PROGRAMME DE FORMATION EN PRÉSENTIEL

CYBERSÉCURITÉ - LES BONNES PRATIQUES

OBJECTIFS PÉDAGOGIQUES

Comprendre les enjeux et adopter les bonnes pratiques
Réduire les risques liés aux cyberattaques
Sécuriser la communication
Prévenir les incidents à travers des cas concrets
Identifier les risques, adopter des réflexes de vigilance
Contribuer à la force de votre entreprise face aux cybermenaces

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

Public concerné
Employés non techniciens informatique

Pré-requis
Connaître les bases informatiques de type bureautique. Le programme tient compte des spécificités de l'entreprise en matière de sécurité informatique

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 comme les faux ordres de virement et les arnaques par téléphone
Prévenir la fuite de données et éviter la divulgation d'informations sensibles
Étudier des cas réels d'attaques et analyser les erreurs commises
- Apprendre la navigation sécurisée sur Internet
Identifier les sites web sécurisés avec HTTPS et 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
Observer la démonstration d'un faux site web et savoir éviter le piège
Réagir efficacement en cas d'incident
Savoir quoi faire face à une attaque de type phishing malware ou vol d'informations
Identifier à qui signaler un incident au sein de l'entreprise
Éviter les erreurs courantes après une attaque
Participer à une simulation d'incident et adopter les réactions appropriées
- Synthétiser les enseignements clés
S'engager personnellement pour renforcer la sécurité au quotidien
Comprendre les motivations des cybercriminels
- Apprendre à créer et gérer des mots de passe sécurisés
- Utiliser un gestionnaire de mots de passe de manière efficace
- Savoir reconnaître un message suspect avant de l'ouvrir
- Identifier les signes d'un appareil compromis
- Mettre à jour ses systèmes et logiciels pour limiter les risques
- Utiliser les réseaux WiFi publics en toute sécurité
Adopter les bons réflexes face à une demande d'informations inhabituelle