PROGRAMME DE FORMATION EN INITIATION A LA SÉCURITÉ INFORMATIQUE

Description

La formation en initiation à la Sécurité Informatique est conçue pour fournir une compréhension de base des principes fondamentaux et des meilleures pratiques en matière de sécurité informatique.

Objectif

Destinée aux débutants, cette formation vise à sensibiliser les participants aux menaces courantes et à leur apprendre les techniques essentielles pour protéger les informations et les systèmes. La formation commence par une introduction aux concepts de base de la sécurité informatique, notamment la confidentialité, l'intégrité et la disponibilité des données.

Objectifs spécifiques

De façon spécifique

- Elle explique les différents types de menaces, comme les logiciels malveillants, les attaques par phishing, et les ransomwares, en mettant en lumière comment ces menaces peuvent affecter les individus et les organisations.
- Les participants apprendront à reconnaître les signes d'une cyberattaque et à prendre des mesures de prévention. La formation couvre des sujets tels que la gestion des mots de passe, l'importance des mises à jour logicielles, et l'utilisation des antivirus. Elle aborde également la sécurisation des réseaux domestiques et professionnels, incluant la configuration des pare-feux et des réseaux sans fil sécurisés.
- Une partie importante de la formation est consacrée aux pratiques de navigation sécurisée sur internet. Les participants apprendront à identifier les sites web sécurisés, à éviter les téléchargements suspects, et à comprendre les risques liés à l'utilisation des réseaux Wi-Fi publics. En outre, la formation introduit les concepts de base de la cryptographie, expliquant comment le chiffrement protège les données sensibles.
- Elle inclut également des conseils sur la protection des données personnelles et sur les réglementations en matière de protection de la vie privée. À la fin de la formation, les participants auront acquis les connaissances nécessaires pour adopter une posture de sécurité proactive dans leur vie personnelle et professionnelle, réduisant ainsi les risques de cyberattaques et de pertes de données.

Prérequis

1. Compétences de Base en Informatique
2. Connaissance des Terminaux Numériques

3. Familiarité avec les Outils de Communication en Ligne
4. Connaissances de Base en Réseaux
5. Intérêt pour la Sécurité Informatique

Public cible

1. Utilisateurs d'Ordinateurs et de Dispositifs Mobiles
2. Employés de Bureau
3. Professionnels des PME
4. Étudiants en Informatique et Technologie
5. Personnel Non Technique dans les Secteurs Technologiques
6. Enseignants et Formateurs
7. Professionnels de la Santé
8. Responsables de la Conformité et de la Sécurité
9. Utilisateurs de Services Bancaires et Financiers en Ligne
10. Toute Personne Intéressée par la Cybersécurité

Débouchés

1. Technicien Support Informatique
2. Assistant Administrateur Réseau
3. Coordinateur de Sécurité
4. Analyste en Sécurité Informatique Junior
5. Consultant en Sécurité Informatique pour Petites Entreprises

Formateurs :

- **Dr ASSOGBA Emery** (+229 69292907)
- **Ing. KASSA Célia**
- **Ing. ODJO Abousidikou**

Méthode de formation : Cours magistraux, TP, TD, étude de cas

Mode d'évaluation : QCM

Critère de validation du certificat : 70% de taux de bonne réponse sur l'ensemble des questions

Nombre total d'heures : 35h

Intitulé	Contenu	Masse horaire
Introduction et Concepts Fondamentaux	Introduction à la Sécurité Informatique Définition et importance Principes de base : confidentialité, intégrité, disponibilité Menaces et Vulnérabilités Types de menaces : malwares, phishing, ransomwares Vulnérabilités courantes Introduction aux Cyberattaques Méthodes d'attaque courantes Études de cas célèbres	07H
Sécurité des Systèmes et des Réseaux	Sécurisation des Systèmes d'Exploitation Mises à jour et correctifs Configuration des pare-feu Utilisation des logiciels antivirus Sécurité des Réseaux Concepts de base des réseaux Sécurisation des réseaux Wi-Fi Configuration des routeurs et des pare-feu	07H
Sécurité des Données et Cryptographie	Sauvegardes et récupération de données Gestion des accès et des permissions Introduction à la Cryptographie Concepts de base : chiffrement et déchiffrement Utilisation des certificats SSL/TLS Exemples d'outils de cryptographie	07H
Sécurité de base de données et du Cloud	Les Nécessaires pour la sécurité d'une base de donnée Les attaques de type SQL Injection Authentification Le contrôle d'accès d'une base de donnée Chiffrement Inférence	07H

	Encryptage d'une Base de donnée Cloud Computing Les mesures de protection du cloud	
Sécurité des Applications et Navigation Internet	Sécurité des applications web Bonnes pratiques pour les développeurs Navigation Sécurisée sur Internet Reconnaissance des sites web sécurisés Éviter les téléchargements suspects Utilisation des VPN pour une navigation sécurisée	07H
Réglementations et Pratiques de Sécurité	Introduction aux lois et réglementations : GDPR, RGPD, PCI-DSS Conformité et audit de sécurité Pratiques de Sécurité au Quotidien Gestion des mots de passe Sensibilisation et formation des utilisateurs Mise en place d'une stratégie de sécurité personnelle Conclusion et Évaluation Résumé et Q&R Examen final et certification	07H

Références bibliographiques

1- Sécurité informatique: principes et méthode Laurent Bloch, Christophe Wolfhugel, Christian Queinnec, Nat Makarévitch, Hervé Schauer, Éditeur Eyrolles, 2009, ISBN 2212125259, 9782212125252, 292 pages

2- The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Jason Andress Éditeur Elsevier, 2011 ISBN 1597496545, 9781597496544 208 pages