Cybersécurité et sensibilisation

Mis à jour le 14 septembre 2026

Conditions d'entrée et prérequis

Connaissances de base en informatique, manipulation du clavier et de la souris.

Niveau d'entrée

Sans diplôme

Public visé

Tout public

Rythme

Temps plein

Durée en centre

7 heures

Validation

- Attestation de réalisation TOSA Digital Cybersécurité

Certification

Oui

Modalités d'évaluation

Quiz, échanges entre participants
Évaluation finale sous forme de QCM
et/ou d'étude de cas / Certification TOSA Digital Cybersécurité

Modalités de suivi

Possibilité de validation par blocs de compétences

Non

Nombre de participants

4 à 12

Entrée-sortie permanente

Non

Formation référencée dans le cadre du marché AKTO : Actions collectives de formations transverses "Bureautique et TIC"

Objectifs professionnels

La formation « **Cybersécurité et sensibilisation** » est une formation courte permettant de comprendre les différents types de menaces en cybercriminalité, de détecter les intrusions et de protéger les données.

- Comprendre les différents types de menaces en cybercriminalité
- S'acculturer aux bonnes pratiques (mot de passe unique par système…etc)
- Détecter les intrusions et réagir face aux malveillances
- Comprendre les risques et les enjeux de sécurité
- Déterminer les données importantes à protéger
- Comprendre les actions à mettre en oeuvre pour protéger les données importantes (mise à jour antivirus, gestion des accès, sauvegarde…)
- Mettre en oeuvre une charte informatique à partager en interne (les pratiques)

Contenu

Module 1 : Introduction à la Cybersécurité
Définition de la cybersécurité
Importance de la cybersécurité dans le monde actuel
Présentation des objectifs de la formation

Module 2 : Types de menaces en cybercriminalité
Virus, malwares, ransomwares
Phishing et ingénierie sociale
Attaques par déni de service (DDoS)
Études de cas réels

Module 3 : Bonnes pratiques en cybersécurité
Gestion des mots de passe (unicité, complexité)
Utilisation de l'authentification à deux facteurs (2FA)
Sécurisation des réseaux Wi-Fi
Précautions à prendre lors de l'utilisation des réseaux sociaux et des emails

Module 4 : Détection des intrusions et réactions face aux malveillances
Signes d'une intrusion (comportements anormaux, alertes de sécurité)
Outils de détection (antivirus, pare-feu)
Procédures à suivre en cas d'intrusion

Module 5 : Risques et enjeux de sécurité
Conséquences financières et légales
Atteinte à la réputation
Perte de données sensibles
Études de cas d'entreprises victimes de cyberattaques

Module 6 : Protection des Données Importantes
Classification des données (sensibles, confidentielles, publiques)
Techniques de chiffrement
Importance des sauvegardes régulières
Gestion des accès et des permissions

Cybersécurité et sensibilisation

Module 7 : Mise en Oeuvre d'une Charte Informatique
Éléments clés d'une charte informatique
Rôles et responsabilités des utilisateurs
Exemples de chartes informatiques
Communication et sensibilisation en interne

Modalités pédagogiques

- Formation modularisée, sous forme de progression pédagogique
- Ateliers pédagogiques permettant la manipulation de l'outil et la mise en situation de l'apprenant pour améliorer les acquis sous forme de « formation action »
- Évaluations régulières par des quiz et des exercices pratiques, évaluation finale

Profil des intervenants

Formateurs expérimentés en formation continue, référents, experts dans le domaine du numérique, habilités en tant qu'examinateur.

Les plus

Codification de la formation : **RS5252**

Délais et modalités d'accès

Inscription et entretien
Positionnement : Questionnaire préalable pour évaluer les connaissances de base des participants.

Vous êtes adhérents AKTO ?
Connectez vous à la plateforme Espace Formation d'AKTO : **espaceformation.akto.fr**

Financements possibles

29 € / heure
Prise en charge à 100% des coûts pédagogiques, dans la limite des fonds disponibles.

Référent handicap

Toutes nos formations sont accessibles à la candidature de personnes en situation de handicap. Nos référents handicap sont à votre écoute pour l'analyse de vos besoins spécifiques et l'adaptation de votre formation.
Contacts : florent.petitdemange@greta-alsace-sud.com ou abida@strasbourg.greta.fr

Réseau

- GRETA Alsace
- Réseau des GRETA d'Alsace

- contact@gip-fcip-alsace.fr
- Contactez nos Conseillers en Formation Professionnelle

Cybersécurité et sensibilisation

- www.greta-alsace.fr