Ref. formation 202501297176

Sensibilisation des utilisateurs - Cybersécurité

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

CAMPUS DU LAC
MEYNARD Céline
05.56.79.52.00
formation.courte@campusdulac.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 :

Inscription obligatoire par un conseiller en insertion professionnelle
Entretien

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Tous les collaborateurs, tous niveaux confondus, sans prérequis technique

Prérequis pédagogiques :

Tous les collaborateurs, tous niveaux confondus, sans prérequis technique

Contrat de professionnalisation possible ?

Non

Objectif de la formation

Nature de l'action : Acquisition de compétences - Comprendre les principaux risques et menaces en matière de cybersécurité. - Adopter les bonnes pratiques pour protéger les données personnelles et professionnelles. - Identifier les signaux d'alerte et savoir réagir face à une menace potentielle. - Sensibiliser à l'impact des comportements individuels sur la sécurité globale de l'entreprise.

Contenu et modalités d'organisation

Comprendre les enjeux de la cybersécurité Accueil et introduction Présentation des participants et de leurs attentes. Objectifs de la journée. Les fondamentaux de la cybersécurité Définitions clés : cybersécurité, cybercriminalité, données sensibles. Les principales menaces : phishing, ransomwares, vols de données, faux sites. Études de cas : exemples concrets d'attaques et leurs impacts. Identifier les risques et les comportements à risque Pourquoi les utilisateurs sont la première cible des cyberattaques. Les erreurs humaines courantes : mots de passe faibles, clics sur des liens douteux. Atelier interactif : reconnaître un email de phishing ou un site frauduleux. Adopter les bonnes pratiques et réagir efficacement Les bonnes pratiques au quotidien Sécurisation des mots de passe : création et gestion (gestionnaires de mots de passe). Navigation sur internet : sécuriser les connexions et éviter les pièges. Partage de données : utiliser des outils sûrs pour collaborer en ligne. Mise à jour et sauvegarde des données : leur importance. Réagir face à une menace Que faire en cas de phishing ou de tentative d'intrusion ? Procédure de signalement en interne : qui alerter et comment. Atelier pratique : simulation d'un incident et mise en œuvre des réflexes de sécurité. Construction d'une charte de cybersécurité Atelier collaboratif : élaboration des bonnes pratiques spécifiques à l'entreprise. Engagement individuel : identifier une action à mettre en place immédiatement. Conclusion et évaluation Synthèse des apprentissages. Plan d'action personnel pour renforcer la cybersécurité.

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

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Non renseigné

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00567861	du 22/01/2025 au 31/12/2028	Bordeaux (33)	CAMPUS DU LAC		Non éligible	FPC