Centre de Formation Professionnelle

FORMATION

CYBERSECURITE - PROTEGER SES DONNEES



Type de cours : Présentiel

Référence : CYB

Durée: 2 jours - 14 heures

ATTESTATION DE FORMATION DELIVRÉE EN FIN DE STAGE

Objectifs

Développer une culture cyber-responsable et maîtriser les bons réflexes pour protéger ses données et celles de son organisation, dans le but de réussir la certification Tosa CyberCitizen.

À l'issue de la formation, le participant sera capable de :

1. Identifier les principaux acteurs, menaces et enjeux de la cybersécurité.
2. Adopter des comportements sûrs en environnement professionnel.
3. Sécuriser ses appareils et données lors des déplacements et du télétravail.
4. Reconnaître les tentatives d'ingénierie sociale (phishing, usurpation, etc.).
5. Mettre en œuvre des pratiques de protection de la vie privée et de sauvegarde.
6. Se préparer efficacement à la certification Tosa CyberCitizen.

Pré-requis :

Aucun prérequis technique. Savoir utiliser un ordinateur, une messagerie et un smartphone.

Public visé :

Salariés, étudiants, demandeurs d'emploi, particuliers souhaitant renforcer leurs compétences en cybersécurité au quotidien.

Méthodes pédagogiques

• Alternance d'apports théoriques, d'ateliers pratiques, de quiz et de cas concrets.

• Méthodes actives : démonstrations, analyse de situations, mises en pratique guidées.

• Supports de cours numériques ou imprimés remis à chaque participant.

• Attestation de formation.

• Évaluation en fin de stage,

Financement possible par votre OPCO ou votre employeur | www.cforpro.com
01 75 50 92 30 DEMANDER UN DEVIS GRATUIT ›

Programme du stage

Partie 1 – Sécurité numérique et environnement professionnel

Accueil et positionnement

Identifier le niveau initial et les attentes des participants.
Présentation du Tosa CyberCitizen.
Réalisation d'un test de positionnement (10 QCM).

Module 1 : Le monde de la cybersécurité

Comprendre les enjeux, les acteurs et les types d'attaques.
Découvrir les attaquants et défenseurs, les institutions du secteur et les principales formes d'attaques.
Approfondir les notions d'identité numérique, d'authentification et de MFA (authentification multifacteur).

Module 2 : Ingénierie sociale et phishing

Identifier les techniques d'hameçonnage et adopter les bons réflexes face aux menaces.
Étudier le phishing, le smishing, les ransomwares et les fake news.
Apprendre les bonnes pratiques de sécurité des mots de passe et l'usage d'un gestionnaire de mots de passe.

Module 3 : Sécurité au bureau

Appliquer les bonnes pratiques de sécurité au poste de travail.
Aborder la sécurisation du PC, la gestion des droits d'accès, l'utilisation des périphériques USB et supports externes.
Comprendre l'importance des mises à jour logicielles régulières.

Module 4 : Données et comportements collaboratifs

Gérer les échanges et partages de données de manière sécurisée.
Étudier l'usage du cloud, des messageries et des réseaux internes.
Identifier les comportements à risque et adopter les bonnes pratiques collectives en environnement professionnel.

Bilan de la Partie 1

Évaluer les acquis intermédiaires à travers un quiz global (20 questions).
Participer à un débrief collectif pour consolider les connaissances.

Financement possible par votre OPCO ou votre employeur | www.cforpro.com
01 75 50 92 30 DEMANDER UN DEVIS GRATUIT ›

Partie 2 – Sécurité mobile, personnelle et préparation à la certification

Réactivation des acquis

Consolider les notions clés de la Partie 1.
Réalisation d'un quiz d'échauffement suivi d'échanges collectifs pour renforcer la compréhension.

Module 5 : Sécurité en déplacement

Identifier les risques liés aux environnements externes lors des déplacements professionnels ou personnels.
Aborder les bonnes pratiques concernant le Wi-Fi public, l'utilisation d'un VPN, le partage de connexion, la sécurité des smartphones et la protection physique des terminaux.

Module 6 : Sécurité à la maison et en télétravail

Adopter une hygiène numérique personnelle adaptée au contexte domestique et au télétravail.
Travailler sur la sécurisation du Wi-Fi domestique, les sauvegardes cloud, la gestion des fichiers externes, la protection de la vie privée en ligne et la sécurité des objets connectés (IoT).

Module 7 : Examen blanc Tosa CyberCitizen

Se familiariser avec la certification Tosa CyberCitizen.
Réalisation d'une simulation complète comprenant 35 questions en 60 minutes, selon le format officiel Tosa.

Module 8 : Débrief et plan d'action individuel

Identifier ses axes de progrès et consolider les acquis en vue de la certification.
Restitution du score individuel, analyse des erreurs et élaboration d'un plan d'entraînement personnalisé.

TEST DE VALIDATION DES COMPETENCES ACQUISES
ATTESTATION DE FORMATION DELIVREE EN FIN DE STAGE

Financement possible par votre OPCO ou votre employeur | www.cforpro.com
01 75 50 92 30 DEMANDER UN DEVIS GRATUIT ›

Témoignages

Thomas R.
“Formation très instructive, concrète et accessible même sans background technique. J’ai appris à identifier les risques réels auxquels nous sommes exposés au quotidien et les bons réflexes à adopter. La partie sur le phishing et les mots de passe était particulièrement bien illustrée. Je la recommande à toute personne travaillant avec des données sensibles.”

Aïcha M.
“Très bonne formation, dispensée avec beaucoup de pédagogie. Le formateur part de cas concrets du quotidien professionnel, ce qui rend les enjeux cyber très tangibles. À l’issue de ces deux jours, j’ai une vision claire des pratiques à mettre en place et des erreurs à ne plus commettre. Formation à recommander absolument en milieu hospitalier.”

Sébastien C.
“Formation dense et bien structurée. Le passage sur la sécurité en télétravail et les Wi-Fi publics correspondait exactement à mes besoins. Le formateur est compétent et à l’écoute. J’ai passé le TOSA CyberCitizen à l’issue et j’ai obtenu un bon score. Je recommande cette formation à mes collègues.”

Martine B.
“Très satisfaite. La formation m’a permis de prendre conscience de la réalité des menaces informatiques et d’adopter de vraies bonnes pratiques. Le format en deux jours est bien dosé, avec une alternance de théorie et de cas pratiques. Mes objectifs ont été atteints et je me sens maintenant bien mieux armée pour protéger les données de mon service.”

Financement possible par votre OPCO ou votre employeur | www.cforpro.com
01 75 50 92 30 DEMANDER UN DEVIS GRATUIT ›