négliger l'importance de la cybersécurité jusqu'à ce qu'un incident se produise ! Sensibiliser les salariés aux enjeux de la cybersécurité permet de se prémunir contre les cybermenaces, de se conformer aux réglementations, de protéger les données sensibles, d'inculquer une culture sécurité et d'éviter les lourdes conséquences financières d'une attaque.

1. Les entreprises face au risque de cybermalveillance, la réglementation et les acteurs

Introduction à la cybersécurité

- **Définition et importance de la cybersécurité**
- **État actuel des cybermenaces dans le secteur de la santé**
- **Impacts potentiels des cyberattaques sur l'organisation**

Panorama des principales menaces

- Phishing et ingénierie sociale
- Malwares (virus, ransomwares...)
- Attaques par déni de service
- Vol de données

Réglementation et conformité

- RGPD et protection des données personnelles
- Obligations légales en matière de sécurité des systèmes d'information
- Responsabilités individuelles et collectives

Mise en pratique

- Identification d'emails de phishing
- Quiz interactif sur les bonnes pratiques

BESOIN D'ÊTRE CONTACTÉ(E) POUR PLUS D'INFORMATIONS OU POUR UN DEVIS ?
APPELEZ NOTRE CONSEILLER pour un premier entretien GRATUIT et SANS ENGAGEMENT.
N° Vert 0 805 384 384 formationcontinue@laho-formation.fr

CYBERSÉCURITÉ
SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

Contenu de la formation

2. Les bonnes pratiques et les bons usages

Bonnes pratiques d'hygiène informatique

- Gestion des mots de passe
- Mises à jour et antivirus
- Sécurisation des appareils mobiles
- Navigation web sécurisée
- Utilisation sûre de la messagerie

Sécurité physique et environnementale

- Protection des accès physiques
- Sécurisation des postes de travail
- Politique du bureau propre

Gestion des incidents

- Identification des signes d'une cyberattaque
- Procédure d'alerte et de signalement
- Rôle de chacun dans la gestion de crise

Mise en situation et conclusion

- Scénarios de cyberattaques et réactions appropriées
- Synthèse des points clés
- Questions/réponses

Ce programme couvre les aspects essentiels de la sensibilisation à la cybersécurité, en alternant théorie et exemples concrets. Il est adapté à tous les collaborateurs utilisant des outils numériques, sans prérequis techniques particuliers.

BESOIN D'ÊTRE CONTACTÉ(E) POUR PLUS D'INFORMATIONS OU POUR UN DEVIS ?
APPELEZ NOTRE CONSEILLER pour un premier entretien GRATUIT et SANS ENGAGEMENT.
N° Vert 0 805 384 384 formationcontinue@laho-formation.fr

CYBERSÉCURITÉ
SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE

Modalités, méthodes et outils pédagogiques

Mise en situation Alternance d'apports théoriques et d'exercices pratiques

Résultats attendus

- Etre mieux armé contre la cybermalveillance

Modalités d'évaluation

Remise d'une grille d'auto-évaluation des acquis, sur les compétences travaillées lors de la formation Processus d'évaluation des acquis tout au long de la formation Evaluation de fin de formation individuelle par le formateur

Modalités de financements

Cap Emploi, Entreprise, Opérateurs de Compétences (OPCO), Particulier, Pôle Emploi

Intervenants

- Une équipe de consultants formateurs experts dans le domaine