

## La formation en résumé

La cybersécurité est aujourd'hui une priorité pour les entreprises de toutes tailles. Avec la multiplication des cyberattaques, protéger vos données sensibles est essentiel pour garantir la pérennité de votre activité. La formation "**Protéger ses données et réduire les menaces**" vous offre les clés pour comprendre les risques, renforcer vos défenses et adopter de bonnes pratiques au quotidien.

### Objectifs :

- Comprendre les piliers la Sécurité Informatique
- Sécuriser les postes de Travail et les Documents
- Reconnaître et éviter les Menaces par Email
- Optimiser la sécurité des mécanismes d'Authentification
- Naviguer sur Internet en toute Sécurité

### Participants :

Toute personne désireuse de comprendre et gérer les risques liés aux données personnelles

### Prérequis :

Aucun prérequis

## Tarif : sur demande

La durée pourra être adaptée en fonction de vos besoins et attentes



1 jours



(7 heures)



Formation exclusivement sur-mesure

## Dates et villes

Lyon - 04 72 53 88 00

Sessions à venir - Nous contacter

## Le contenu

### Comprendre les Fondements de la Sécurité Informatique

- Expliquer les trois piliers fondamentaux de la sécurité informatique : intégrité, confidentialité, disponibilité.
- Illustrer comment ces concepts interagissent pour assurer une protection complète des données.

### Sécuriser les Postes de Travail et les Documents

- Développer des pratiques de gestion sécurisée des documents et des fichiers sensibles.
- Identifier les risques associés aux ordinateurs partagés et aux failles courantes.
- Apprendre les méthodes efficaces de suppression sécurisée des données

### Reconnaître et Éviter les Menaces par Email

- Identifier les différents types de spam et leurs impacts.
- Comprendre les techniques de phishing et savoir comment les détecter.
- Apprendre à se protéger contre l'usurpation d'identité via des emails malveillants.

### Optimiser la Sécurité des Mécanismes d'Authentification

- Créer des mots de passe robustes et comprendre l'importance de leur gestion.
- Utiliser efficacement les gestionnaires de mots de passe pour simplifier la sécurisation.
- Mettre en œuvre la double identification et explorer les avantages de l'identification biométrique.

### Naviguer sur Internet en Toute Sécurité

- Comprendre l'importance des pare-feu et savoir se protéger sur les réseaux Wi-Fi publics.
- Identifier les différents types de virus, incluant les virus classiques et les rançongiciels, et savoir s'en prémunir.
- Adopter des pratiques sûres sur les réseaux sociaux et lors des achats en ligne.
- Utiliser le Cloud de manière sécurisée pour le stockage et la gestion des données

# Moyens pédagogiques et d'encadrement

## **Moyens pédagogiques et d'encadrement :**

Formation interentreprises avec alternance d'apports théoriques et pratiques.

Pédagogie active : Echanges, analyses de pratiques, mises en situation, cas réels d'entreprises, jeux

Support de formation et ressources mis à disposition des participants.

Groupe de 3 à 12 participants maximum.

Formation animée par un de formateur expert du domaine sélectionné selon un processus qualité certifié.

## **Suivi et évaluation de la formation :**

Les acquis sont évalués en cours et en fin de formation notamment au travers de QCM, mises en situations, mise en pratiques, présentations... Qui feront l'objet d'une analyse/correction et d'un retour du formateur.

Une évaluation de satisfaction est complétée par les participants et un tour de table collectif est réalisé avec le formateur en fin de formation.

## **Matériel requis (si distanciel) :**

Un ordinateur avec une connexion à Internet haut débit

Un microphone et une caméra pour faciliter les échanges en temps réel lors des classes virtuelles

Une adresse mail pour la réception des liens de connexi

