

# Formation Fondamentaux de la Cybersécurité

## Informations

Durée : 2 jours (14h.)

Tarif\* : Nous consulter

Réf : CYBF

Niveau : Facile

intra

Mise à jour le 30/12/25

\*tarif valable jusqu'au 31/12/2026

## Prochaines sessions

Contactez-nous pour connaître nos futures sessions.

## Pré-requis

- Connaissances de base en informatique
- Utilisation courante d'outils numériques (poste de travail, Internet)
- Aucun prérequis nécessaire en cybersécurité

## Objectifs

Objectifs pédagogiques :

- Comprendre les enjeux et objectifs de la cybersécurité
- Identifier les principales menaces et types d'attaques
- Comprendre les notions fondamentales de sécurité de l'information
- Connaître les bonnes pratiques de protection des systèmes et des données
- Sensibiliser aux comportements à risque

Objectifs opérationnels :

- Identifier les risques de sécurité dans un environnement numérique
- Adopter les bonnes pratiques de sécurité au quotidien
- Reconnaître les tentatives d'attaques courantes (phishing, malwares...)
- Appliquer des règles de base pour sécuriser postes, mots de passe et données
- Contribuer à une meilleure culture cybersécurité dans l'organisation

## Programme

### Jour 1 - Introduction à la cybersécurité et aux menaces

#### Enjeux de la cybersécurité

Pourquoi la cybersécurité est essentielle aujourd'hui  
Impacts financiers, juridiques et organisationnels  
Panorama des cybermenaces  
Notion de risque et de vulnérabilité

#### Principes fondamentaux de la sécurité

Confidentialité, intégrité, disponibilité (CIA)  
Authentification, autorisation et traçabilité  
Défense en profondeur  
Responsabilité des utilisateurs

#### Panorama des menaces

Malwares (virus, ransomwares, spywares)  
Phishing et ingénierie sociale  
Attaques sur les mots de passe  
Attaques réseau et applications

#### Atelier pratique

Analyse de scénarios d'attaques réelles  
Identification des failles exploitées  
Discussion autour des bons réflexes à adopter

### Jour 2 - Bonnes pratiques et premiers mécanismes de protection

#### Sécurité des postes et des accès

Gestion des mots de passe

# Formation Fondamentaux de la Cybersécurité

Authentification forte (MFA)  
Mises à jour et correctifs  
Sécurisation des postes de travail

## Sécurité des données

Protection des données sensibles  
Sauvegardes et restauration  
Chiffrement (principes)  
Partage sécurisé de l'information

## Sensibilisation et hygiène numérique

Comportements à risque  
Sécurité des emails et de la navigation web  
Télétravail et mobilité  
Rôle de l'utilisateur dans la cybersécurité

## Atelier pratique

Détection d'emails de phishing  
Évaluation des pratiques de sécurité existantes  
Élaboration d'une checklist de bonnes pratiques