PROGRAMME DE FORMATION
Sécurité de l'information

Objectif : A l'issue de la formation, chaque apprenant sera capable de :
- Comprendre les risques informatiques et frauduleux pesant sur l'activité de son employeur,
- Appliquer au quotidien les règles et bonnes pratiques nécessaires pour contrer les attaques,
- Sensibiliser lui-même d'autres employés de son organisation aux risques cyber et aux bonnes pratiques,
- Être une force de proposition pour améliorer la sécurité de son activité.

Pour qui : Utilisateurs du système d'information de l'entreprise

Prérequis : Aucun

Durée : 1 jour (7 heures)

Formateur : Consultant Expert en sécurité de l'information

Moyens : Support informatique.

Méthode pédagogique : Dans une pédagogie active le formateur alterne, pour chaque thème, présentation théorique et mise en pratique. L'apprenant observe puis met en application. Le formateur accompagne les apprentissages individuels.

Évaluation des compétences :
- Cas pratiques réalisés au cours de la formation
- Bilan des acquis avec le formateur

La formation abordera différentes thématiques de cybersécurité du quotidien du salarié, et se déroulera selon le plan suivant :

La cybercriminalité
Découverte du monde de la cybercriminalité – organisation, motivation, objectifs

Les outils des hackers
Appréhender les principales techniques courantes des hackers

Le phishing
Apprendre à reconnaître des emails frauduleux ou suspect, principale porte d'entrée des fraudeurs en entreprise

Malware & Ransomware
Comprendre ces notions et les conséquences de ces menaces sur l'entreprise

L'ingénierie sociale
Apprendre comment un fraudeur retrouve et analyse les traces numériques d'un individu pour nourrir son attaque en manipulant ses victimes, maîtriser l'usage des réseaux sociaux pour limiter son exposition

Les fraudes (faux fournisseur, au président, faux service technique)
Découvrir de ces techniques de fraude, et apprendre plusieurs méthodes pour les détecter en mettant en défaut un attaquant

La fuite d'information
Découvrir les principales situations de vol d'information, et découvrir des techniques simples assurant la confidentialité

Les bonnes pratiques a appliquer au quotidien
Comprendre quelles pratiques de sécurité sont indispensables, (re)découvrir les règles imposées ou souhaitées par son employeur, être capable de faire des simulations simples de crises afin de réfléchir aux meilleures solutions pour s'en protéger ou pour en limiter les effets

Réagir en cas d'attaque
Appréhender les concepts de la gestion de crise