



Flashez ce QRCode
pour accéder à notre
site internet



Formation Cybersécurité destinée aux collaborateurs



Durée

7.00 Heures
1 Jour



Pré Requis

Disposer d'une adresse mail
professionnelle



Public Concerné

Tout public

Référence

STD-CYBER2

Objectifs :

- Sensibiliser aux cybermenaces courantes et à leurs conséquences
- Apprendre les bonnes pratiques pour protéger les données dans leur quotidien
- Développer des réflexes pour reconnaître et signaler les incidents ou comportements suspects

Qualification Intervenant (e)(s)

Expert cybersécurité salarié d'une entreprise labellisée ExpertCyber et certifiée ISO 27001

Introduction à la cybersécurité

- Qu'est-ce que la cybersécurité ?
- Les menaces principales
- **Atelier pratique 1** : identifier un phishing

Les bonnes pratiques de sécurité numériques

- Gestion des mots de passe
- Sécuriser ses appareils et connexions
- Gestion des mails et des fichiers
- **Atelier pratique 2** : Création d'un mot de passe sécurisé
- **Atelier pratique 3** : Détecter des emails suspects

La protection des données sensibles et les risques internes

- Les risques internes
- **Atelier pratique 4** : Identifier les risques internes
- Protéger les données sensibles
- **Atelier pratique 5** : Classer des informations sensibles

Réagir face à un incident de cybersécurité

- Comment reconnaître un incident de cybersécurité ?
- Comment réagir face à un incident de cybersécurité ?
- **Atelier pratique 6** : Réagir aux différents types d'incidents

Conclusion



Moyens pédagogiques

- Support de la formation en format PDF
- Une affiche récapitulant les bonnes pratiques
- Une affiche récapitulant la réaction à avoir en cas d'attaque



Modalités d'évaluation

Evaluation de l'atteinte des objectifs par les stagiaires