Formation lot n°7

CYBERSECURITE, SENSIBILISATION

Rèférence : WEB012 **DUREE : 1 jour, soit 7 heures**

OBJECTIFS DE CETTE FORMATION : Comprendre les types de cyber risques auxquels votre organisation est ou sera confrontée. Savoir comment réagir face à ces multiples menaces. Identifier les ressorts du management de la sécurité des systèmes d'information. Avancer dans votre transformation digitale en anticipant les risques de malveillance.

PARTICIPANT : Toute personne souhaitant acquérir les notions de bases de la cyber criminalité. (responsables marketing, planneurs stratégiques, chefs de produit, documentalistes).

PRE-REQUIS : Bonne compréhension des stratégies d'entreprise sur Internet. Une connaissance des principaux médias et réseaux sociaux est un plus.

FORMATEURS : spécialiste en cybersécurité.

MODALITES ET PEDAGOGIE :

- Questionnaire d'évaluation en amont et en fin de formation
- Evaluation à chaud et à froid
- Equipement informatique mis à disposition
- Assistance téléphonique
- Support Stagiaire
- Attestation de fin de stage

METDODE ET TECHINIQUE PEDAGOGIQUE

Les méthodes pédagogiques proposée visent à équilibrer théorie et pratique pour développer des compétences variées :

1. Apprentissage par projet : Les étudiants travaillent sur des projets concrets pour résoudre des problèmes réels.
2. Apprentissage par problèmes : Études de cas et défis pour encourager la réflexion critique et la résolution de problèmes.
3. Travail en groupe : Collaboration sur des tâches informatiques (création d'applications, gestion de réseau).
4. Labs pratiques : Exercices pratiques sur des ordinateurs ou des environnements de développement pour appliquer les connaissances.
5. Gamification: Jeux interactifs pour enseigner des concepts de manière ludique.
6. Études de cas : Analyse de situations réelles pour comprendre l'application des concepts.
7. Suivi continu : Évaluations régulières pour aider les étudiants à améliorer leurs compétences.

PROGRAMME

MATIN:

COMPRENDRE LES RISQUES

Disposer d'une vision exhaustive des risques internes et externes de cyber-malveillance
Comprendre simplement les cyber-menaces et les capacités de nuisance des pirates informatiques
Connaître les dispositifs disponibles (organisationnels, juridiques et techniques) pour contrer les cyber-attaques, aussi bien en termes de protection que de prévention

REAGIR FACE A UNE CYBERATTAQUE

Déposer une plainte auprès du procureur de la République
Exercice d'application : rédaction du plan détaillé de la plainte
Notifier la violation de données personnelles à la Commission nationale de l'informatique et des libertés
Gérer la communication
Mettre en place un plan média : communiqué de presse, bandeau sur le site internet,

APRES-MIDI:

communication sur les médias sociaux, Facebook et Twitter, script de réponse aux questions des journalistes
Préparer un communiqué destiné aux clients
Exercice d'application : rédaction d'un communiqué aux clients dont les données personnelles ont été volées
Gérer l'aspect assurantiel

PREVENIR LE RISQUE DE CYBERATTAQUE PAR LA MISE EN PLACE D'ACTIONS PREVENTIVES

Sécuriser les systèmes d'information contre les risques externes
Sécuriser des systèmes d'information contre les risques internes
Mettre en place une charte informatique destinée aux salariés, administrateurs et prestataires externes
Mettre en place une charte d'utilisation du réseau Wi-Fi