Présentiel

Sensibilisation à la cybersécurité

Code produit : F-DON2 / Version : v1

ELEMENTS DE CONTEXTE

La digitalisation des entreprises s'accélère.

Aujourd'hui, dans un monde interconnecté, l'exposition aux risques de cyberattaques est amplifiée. D'autant plus que ces informations sont aisément accessibles, depuis n'importe où, dans l'ensemble des services de l'entreprise.

La sécurité des opérations, des transactions et des données critiques dépasse aujourd'hui les murs de l'entreprise.

Dans ce contexte, les cyberattaques en lien avec la transformation digitale des entreprises se multiplient.

Le principal risque induit par la transformation numérique est le développement de la cybercriminalité face à un niveau de protection des entreprises aujourd'hui encore insuffisant.

FINALITE DE LA FORMATION

Prendre conscience de la nécessité de s'engager dans une démarche de prévention du risque.

OBJECTIFS PEDAGOGIQUES

- Découvrir les différentes techniques utilisées par les pirates pour accéder à leurs systèmes d'informations
- Identifier les différentes méthodes de protection
- Favoriser la prévention du risque en cernant les bonnes pratiques en vigueur

PUBLIC CONCERNE/EMPLOI VISE

Tout professionnel.

PREREQUIS

Aucun.

Présentiel

MODALITES

Durée : 14 heures / 2 jours

Type : Présentiel

Méthodes et moyens pédagogiques : Le formateur privilégiera les techniques d'animation interactive :

- Apports cognitifs
- Des études de cas apportés par chacun des participants et des mises en situations étayent les apports et facilitent la prise de conscience et l'acquisition de nouvelles pratiques
- Pédagogie active alternant mises en situation et analyses de pratiques professionnelles

Validation des acquis : QCM, tour de table, observation.

Sanction de la formation : Attestation de fin de formation.

Profil de l'intervenant : Consultant expert en cybersécurité

Passionné par les technologies de l'information et de la communication depuis de nombreuses années, il n'a eu de cesse d'accroitre ses connaissances dans ce secteur d'activité en perpétuelle évolution. Pour concevoir des applications cyber résilientes, il est nécessaire d'intégrer des concepts de sécurité informatique au plus tôt dans le processus de conception.

Ses compétences connexes dans le monde judiciaire et dans celui de la formation concourent à améliorer cet objectif.

PROGRAMME

❖ **MODULE 1**

Analyse des pratiques professionnelles

- Cas concrets du formateur
- Cas concrets amenés par chacun des stagiaires
- Echanges avec le formateur sur chaque cas, évaluation des pratiques et identification des éléments d'amélioration qui seront ensuite travaillés pendant la formation.

Introduction (30 min)

- La cybersécurité c'est quoi ?
- Le mot de passe : Premier rempart de la sécurité

Les menaces sociales (45 mn) + Démo 1 (15 mn)

- Le phishing, l'ingénierie sociale, (démo)
- La réputation, l'usurpation d'identité
- Les bons réflexes

Présentiel

Les menaces informatiques (45 mn) + Démo 2 (15 mn)

- Les rançongiciels
- Les mécanismes de propagation, clé USB (démo)
- Les bons réflexes

❖ **PAUSE**

Formation en cybersécurité

Les réseaux sans fil (45 mn) + Démo 3 (15 mn)

- Attaque de l'homme du milieu
- Goodies, GSM, Portail captif (démo)
- Bonnes pratiques

Anonymisation et IoT (45 mn) + Démo 4 (15 mn)

- Le darknet (Défaçage de site, Le réseau Tor, Les achats sur le darknet)
- L'IoT (Présentation et compromission par attaque DDoS et RF)

❖ **DEJEUNER**

❖ **MODULE 2**

Réagir à un cyber incident (45 mn) + Démo 5 (15 mn)

- Les quatre phases d'un incident
- Elaboration de guides d'intervention
- Les bons réflexes de confinement
- Anticiper un cyber incident
- Exercices de simulation

Que faire après à un cyber incident (30 mn)

- Constitution d'un dossier de plainte
- Dépôt de plainte, action en justice
- Action en justice dans quel cas ?

Que faire après à un cyber incident (45 mn)

- Prestataire de la sécurité des systèmes d'information
- Les obligations légales (RGPD, LPM, HDS, etc)
- Services institutionnels
- Sources d'information

❖ **Evaluation des connaissances**
- (QCM)

❖ **Identification d'axes d'amélioration individuels et indicateurs de suivi**

❖ **Plan d'action individuel**

❖ **Bilan de la formation.**

LES + ASFO

Nos responsables pédagogiques et intervenants sont des experts reconnus dans leur métier.

Certification AFNOR selon le référentiel ISO 9001.