Sensibilisation à la Cybersécurité

De plus en plus d'entreprises prennent conscience aujourd'hui que la cybersécurité n'est plus une option. Pourtant il reste un maillon faible dans la mise en œuvre de la sécurité : la sensibilisation. Des cyberattaques à grande échelle ont été possibles grâce à une non-connaissance des pièges simples.

Durée : 1 jour - 7 heures

Prix inter : 850 € ht

Prix intra : nous contacter

Délais d'accès : inscriptions jusqu'à 1 semaine avant le début de la formation

Méthodes pédagogiques
12 participants maximum.Alternance d'apports théoriques et pratiques. Support de cours et documents d'application remis en fin de formation.

Validations des acquis
Quizz final et évaluation de la formation.

Formateur
Formateur expert en cybersécurité et en sensibilisation des personnes.

Compétences visées

- Appliquer les bonnes pratiques de la cybersécurité
- Rester en veille sur les menaces potentielles

Objectifs pédagogiques

- Appréhender et comprendre les attaques informatiques
- Identifier les menaces informatiques
- Adopter les bonnes pratiques pour se protéger

Public

Toute personne voulant être sensibilisée aux menaces liées aux attaques informatiques et savoir s'en protéger.

Formation accessible aux personnes en situation de handicap moteur. Pour la prise en compte d'autres situations de handicap, veuillez contacter notre référent handicap depuis http://www.cap4learning.com/contact

Prérequis

Aucun prérequis n'est nécessaire.

Programme

Introduction à la cybersécurité

- Définir les notions d'information et de système d'information
- Identifier la sécurité des systèmes d'information
- Lister les bénéfices de sécuriser les actifs de l'entreprise
- Enumérer les attaques informatiques d'aujourd'hui et leurs motivations
- Identifier les risques pour l'entreprise

Les attaques indoor

- Définir les attaques par clé USB
- Décrire les possibles attaques via le réseau Ethernet
- Identifier les vols ou destructions de matériels
- Identifier une attaque par un employé mal intentionné

Les attaques distantes

- Identifier la portée et la sécurité de son réseau WIFI
- Lister les attaques via le Web

Les attaques par ingénierie sociale

- Décrire la notion d'ingénierie sociale
- Définir la méthode du phishing
- Repérer des personnes malveillantes au téléphone
- Vérifier la provenance de ses mails et pièces jointes
- Exemples d'attaques basées sur l'ingénierie sociale

Les attaques aux mots de passe

- Définir le rôle et les usages des mots de passe
- Lister les attaques via les mots de passe
- Gérer ses mots de passe
- Décrire l'intérêt de la double authentification

Les bonnes pratiques de sécurité au quotidien

- Identifier les réflexes à appliquer dans son travail
- Détecter des menaces potentielles
- Réagir rapidement à un événement de sécurité
- Alerter son entreprise d'un incident