

# CYBERSECURITE : SENSIBILISATION DES UTILISATEURS



## PARTICIPANT(S) :

Tous les collaborateurs, tous niveaux confondus, sans prérequis technique.

## ORGANISATION :

**Durée** : 7 heures

**Lieux** : Campus du lac de Bordeaux ou de Libourne

## INTERVENANT(S) :

Formateur expert en gestion des risques informatiques

## VALIDATION DE LA FORMATION :

L'intervenant mesurera, tout au long de la formation, l'acquisition des connaissances des participants à travers la mise en place de situation in situ.

Délivrance d'une attestation de formation conforme à la législation en vigueur.

Un support de cours sera remis à chaque participant.

### CAMPUS DU LAC

N° SIRET 410 581 102 00010  
Code APE-NAF 8542Z  
N° Existence 7233 042 4333

#### Site de Bordeaux

10 rue René Cassin  
CS 31996  
33071 Bordeaux Cedex  
Tél. 05 56 79 52 00

[campus@formation-lac.com](mailto:campus@formation-lac.com)

#### Site de Libourne

33 rue Max Linder  
33504 Libourne Cedex  
Tél : 05 56 79 52 00

[campus@formation-lac.com](mailto:campus@formation-lac.com)

## PARTIE 1

### OBJECTIFS

#### **Nature de l'action : Acquisition de compétences**

- Comprendre les principaux risques et menaces en matière de cybersécurité.
- Adopter les bonnes pratiques pour protéger les données personnelles et professionnelles.
- Identifier les signaux d'alerte et savoir réagir face à une menace potentielle.
- Sensibiliser à l'impact des comportements individuels sur la sécurité globale de l'entreprise.

### MÉTHODES ET OUTILS PEDAGOGIQUES

- Apports théoriques : Présentations interactives et supports visuels.
- Exercices pratiques : Études de cas, quiz, simulations de menaces.
- Travail collaboratif : Élaboration de bonnes pratiques en groupe.
- Échanges : Questions-réponses et partage d'expériences entre participants.

Ce programme vise à développer une culture de la cybersécurité au sein de l'entreprise en rendant les utilisateurs conscients et acteurs de la protection des données.

### CONTENU DU PROGRAMME

#### **Comprendre les enjeux de la cybersécurité**

##### **Accueil et introduction**

Présentation des participants et de leurs attentes.  
Objectifs de la journée.

##### **Les fondamentaux de la cybersécurité**

Définitions clés : cybersécurité, cybercriminalité, données sensibles.  
Les principales menaces : phishing, ransomwares, vols de données, faux sites.  
Études de cas : exemples concrets d'attaques et leurs impacts.

##### **Identifier les risques et les comportements à risque**

Pourquoi les utilisateurs sont la première cible des cyberattaques.  
Les erreurs humaines courantes : mots de passe faibles, clics sur des liens douteux.  
Atelier interactif : reconnaître un email de phishing ou un site frauduleux.

##### **Adopter les bonnes pratiques et réagir efficacement**

###### **Les bonnes pratiques au quotidien**

Sécurisation des mots de passe : création et gestion (gestionnaires de mots de passe).  
Navigation sur internet : sécuriser les connexions et éviter les pièges.  
Partage de données : utiliser des outils sûrs pour collaborer en ligne.  
Mise à jour et sauvegarde des données : leur importance.

# CYBERSECURITE : SENSIBILISATION DES UTILISATEURS

## **PARTICIPANT(S) :**

Tous les collaborateurs, tous niveaux confondus, sans prérequis technique.

## **ORGANISATION :**

**Durée :** 7 heures

**Lieux :** Campus du lac de Bordeaux ou de Libourne

## **INTERVENANT(S) :**

Formateur expert en gestion des risques informatiques

## **VALIDATION DE LA FORMATION :**

L'intervenant mesurera, tout au long de la formation, l'acquisition des connaissances des participants à travers la mise en place de situation in situ.

Délivrance d'une attestation de formation conforme à la législation en vigueur.

Un support de cours sera remis à chaque participant.

### **CAMPUS DU LAC**

N° SIRET 410 581 102 00010

Code APE-NAF 8542Z

N° Existence 7233 042 4333

#### Site de Bordeaux

10 rue René Cassin

CS 31996

33071 Bordeaux Cedex

Tél. 05 56 79 52 00

[campus@formation-lac.com](mailto:campus@formation-lac.com)

#### Site de Libourne

33 rue Max Linder

33504 Libourne Cedex

Tél : 05 56 79 52 00

[campus@formation-lac.com](mailto:campus@formation-lac.com)

## **PARTIE 2**

### **Réagir face à une menace**

Que faire en cas de phishing ou de tentative d'intrusion ?

Procédure de signalement en interne : qui alerter et comment.

Atelier pratique : simulation d'un incident et mise en œuvre des réflexes de sécurité.

### **Construction d'une charte de cybersécurité**

Atelier collaboratif : élaboration des bonnes pratiques spécifiques à l'entreprise.

Engagement individuel : identifier une action à mettre en place immédiatement.

### **Conclusion et évaluation**

Synthèse des apprentissages.

Plan d'action personnel pour renforcer la cybersécurité.