FORMATION **ESSENTIELLE**

CYBERSÉCURITÉ : QUELLES RESSOURCES POUR LIMITER LES RISQUES DANS SON ACTION

nouveau

OBJECTIFS

- Connaître les principes de la Cybersécurité
- Maîtriser les enjeux et le droit commun
- Quelle hygiène informatique mettre en œuvre dans son action
- Apprendre à protéger son action

Public concerné : Tout public

Formation en E-learning + distanciel
Durée : 7h00

CONTENU PÉDAGOGIQUE

Accès à la plateforme d'e-learning
(3h au minimum obligatoire)

Formation animée par Formateur-Expert

Les grands principes de la cybersécurité
- Introduction
- La sécurité et les risques
- Panorama des périls
- L'arsenal
- La stratégie du donjon
- La stratégie du millefeuille
- Protéger et informer
- Verrouiller les portes
- Qui va là ?
- Le principe du zéro trust
- La détection
- Les tests de sécurité
- Contre-attaque
- La sécurité des applications

Notion de bases, enjeux et droit commun
Définitions
- Intelligence économique, sécurité économique globale
- Cybersécurité

Les enjeux de la sécurité des SI
- La nouvelle économie de la cybercriminalité
- Panorama des menaces selon une typologie
- Les vulnérabilités
- 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

L'hygiène informatique pour les utilisateurs
Connaître le système d'information et ses utilisateurs
- Faire une cartographie du SI
- Identifier le patrimoine de son ordinateur

Maîtriser le réseau de partage de documents
- Interne
- Sur internet

Définir une véritable politique de mise à jour des logiciels
- Qui est en charge ?
- A quel moment ?

Authentifier l'utilisateur
- Méthode d'authentification
- Bonnes pratiques pour un bon mot de passe

Gestion et organisation de cybersécurité
Définitions
- Intelligence économique, sécurité économique globale
- Cybersécurité

Les enjeux de la sécurité des SI
- La nouvelle économie de la cybercriminalité
- Panorama des menaces selon une typologie
- Les vulnérabilités
- 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

Protection de l'innovation et cybersécurité
Modalités de protection du patrimoine immatériel de la structure (entreprise, collectivité, association, ...)
- Les différentes mesures et éventuelles obligations
- Dispositif de zone à régime restrictif
- Protection du potentiel scientifique et technique de la nation
- Droit de la propriété intellectuelle lié aux outils informatiques

Cyber-assurances
- Présentation d'un domaine nouveau et émergent
- Les offres de cyber-assurance

Cas Pratiques
- Cyber-attaque avérés

CYBERSÉCURITÉ : QUELLES RESSOURCES POUR LIMITER LES RISQUES DANS SON ACTION

LIBRA FORMATION

nouveau

ORGANISATION PÉDAGOGIQUE

Pré-requis
- Aucun

Formateur
- 1 consultant spécialisé

Moyens pédagogiques et techniques :
- Accueil des stagiaires dans une salle adaptée à la formation en présentiel (INTER ou INTRA) ; visioconférence zoom en distanciel.
- Présentation académique de la formation
- Travaux pratiques : Quiz / QCM en distanciel ; étude de cas en présentiel.
- Délivrance d'un support de formation après la session

Dispositif de suivi et d'évaluation des résultats de la formation :
- Feuille d'émargements
- Évaluation de la formation en fin de session
- Remise d'un Certificat de réalisation de la formation
- Service Après-Formation LIBRA : possibilité à l'issue de la formation d'interroger le formateur via une adresse e-mail dédiée