FORMATION A LA PREVENTION D'UNE CYBER ATTAQUE

F-DON2

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.

Objectifs

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

Public Visé

Tout professionnel.

Durée : nous contacter

Pré Requis

Aucun.

Parcours pédagogique

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

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.

Objectifs pédagogiques

- 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

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

Qualification Intervenant(e)(s)

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.

Méthodes et modalités d'évaluation

Mises en situation, attestation de fin de formation.

Modalités d'Accessibilité

Accès PMR

ASFO GRAND SUD
0 800 64 31 33 (n°gratuit)
contact@groupelfc.com
www.asfograndsud.com
SIRET : 83420427300017
Code APE : 8559A
Organisme de formation enregistré sous le n°76310897031 auprès du Préfet de la Région Occitanie. (Cet enregistrement ne vaut pas agrément de l'Etat)