Ref. formation 202601359356

Cybersécurité : Sensibilisation

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

MODULA FORMATION
Emilie CRAVEA
05.56.44.58.68
contact@modula-formation.com

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Entretien
Inscription directe ou par un conseiller en insertion professionnelle

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Non renseigné

Prérequis pédagogiques :

Avoir des connaissances de base de l'environnement Windows. Formation à destination de tout actif voulant appréhender les fondamentaux de la cybersécurité.

Contrat de professionnalisation possible ?

Non

Objectif de la formation

- Identifier les principales menaces de cybersécurité et leurs impacts sur l'entreprise. - Adopter les bonnes pratiques pour sécuriser ses usages numériques. - Détecter les signaux d'intrusion et adopter les bons réflexes en cas d'attaque. - Mettre en œuvre des mesures de protection simples (sauvegardes, mots de passe, antivirus). - Construire une charte informatique adaptée à son organisation.

Contenu et modalités d'organisation

1. INTRODUCTION A LA CYBERSÉCURITÉ – Définition et enjeux de la cybersécurité – Contexte réglementaire et obligations légales – Impact des cyberattaques sur les entreprises 2. TYPOLOGIE DES MENACES EN CYBERCRIMINALITÉ – Les principales attaques : phishing, ransomware, ingénierie sociale – Études de cas et exemples concrets – Comment identifier une menace : méthodes d'identification des attaques 3. BONNES PRATIQUES EN SÉCURITÉ INFORMATIQUE AU QUOTIDIEN – Gestion des mots de passe et authentification sécurisée – Sécurisation des accès aux applications, aux données, usage des réseaux et appareils – Sensibilisation aux comportements à risque (emails, téléchargements, réseaux Wi-Fi...) 4. DÉTECTION ET RÉACTION FACE AUX INTRUSIONS – Identifier les signes d'une cyberattaque – Les bonnes pratiques en cas de suspicion d'intrusion : Protocoles internes et réflexes à adopter – Présentation d'outils de surveillance et d'alerte 5. MISE EN ŒUVRE DES MESURES DE PROTECTION – Mise à jour et gestion des antivirus et pares-feux – Stratégies de sauvegarde et protection des données – Gestion des accès et rôles des utilisateurs 6. ÉLABORATION D'UNE CHARTE INFORMATIQUE INTERNE – Objectifs et contenu d'une charte informatique – Rédaction et diffusion de la charte en entreprise – Étude de cas : mise en place d'une politique de sécurité

Parcours de formation personnalisable ? **Oui** Type de parcours ***Non renseigné***

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Formations dans le domaine informatique

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00670474	du 01/01/2026 au 31/12/2026	Bruges (33)	MODULA FORMATION		Non éligible	FPC