

PROGRAMME DE FORMATION EN PRÉSENTIEL

# CYBERSÉCURITÉ - AVANCÉ

## OBJECTIFS PÉDAGOGIQUES

Sensibiliser les employés aux bonnes pratiques de cybersécurité  
Réduire les risques liés aux cyberattaques  
Comprendre le fonctionnement du Dark Web

Réagir efficacement en cas d'incident  
Éviter les erreurs courantes après une attaque

Nos équipes s'engagent à vous rappeler sous 24 à 72 heures

### Public concerné

Employés non informaticien

### Pré-requis

Connaître les bases informatiques de type bureautique

### Durée de la formation

En distanciel

4 heures

En présentiel

1/2 journée

La durée vous sera confirmée après étude de vos besoins.

### Prix de la formation

En distanciel

Nous consulter

En présentiel intra

À partir de 1000€ ht la 1/2 journée

### Lieu de la formation

Dans vos locaux ou à distance

### Moyens et méthodes pédagogiques

Explications, démonstrations, exercices, vérification des acquis

### Profil du(des) formateur(s)

Plusieurs années d'expérience dans l'enseignement et dans la production.

### Modalités d'évaluation

Questionnaire d'évaluation en fin de session

### Moyens techniques

Un ordinateur par personne. Vidéo projecteur. Connexion Internet

10/2025

► Reconnaître les tentatives de fraude et d'escroquerie  
Identifier les escroqueries en ligne telles que les faux ordres de virement et les arnaques par téléphone  
Prévenir la fuite de données et éviter la divulgation d'informations sensibles  
Participer à un atelier pratique pour appliquer les notions vues  
► Étudier des cas réels d'attaques et comprendre les erreurs commises  
Apprendre la navigation sécurisée sur Internet  
Identifier les sites web sécurisés grâce au protocole HTTPS et aux certificats de sécurité  
Comprendre les risques liés au téléchargement de fichiers et à l'installation de logiciels  
Gérer ses informations personnelles sur les réseaux sociaux

► Découvrir comment repérer un faux site web et éviter le piège  
Comprendre le fonctionnement du Dark Web  
Définir le Dark Web et le différencier du Web visible et du Deep Web  
Identifier ses usages légitimes et illégaux  
Connaître les dangers du Dark Web comme la vente de données volées et la cybercriminalité  
Vérifier si ses propres données sont exposées sur le Dark Web  
► Réagir efficacement en cas d'incident  
Savoir comment agir face à une attaque de type phishing malware ou vol d'informations  
Identifier les personnes à contacter pour signaler un incident  
Éviter les erreurs courantes après une attaque  
Participer à une simulation d'incident et adopter les bons réflexes  
► Synthétiser les enseignements clés du module  
S'engager personnellement pour renforcer la sécurité numérique