CAP4LEARNING

# Sensibilisation à la Cybersécurité et ingénierie sociale

Durée : 2 jours - 14 heures

Prix inter : 1600 € ht

Prix intra : nous contacter

**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.

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. L'ingénierie sociale ("social engineering") est une technique qui permet d'accéder à des informations par la manipulation de personnes et elle ne s'applique pas seulement au domaine de l'informatique, car elle peut survenir dans la vie de tous les jours et plus particulièrement sur le lieu de travail. Téléphone,

## Compétences visées

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

## Objectifs pédagogiques

- Appréhender et identifier les attaques informatiques
- Identifier les menaces informatiques
- Identifier les menaces par ingénierie sociale
- Adopter les bonnes pratiques pour se protéger

## Public

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

## 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 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 attaques par ingénierie sociale et les vulnérabilités humaines**

- Définir l'ingénierie sociale, lister les risques
- Identifier les sentiments, comportements et instincts de l'humain
- Lister les vulnérabilités courantes
- Énumérer les modes de perception
- Définir la PNL, programmation neuro-linguistique
- Inciter à faire une action
- Manipuler une personne, créer un faux document
- Usurper une identité

**Le phishing (hameçonnage)**

- Identifier le phishing par émail
- Identifier le phishing via le web
- Identifier le phishing par téléphone
- Signaler un phishing

**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

Cap4 Learning - Organisme de formation enregistré sous le numéro 11756080075.
Cet enregistrement ne vaut pas agrément de l'état