Centre de Formation Professionnelle

FORMATION

CYBERSECURITE A DISTANCE

Objectifs

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.

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

Type de cours : Disanciel

Référence : CYB-DIS

Durée: 26 heures

ATTESTATION DE FORMATION DELIVRÉE EN FIN DE STAGE

Pré-requis :

Notions de réseaux informatiques et d'internet.

Public visé :

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

Méthodes pédagogiques

- Technologie HTML5
- Norme SCORM
- Un ordinateur nécessaire
- Accès internet,
- Support de cours,
- Évaluation en fin de stage,

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
Internet : 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

III - SÉCURITÉ SUR INTERNET

CyberSécurité Unité 1 - Internet : de quoi s'agit-il ? • Introduction • Internet schématisé • Cybermalveillance • Ingénierie sociale • Contre-mesures possibles • En cas d'incident • Réseaux sociaux • Conclusion 3

IV - SÉCURITÉ DU POSTE DE TRAVAIL ET NOMADISME

Unité 1 - Applications et mises à jour
• Introduction
• Concept de vulnérabilité en sécurité informatique
• Mise à jour
• Installation d'applications

Unité 2 - Les fichiers en provenance d'Internet
• Introduction
• Les formats et les extensions d'un fichier
• Y a-t-il des formats plus risqués que d'autres ?
• Y a-t-il des sources plus sûres que d'autres ?
• J'ai déjà eu recours à une pratique déconseillée sans aucun problème
• Se protéger des rançongiciels
• Conclusion

Unité 3 - La navigation Web • Introduction • Comment fonctionne concrètement un navigateur ? • Vous avez dit "typosquatting" ? • Le moteur de recherche, la porte d'entrée du web • Et les "cookies" alors ?
• Le navigateur bienveillant pour la santé de votre ordinateur • Le contrôle parental • Conclusion

Centre de Formation Professionnelle CFORPRO - Tour de l 'horloge- 4 Place louis Armand 75603 Paris- Siret 50218786700010 - Déclaration N°11754276775 - Tél: 01.75.60.92.30 - Fax: 01.79.73.89.51 - Mail : contact@cforpro.com

Témoignages

Cédric G.
“Très satisfait. Formation très riche et très complète. Mes objectifs ont tout à fait été atteints.”

Nicolas C. (Société LABOR HAKO)
“Très satisfait, présentation de toutes les “best practices” et conseils d’améliorations pour mon entreprise actuelle. Je la recommande.”

Noëlle C.
“Cette formation m’a fait prendre connaissance des risques du numérique et comment se proteger. Formation à recommander à tous mais après un raffraichissement.”