

CYBERSÉCURITÉ : Notions de bases, enjeux et droit commun

Chef d'entreprise, face à ces risques, êtes-vous prêt ?



Les cyber attaques sont massives, multiples et incessantes. La gravité de leurs impacts ne fait que s'accroître au fil du temps. C'est une **criminalité organisée** à l'échelle mondiale tournée vers **l'extorsion de fonds** dont la cible principale sont les acteurs économiques.

Si les grandes organisations restent des **cibles privilégiées**, force est de constater que ces attaques se propagent de plus en plus vers la PME et le particulier.

Nul ne peut se croire totalement à l'abri. Lorsque les systèmes d'information sont atteints il est souvent trop tard pour réagir.

L'exposition à ce phénomène concerne tout utilisateur (téléphone mobile, ordinateur portable, ...). Au-delà des parades technologiques et logicielles, chacun(e) est porteur d'une **responsabilité**.

Erreurs, négligences ou pratiques frauduleuses, les **failles de sécurité** exposent désormais les organisations à un **risque stratégique**.

Comment faire face ? Vos collaborateurs sont-ils suffisamment prudents ? Sont-ils conscients des risques encourus par certaines habitudes d'apparences anodines ?....

Afin d'éviter d'avoir à gérer une crise sans précédent, assurez-vous que votre organisation adopte les réflexes élémentaires qui permettent de repousser de telles menaces !

Objectifs pédagogiques

- ✦ Identifier l'articulation entre cybersécurité, sécurité économique et intelligence économique
- ✦ Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI).
- ✦ Connaître les définitions et la typologie des menaces.

Public concerné

Chefs d'entreprises et cadres dirigeants, artisans, responsables d'association et de collectivités, responsables informatique.

Durée 3 heures

Lieu Groupe Sup de Co La Rochelle

Tarif 190 € net de taxe

MODULE 1 : Programme de formation

CYBERSÉCURITÉ : Notions de bases, enjeux et droit commun

PROGRAMME DE FORMATION

- ⊕ **Définition :**
 - Intelligence économique, sécurité économique globale
 - Cybersécurité Sécurité des SI (prévention) + Cyberdéfense (réaction) + Cybercriminalité (sanction) = Cybersécurité
- ⊕ **Les enjeux de la sécurité des SI**
 - La nouvelle économie de la cybercriminalité
 - Panorama des menaces selon une typologie
 - Les vulnérabilités (exemples, détermination, veille)
 - Focus sur l'ingénierie sociale
- ⊕ **Les propriétés de sécurité**
 - Présentation du principe de défense en profondeur
 - Identification et évaluation des actifs et des objectifs de sécurité
- ⊕ **Aspects juridiques et assurantiels**
 - Responsabilités
 - Préservation de la preuve
 - L'offre assurantielle
- ⊕ **Le paysage institutionnel de la cybersécurité**
 - La prévention
 - Le traitement des cyberattaques et la réponse judiciaire
 - Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers



Les + de la formation

⊕ La formation est animée par un consultant-expert en analyse des risques et management stratégique dont la société est référencée sur la plateforme cybermalveillance.gouv.fr.

Titulaire d'un DESS en système d'information et d'un MBA de la Sorbonne, il a exercé au sein de l'Armée de l'air pendant près de 20 ans puis chez IBM pendant 10 ans.

⊕ Aucun prérequis en termes de connaissances technologiques n'est attendu des participants.

⊕ Etudes de cas réels, retours d'expériences, apports conceptuels et échanges directs avec les participants sont au rendez-vous de cette formation.

⊕ Cette formation s'adresse aux dirigeants d'entreprises : enjeux stratégiques, évaluation des risques et décision managériale sont les principales finalités de cette journée.