# Formation Cybersécurité : Fondamentaux de la sécurité et Cyber Hygiène

| | |
|---|---|
| **Durée :** | 1 jours (7 heures) |
| **Public :** | Tous |
| **Pré-requis :** | Connaissance des outils informatiques |
| **Objectifs :** | Comprendre les enjeux de la sécurité d'un réseau informatique et savoir la mettre en œuvre |
| **Référence :** | Cyb1 |
| **Prix:** | 550 €HT / Participant |

## Contexte

Les tentatives d'intrusion des infrastructures sont quotidienne. En adddition, les mauvaises pratiques exposent de façon exponentielle les entreprises à des risques:
- dégradation voire rupture de l'activité,
- Atteinte à l'image de l'entreprise,
- perte financières,
- defaut de conformité (GDPR,...)

Dès lors, comment sensibiliser les utilisateurs à la sécurité informatique et leur faire adopter les bonnes pratiques de manière durable et en adéquation à l'évolution des méthodes de travails ?

## Analyse du risque et des menaces

Enjeux de la sécurité
Panorama des risques et menaces informatiques
Analyse des risques et élaboration des scénarios
Caractérisation des menaces (sources, vulnérabilités, objectif)
Savoir faire un inventaire des menaces caractéristiques
Adéquation risque-menace et disponibilité
**Atelier pratique : élaboration d'un scénario de risque, caractérisation de quelques menaces courantes**

## Les différents niveaux de gestion de la sécurité

Sécuriser les données, les échanges, et le réseau
Sécurité du système d'exploitation, réduction de la surface d'attaque
Sécurité des applications
Gestion des identités
Auditer un système

## Sécurité des données

Les problématiques de l'accès physique
Identification des ressources critiques
Chiffrer les données

## Sécurité des échanges de données

Contraintes de sécurité : intégrité, confidentialité, non-répudiation
Principes de chiffrement, symétrique, asymétrique (clés privées, secret partagé..)
Contraintes liées au support (espionnage, liaisons sans fil..)

## Les bonnes pratiques informatiques en interne comme en externe

Comment reperer et limiter les tentatives de social Ingeneering ?
Connaissez-vous bien votre parc informatique ?
Effectuez-vous des sauvegardes régulières ?
Appliquez-vous régulièrement les mises à jour ?
Utilisez-vous un antivirus/antimalware ?
Avez-vous implémenté une politique d'usage de
mots de passe robustes ?
Avez-vous activé un pare-feu ?
En connaissez-vous les règles de filtrage ?
Comment sécurisez-vous votre messagerie ?
Comment séparez-vous vos usages informatiques ?
Comment maîtrisez-vous le risque numérique
lors des missions et des déplacements professionnels ?
Comment vous informez-vous ? Comment sensibilisez-vous vos collaborateurs?
Savez-vous comment réagir en cas de cyberattaque ?