Formation **Sensibilisation à la sécurité informatique**

Cette formation constitue une sensibilisation à la sécurité informatique. Elle est destinée à toute personne souhaitant connaitre les bases de la cybersécurité : à l'issue, vous connaîtrez les grands concepts et principes de la sécurité informatique, saurez éviter les pièges classiques et aurez acquis les bons réflexes pour protéger votre organisation des vols d'identité et autres piratages.

Durée
1 jour

Objectifs pédagogiques

- Connaître les rudiments de la sécurité informatique
- Comprendre les concepts de base de la sécurité informatique en entreprise
- Connaître le droit des TIC et la sécurité en Europe
- Comprendre comment détecter les situations à risques
- Acquérir les bases de la sécurité réseau et de la cryptographie
- Identifier les méthodes et techniques pour intégrer la sécurité au sein des projets

Public
Tous

Prérequis
Aucun

Programme de formation

Introduction
Présentation générale de la formation, objectifs et approche pédagogiques

Concepts de base de la sécurité informatique en entreprise
Les enjeux de la sécurité des Systèmes d'Information
Les besoins de sécurité
Définitions et notions annexes : intégrité, non-répudiation, authentification, confidentialité, disponibilité, menace, vulnérabilité, attaque...

Que dit la loi ? Le droit des T.I.C. et la sécurité en Europe

Les situations à risques
Connaître son Système d'Information
Maîtriser le réseau
Sécuriser les terminaux, et les dispositifs de stockage
Gérer les utilisateurs
Sécuriser physiquement
Contrôler la sécurité du S.I
Panorama de quelques menaces

Sécurité réseau et cryptographie

Sécurisation d'un réseau, filaire et sans fil
Les bases de la cryptographie
La sécurité des applications et applications web

La sécurité au sein d'une organisation

Intégrer la sécurité dans les projets
Difficultés liées à la prise en compte de la sécurité

Exemples d'ateliers pratiques réalisés durant la formation

Expérimentation d'une clé USB modifiée par des personnes malintentionnées
Expérimentation de l'utilisation de failles de sécurité d'un site Internet vulnérable, exfiltration des données, escalade de privilèges

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques.
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.