Programme – Sensibilisation à la cybersécurité

Apprendre à se protéger contre les cyber-menaces grâce à des pratiques simples et efficaces.

Durée : 2,5 heures

Session : présentielle – FOAD - mixte

PSH **Aménagements** & compensations

Tarifs : Intra : de 400€ à 590€ (nb de sessions)
Inter : de 90€ à 110€ (FOAD, présentiel)

contact@formacadre.com

Renseigner le formulaire de pré-inscription

Sensibilisation à la cybersécurité

La formation « **sensibilisation à la Cybersécurité** », en format court de 2 heures et demie, est ouverte à tous sans prérequis. Elle permet à chaque utilisateur de devise informatique de comprendre les enjeux, d'identifier les menaces auxquelles il se confronte au quotidien et d'apprendre à s'en protéger facilement et efficacement. Délais d'accès à la formation : De 2 à 6 semaines en fonction du financement demandé. Contactez-nous par email ou téléphone pour informations, devis et inscriptions.

Public, prérequis & accessibilité

Aucun prérequis ou profil n'est demandé, cette session de formation concerne toutes les personnes désireuses de se sensibiliser.
Accessibilité : l'OF étudiera l'adaptation des moyens de la prestation pour les personnes en situation de handicap en fonction du lieu choisi.

Moyens pédagogiques, techniques & humains

La formation est proposée en présentiel, FOAD ou mixte. Nos sessions, interactives et ludiques, permettent une implication forte des apprenants et l'atteinte des objectifs fixés.

En présentiel ou à distance, les participants ont accès aux mêmes activités ludiques et pertinentes, disponibles en ligne ou hors connexion. Ils testent leur niveau d'avancement après chaque atelier sur un format 20% de théorie et 80% de mise en pratique. En fin de session, un test de compétences est à compléter, et corrigé en groupe.

Notre intervenant est formé aux bonnes pratiques imposées par l'ANSSI et la CNIL.

[Contenu du cours]

Contenus	Objectifs
Session de formation : 2,5 heures	
M1 : **Introduction à la formation** (20min) Présentation générale de la cybersécurité et de ses impacts au quotidien, prise en main des outils interactifs.	**M1** : Se sensibiliser à l'importance de la Cybersécurité. Compétence acquise : Repérer les différentes cyberattaques.
M2 : **Atelier n°1 – les mots de passe** (40min) Le 1er atelier est consacré à la composition et l'utilisation des mots de passe. Les participants apprennent à constituer un mot de passe sécurisé, basé sur les recommandations de l'ANSSI. Un cas pratique dans lequel ils jouent le rôle d'un hackeur leur permet d'identifier les comportements sensibles et les éviter.	**M2** : Appréhender les techniques utilisées par les cybercriminels. Compétence acquise : Définir un mot de passe sécurisé.
M3 : **Atelier n°2 – Les emails** (30min) Le 2ème atelier aborde les différentes méthodes de phishing. A l'aide d'une boite de messagerie où se trouvent de vrais messages et des emails frauduleux, les stagiaires apprennent à déjouer les pièges des cybercriminels. Ils sont sensibilisés aux bonnes pratiques diffusées par la CNIL.	**M3** : Apprendre à se protéger contre les menaces. Compétence acquise : Reconnaitre un email frauduleux.
M4 : **Atelier n°3 – Le facteur humain** (40min) Le dernier atelier met en évidence le rôle de l'humain dans les défaillances de cybersécurité. Un jeu interactif invite les participants à contrer des attaques communes.	**M4** : Comprendre le rôle central de l'humain. Compétence acquise : Adopter un comportement responsable.
M5 : **Conclusion et QR** (20min) Echange avec les participants, partage de supports et documentation, QCM final d'évaluation.	**M5** : Valider les compétences.