
Programme de Formation

E-Learning : Cybersécurité - SSI

Description

Points Forts

Formation exhaustive en 125 modules pour maîtriser les fondamentaux de la cybersécurité : bonnes pratiques, menaces, navigation, nomadisme, mots de passe et poste de travail.



Public visé

- Salariés, agents publics, étudiants ou demandeurs d'emploi
- Professionnels du numérique ou utilisateurs réguliers d'outils informatiques
- Toute personne souhaitant renforcer sa posture de cybersécurité dans un cadre personnel ou professionnel



Objectifs pédagogiques

Cette formation vous permettra :

1. De comprendre les menaces et enjeux de la cybersécurité au quotidien
2. D'adopter les bons réflexes face aux risques numériques
3. De sécuriser son poste, ses données, et ses usages personnels et professionnels
4. De maîtriser les bases de l'authentification et du chiffrement
5. De prévenir les attaques sur Internet, dans la messagerie et les réseaux

Organisation

Durée : 26 heures

Mode d'organisation : E-learning

Contenu pédagogique



Description

La formation **CyberSécurité** se structure autour de **4 grands domaines**, eux-mêmes décomposés en **5 unités** chacun (soit 125 modules au total). Chaque unité est interactive et s'appuie sur des situations concrètes :

1. Panorama de la sécurité des systèmes d'information (SSI)

- Enjeux du cyberspace, menaces, attaques, motivations
- Acteurs institutionnels et professionnels de la cybersécurité
- Bonnes pratiques : sauvegarde, Wi-Fi, mots de passe, navigation sécurisée
- Responsabilité individuelle et protection des données personnelles

2. Sécurité de l'authentification

- Types et principes d'authentification
- Attaques sur les mots de passe et contre-mesures
- Construction, mémorisation et gestion de mots de passe forts
- Notions de cryptographie, chiffrement symétrique/asymétrique, certificats

3. Sécurité sur Internet

- Principes de fonctionnement du Web, ingénierie sociale



- Formats de fichiers à risque, rançongiciels, sécurité du navigateur
- Messagerie électronique et menaces associées
- Architecture d'une connexion Web, HTTPS, proxys, cookies, réseaux sociaux

4. Sécurité du poste de travail et nomadisme

- Mise à jour des applications et systèmes
- Sécurisation des terminaux mobiles et ordinateurs portables
- Gestion des comptes utilisateurs, sauvegardes, chiffrement
- Sécurité des périphériques USB, effacement sécurisé, séparation pro/perso



Prérequis

- Aucune compétence technique poussée requise.
- Savoir naviguer sur Internet et utiliser un ordinateur ou smartphone.



Modalités pédagogiques

- Formation 100 % en ligne compatible HTML5 et norme SCORM
- Modules interactifs, exemples concrets, schémas explicatifs
- Accessible sur ordinateur et smartphone (responsive design)
- Progression par domaines avec évaluation intégrée à chaque unité



Moyens et supports pédagogiques

- 125 modules répartis sur 4 grands domaines et 20 unités
- Exercices de validation, quiz, fiches pratiques
- Supports visuels, démonstrations, animations pédagogiques
- Suivi personnalisé via plateforme LMS compatible SCORM



Modalités d'évaluation et de suivi

- Quiz intégrés à chaque unité pour valider les acquis
- Suivi de progression individuel via plateforme SCORM
- Attestation de suivi ou de réussite possible à l'issue de la formation
- Possibilité d'intégration à un parcours plus large de certification en cybersécurité