

 DATE : DURÉE : 7 h

La cybersécurité en entreprise

 **HORAIRES DE FORMATION**
Matin : 9 h 00 – 12 h 30
Après-midi : 13 h 45 – 17 h 15 **LIEU DE LA FORMATION**
Sur site **BÉNÉFICIAIRES** **PRÉREQUIS**

Connaître l'environnement Windows.

 **MODALITÉS PÉDAGOGIQUES
D'ACCOMPAGNEMENT**Animation en face à face présentiel.
Cette formation peut être réalisée
de façon collective ou individuelle. **DÉMARCHE PÉDAGOGIQUE**

- Tour de table en début de module.
- Pour chaque objectif pédagogique et contenu associé :
 - phase initiale de questionnement collectif et mise en contexte ;
 - phase médiane d'appropriation : pédagogie individualisée, en autonomie accompagnée ;
 - phase conclusive collective : réponse aux questions des participant·es, apport de compléments, synthèse et consultation de l'aide-mémoire associé.

 MOYENS ET RESSOURCES

- Mise à disposition d'un PC fixe ou portable muni du logiciel visé (Système d'exploitation : Windows).
- Animation avec vidéoprojection assurée par un formateur ou une formatrice expérimentée, ayant les compétences adaptées aux objectifs pédagogiques.
- Utilisation de supports d'animation pour chaque contenu abordé.
- Remise de supports de conservation numériques à l'issue de la formation

 MODALITÉS D'ÉVALUATIONQuestionnaire d'évaluation
Évaluation du stage à travers
une enquête de satisfaction.

*Nos locaux sont accessibles aux personnes à mobilité réduite.
Si des aménagements concernant par exemple le poste de travail ou les horaires vous semblent requis, contactez-*



Objectifs pédagogiques et contenus

À l'issue de la formation, le bénéficiaire est capable de :

- Comprendre l'importance de la cybersécurité dans le contexte professionnel
- Identifier les principales menaces et comprendre les risques associés.
- Apprendre les bonnes pratiques pour se protéger contre les cybermenaces
- Comprendre comment les erreurs humaines peuvent être exploitées et comment les minimiser.

Introduction et enjeux de la cybersécurité

Définition de la cybersécurité
Importance de la cybersécurité pour les entreprises
Exemples d'incidents de cybersécurité récents et leurs impacts

Menaces et risques cyber

Types de menaces
Techniques d'attaque courantes
Conséquences des cyberattaques pour les entreprises

Bons réflexes et bonnes pratiques

Utilisation de mots de passe sécurisés
Mise à jour régulière des logiciels
Reconnaissance des tentatives de phishing
Sécurisation des appareils mobiles
Utilisation d'un VPN

Réduction des risques liés à l'erreur humaine

Importance de la sensibilisation et de la formation continue
Exemples d'erreurs humaines courantes
Stratégies pour réduire les erreurs

Développer une cyberculture au sein de l'entreprise

Importance de la cyberculture
Rôles et responsabilités de chacun
Intégration de la cybersécurité dans les processus quotidiens