FORMATION

CYBERSECURITE

Type de cours : Distanciel

Référence : CYB-DIS

Durée: 26 h de formation

²Objectifs

Acquérir une vision globale , théorique et pratique, de la sécurité sur le plan des lois mais aussi des outils, concepts et mécanismes permettant de faire face aux attaques visant sécurité des systèmes informatiques.

s Cette formation Cybersécurité vous permettra, en 125 modules, de vous sensibiliser et vous initier à la cybersécurité ; quel que soit votre niveau, apprenez et assimilez des notions de base de la SSI utiles au travail comme à la maison.

ATTESTATION DE FORMATION DELIVRÉE EN FIN DE STAGE

Méthodes pédagogiques

Technologie
HTML5 • Norme SCORM
Un poste de travail par stagiaire,
Accès internet,
Support de cours,
Évaluation en fin de stage,
Attestation de formation.

Pré-requis :

Notions de réseaux informatiques et d'internet.

Public visé :

Responsables sécurité informatique, Administrateurs sécurité, Gérants d'entreprise, Managers.

Programme du stage

I- PANORAMA DE LA SSI

Unité 1 - Un monde numérique hyper-connecté • Une diversité d'équipements et de technologies • Le cyberespace, nouvel espace de vie • Un espace de non-droits ?

Unité 2 - Un monde à hauts risques
• Qui me menace et comment ? • Les attaques de masse
• Les attaques ciblées • Les différents types de menaces
• Plusieurs sources de motivation
• Les conséquences pour les victimes de cyberattaques • Conclusion

Unité 3 - Les acteurs de la cybersécurité
• Le livre blanc pour la défense et la sécurité nationale
• La stratégie nationale pour la sécurité du numérique
• L'ANSSI • Autres acteurs de la cybersécurité
• D'autres experts pour m'aider • Conclusion

Unité 4 - Protéger le cyberespace
• Les règles d'or de la sécurité • Choisir ses mots de passe • Mettre à jour régulièrement ses logiciels
• Bien connaître ses utilisateurs et ses prestataires
• Effectuer des sauvegardes régulières • Sécuriser l'accès Wi-fi de son entreprise ou son domicile
• Être prudent avec son smartphone ou sa tablette • Protéger ses données lors de ses déplacements
• Être prudent lors de l'utilisation de sa messagerie • Télécharger ses programmes sur les sites officiels des éditeurs • Être vigilant lors d'un paiement sur Internet • Séparer les usages personnels et professionnels • Prendre soin de ses informations et de son identité numérique • Conclusion

Unité 5 - Mon rôle dans la sécurité numérique • Introduction • Les données • Risques sur les données • Protéger les données • Responsabilités face aux risques

II- SÉCURITÉ DE L'AUTHENTIFICATION

Unité 1 - Principes de l'authentification • Introduction
• Objectif de l'authentification
• Facteurs d'authentification
• Les types d'authentification
• Limites des facteurs d'authentification
• Les risques liés aux mots de passe

ternet : de quoi s'agit-il ? • Introduction • Internet schématisé • Cyber-malveillance • Ingénierie sociale • Contre-mesures possibles • En cas d'incident • Réseaux sociaux • Conclusion 3

Unité 2 - Attaques sur les mots de passe • Introduction
• Les attaques directes
• Les attaques indirectes
• Conclusion

Unité 3 - Sécuriser ses mots de passe • Introduction • Un bon mot de passe • Comment mémoriser un mot de passe fort ? • Comment éviter la divulgation de mot de passe ?
• Conclusion

Unité 4 - Gérer ses mots de passe • Introduction • Gérer la multiplication des mots de passe • Configurer les logiciels manipulant les mots de passe • Transmettre des mots de passe sur le réseau • Conclusion

Unité 5 - Notions de cryptographie • Introduction • Principe général • Chiffrement symétrique • Chiffrement asymétrique • Signature électronique, certificats et IGC • Conclusion www.onlineformapro.com Détail formation : CyberSécurité Unité 1 - In