Fiche de formation
Sensibilisation à la Cybersécurité

CONTACT POUR CETTE FORMATION

Miora RAHARINIRINA
Chargée de mission formation
almond.institute@almond.eu
07 64 42 71 56

- Version 1.0
- 06/12/2023

Sensibilisation à la Cybersécurité

Les objectifs pédagogiques

Cette formation vise à sensibiliser vos équipes aux risques informatiques et à leurs conséquences. Ce module présente les techniques couramment utilisées par les pirates informatiques en vulgarisant le sujet pour un auditoire non technique. Il détaille les bonnes pratiques à adopter pour se prémunir contre la plupart des attaques.

01. Comprendre **les risques cybersécurité les plus courants.**

02. Acquérir **les bonnes pratiques en termes de sécurité.**

03. **Repérer les signes** d'une attaque informatique et **réagir.**

Sensibilisation à la Cybersécurité

Informations pratiques

Public

- Toute personne au sein d'une organisation amené à utiliser le système d'information: Poste de travail, e-mail, smartphone. La formation est construite de manière à être accessible à tous, sans connaissances préalables dans le domaine informatique.

Modalités et délai d'accès

Le stagiaire est considéré inscrit lorsque :

- Les prérequis et besoins sont identifiés et validés
- La convention de formation signée

Les demandes d'inscription peuvent être envoyées jusqu'à 10 jours ouvrés avant le début de la formation.

Prérequis

- Aucun prérequis

Pour aller plus loin

Cette formation permet de préparer la formation suivante :

- Les fondamentaux du risque

Évaluation des acquis

Réalisation d'un questionnaire en ligne final recouvrant l'ensemble des notions apprises.

Accessibilité

Que vous soyez reconnu en situation de handicap ou pas, rendre notre formation accessible à toutes et à tous fait partie de notre engagement.

Si vous avez besoin d'une compensation ou adaptation pour le contenu, les supports, le « lieu », le matériel utilisé, les horaires, le rythme, **nous sommes à votre écoute.**

Sensibilisation à la Cybersécurité

La formation en présentiel ou distanciel

Programme

Introduction – Les enjeux de la cybersécurité	Faiblesses du matériel	Sécurité des périphériques nomades	Mots de passe faibles	Les logiciels malveillants	L'ingénierie sociale
→ La multiplication des attaques et de leurs impacts → Fuites de données importantes → Les sanctions CNIL → Idées reçues → L'impact d'un incident de sécurité → Typologie des attaquants → Le marché noir des failles	→ Les risques des équipements USB → Les recommandations	→ Les risques du nomadisme → Le chiffrement des données → L'effacement des données → Les recommandations	→ Les types d'attaques sur les mots de passe → Exemple de fuites de données massives → Les recommandations	→ Sécurité des réseaux internes → Antivirus → Les mises à jour → Les recommandations	→ Comment la détecter ? → Fraude par email, téléphone, au président → Les recommandations

Les plus de la formation

- Une formation dispensée par un expert en sécurité offensive ayant réalisé de nombreux tests d'intrusion
- Des recommandations opératoires

Tarifs et infos

- **Durée:** 2 heures
- **Tarif:** Contactez-nous
- **Financement:** Prise en charge OPCO