EduGroupe
Accompagner pour réussir

Devenez un maillon fort de la sécurité de votre structure

Référence : **SECUSER1** Durée : **1 jour (7 heures)** Certification : **Aucune**

Connaissances préalables

- 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 préparée

- Aucune

Méthodes pédagogiques

- 6 à 12 personnes maximum par cours, 1 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 et de réflexions

Formateur·rice

- Consultant-Formateur expert Sécurité offensive

Méthodes d'évaluation des acquis

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

Contenu du cours

1. 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

2. Cadre légal

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

3. 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

4. Les attaques distantes

- Identifier la portée et la sécurité de son réseau WIFI
- Lister les attaques via le Web

5. 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

6. 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

7. 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

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.