Devenez un maillon fort de la sécurité de votre structure

Référence : **SECUSER1** Durée : **1 jour** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Aucune connaissance spécifique demandée. • Savoir utiliser les outils informatiques et communicants (téléphone, ordinateur, messagerie, Internet, ...).

PROFIL DES STAGIAIRES

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

OBJECTIFS

• Prendre conscience des comportements à risque et apprendre les principales règles d'usage en matière de sécurité informatique. • Appréhender et comprendre les attaques informatiques. • Identifier les menaces informatiques. • Adopter les bonnes pratiques pour se protéger.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

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

Cadre légal

- Politique de sécurité
- Charte informatique
- Protection des données personnelles
- RGPD
- LPM

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 par ingénierie sociale

- Décrire la notion d'ingénierie sociale
- Définir la méthode du phishing
- Repérer des personnes malveillantes au téléphone
- Vérifier la provenance de ses mails et pièces jointes
- Exemples d'attaques basées sur l'ingénierie sociale

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 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