Laho
TERRE DE FORMATIONS
CCI HAUTS-DE-FRANCE

WEB, DIGITAL ET IA

FORMATION INTER-ENTREPRISES *

1 jour

Cybersécurité : Sensibilisation à la sécurité informatique

à partir de 490 € net de taxe par participant

OBJECTIFS DE LA FORMATION

- Prendre conscience des enjeux et des risques relatifs à la cybersécurité dans une organisation
- Connaître les acteurs et les ressources de la cybersécurité
- 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

PUBLIC VISÉ

Tout public

PRÉ-REQUIS

Sans niveau spécifique

AIDES AU FINANCEMENT **

Cap Emploi
Opérateurs de Compétences (OPCO)
France Travail
Entreprise

*** sous conditions*

MODALITÉS PÉDAGOGIQUES

100% Présentiel

MÉTHODES ET OUTILS PÉDAGOGIQUES

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

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 D'ACCÈS

Bulletin d'inscription
Demande de devis

ACCESSIBILITÉ ET HANDICAP

Contactez-nous

** Toutes nos formations sont possibles en INTRA-ENTREPRISE (devis sur demande).*

FORMATION INTER-ENTREPRISES *

Cybersécurité : Sensibilisation à la sécurité informatique

1 jour

PROGRAMME 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

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.

CETTE FORMATION EST PROPOSÉE DANS NOS CENTRES DE :

ARRAS

Session 1 : 6 octobre 2026

BOULOGNE-SUR-MER

Session 1 : 9 juin 2026

Session 2 : 5 novembre 2026

Laho
TERRE DE FORMATIONS
CCI HAUTS-DE-FRANCE

Retrouvez toutes les informations
sur laho-formation.fr

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**