

## Cybersécurité: protégez votre entreprise des menaces numériques

Durée : 7 heures

### Programme de formation

#### Public visé

Dirigeants d'entreprise et leurs salariés

#### Pré-requis

Être familier avec l'utilisation d'un PC

#### Objectifs de la formation

- Comprendre les conséquences d'une attaque par phishing
- Prendre conscience de la sensibilité des informations stockées dans les messageries
- Apprendre à sécuriser ses comptes de messagerie
- Comprendre les risques liés aux mots de passe
- Utiliser un gestionnaire de mots de passe

#### Description / Contenu

##### **Sensibilisation aux mails frauduleux et protection des données**

##### **Etape 1 : Simulation d'attaque par mail frauduleux**

- Simulation d'attaques de phishing
- Identification des signes d'une attaque
- Discussion sur les conséquences

##### **Etape 2 : Exploration des documents sensibles dans sa messagerie**

- Parcours d'une boîte mail fictive contenant des documents sensibles
- Risques associés à leur exposition
- Présentation des bonnes pratiques pour la protection des documents.

##### **Etape 3 : Mise en place de la sécurité sur les boîtes mails**

- Configuration des paramètres de sécurité sur une boîte mail.

##### **Gestion des mots de passe et compromission de données**

##### **Etape1 : Compréhension de la compromission de données**

- Exemples de données compromises
- Discussion sur les conséquences pour les entreprises
- Complexité et unicité des mots de passe.

##### **Etape 2 : Utilisation des gestionnaires de mots de passe**

- Démonstration et utilisation des gestionnaires de mots de passe (Bitwarden)
- Configuration pour une utilisation quotidienne.



## **Bilan et conclusion**

- Réponses aux questions des participants sur les sujets abordés.
- Récapitulatif des points clés de la formation.

## **Modalités pédagogiques**

- Apports théoriques et cas pratiques
- Simulation de situations critiques permettant à l'apprenant de se mettre en situation selon différents scénarios pédagogiques répondant aux objectifs de formation
- Échanges entre les participants

## **Moyens et supports pédagogiques**

- Supports numériques
- Ressources sur la cybermalveillance

## **Modalités d'évaluation et de suivi**

Avant la formation :

- Auto-positionnement sur les connaissances
- Evaluation des besoins par le formateur sous forme de questionnaire

Pendant et après la formation :

- Contrôle de l'acquisition des compétences du stagiaire par le formateur
- Evaluation de satisfaction du stagiaire

## **Modalités d'accessibilité**

Votre accueil et votre confort nous tiennent à coeur!

Notre référent handicap, Mikaël Trideau, est là pour vous écouter, vous accompagner et trouver avec vous les solutions adaptées à vos besoins. Contactez-le si besoin au 02 43 49 84 52, il vous répondra avec bienveillance.

Nos locaux sont accessibles aux personnes à mobilité réduite.

Nous prendrons le temps d'échanger avec vous pour imaginer ensemble les adaptations les plus appropriées : supports pédagogiques sur-mesure, matériel adapté, accompagnement humain, recours à notre réseau de partenaires...

N'hésitez pas à nous en parler dès votre inscription.

Nous trouverons des solutions, avec vous et pour vous!

## Profil du / des Formateurs

Tous nos formateurs sont des experts dans le domaine.

## Responsable de stage

Nathalie MILSENT