

# ACQUÉRIR UNE CULTURE CYBERSÉCURITÉ ET ADOPTER LES BONNES PRATIQUES EN ENTREPRISE

IRE69

1 jour (7h) 950,00 €<sup>HT</sup>

## Objectifs

Développer une culture cybersécurité • Adopter les bonnes attitudes et réflexes afin d'éviter les menaces informatiques dans son activité professionnelle ou privée • Concevoir et gérer des mots de passe forts • Comprendre l'impact de l'ingénierie sociale

### Profil Stagiaire(s)

Cette formation s'adresse à tout utilisateur souhaitant acquérir une culture en cybersécurité et prévenir les cyber-attaques.

### Pré-requis

Cette formation ne nécessite aucun pré-requis.

### Profil animateur(s)

Cette formation est animée par un consultant spécialisé dans la sécurité des SI

## PROGRAMME

### Introduction

Evolution numérique

Les principaux inducteurs technologiques : mobile, réseaux sociaux, collaboratif, cloud, Big Data, BI, internet des objets, gamification, intelligence artificielle...

Les prévisions technologiques

### Cybersécurité : Un enjeu majeur

Qu'est-ce que la cybersécurité ?

Quels sont les métiers autour de la cybersécurité ?

Quels sont les types d'attaque (attaques de masse et les attaques ciblées)

Connaître les pièges les plus classiques dans lesquels tombent les collaborateurs

### Gérer ses mots de passe

Identifier un mot de passe fort

Savoir créer un mot de passe fort

Connaître la technique de la phrase de passe

L'authentification unique

Le coffre-fort numérique

### Connaître les techniques d'attaque exemple : Phishing

Connaître le principe du phishing

Se familiariser avec les différentes techniques employées par les hackers

Donner quelques exemples d'attaques

### Qu'est-ce que le Ransomware ?

Connaître le ransomware

Reconnaître les techniques utilisées par les pirates informatiques

Donner les bonnes pratiques de la cybersécurité en cas d'attaque

### Éviter le nomadisme numérique (séparation données personnelles et données professionnelles)

## Méthodes pédagogiques & Evaluation

Cette formation alterne des apports théoriques mais aussi des exemples concrets inspirés de la vie courante autour de la cybersécurité.

### Suivi & Evaluation

Pour assurer un suivi individuel, Demos a mis en place 2 types d'évaluation :

Une évaluation de compétences en ligne en début et en fin de formation qui peut prendre

différentes formes selon le contenu de la formation suivie : Tests d'évaluation des acquis, cas

## Contactez-nous

Conseiller formation

09 88 66 10 00

inscriptions@demoss.fr

## Nos sessions

16 oct. 2023 : Paris

8 janv. 2024 : A Distance

16 déc. 2024 : Paris

# ACQUÉRIR UNE CULTURE CYBERSÉCURITÉ ET ADOPTER LES BONNES PRATIQUES EN ENTREPRISE

IRE69

1 jour (7h) 950,00 €<sup>HT</sup>

pratiques, mises en situation, soutenance devant un jury pour les formations à finalité certifiante.

Une évaluation de la satisfaction de chaque stagiaire est réalisée en ligne. Cette évaluation est complétée par l'appréciation du formateur à l'issue de chaque session.

## Ressources pédagogiques

Support de formation, exercices...

## Moyens techniques

Nos centres de formation DEMOS, accessibles aux personnes à mobilité réduite, sont tous équipés :

- Salles de formation lumineuses, spacieuses, design, ergonomiques, mobiles et équipées d'écrans plasma, de PC portables/fixes si nécessaire à la formation suivie
- Accès au wifi haut débit sur l'ensemble des lieux
- Espace de colearning et webcorners
- Cafés, collations et rafraîchissement sont offerts

Les sessions "A distance" sont réalisées avec l'outil de visioconférence Teams, permettant au formateur d'adapter sa pédagogie.