

Annexe 1 au Cadre de réponse - ACM TRANSVERSES (À fournir par module)



Intitulé du module :

Sécuriser ses pratiques numériques (cybersécurité / RGPD)

Contenu du programme

Introduction à la cybersécurité

- Les cyberattaques ciblant les entreprises : exemples concrets (fraudes aux paiements, usurpation d'identité, piratage, rançongiciels).
- Conséquences des attaques : impact financier et réputationnel.

Sécuriser ses équipements et ses connexions

- Sécurisation des équipements (ordinateurs, smartphones, tablettes) : Installation et mise à jour des logiciels de protection et paramétrage des équipements
- Sécurisation des connexions Internet : configurations de sécurité essentielles box et wifi, VPN et réseaux publics
- Installation sûre d'un logiciel : sources et limitation d'autorisations des applications

Gérer les mots de passe et repérer les arnaques

- Créer et gérer un mot de passe robuste : règles, gestionnaire de mot de passe
- Identifier et éviter le phishing
- Techniques de manipulation et arnaques courantes

Protéger les données sensibles et respecter le RGPD

- Comprendre la notion de données à caractère personnel : droits des utilisateurs
- Gérer ses propres données et celles des clients : stockage, chiffrement, CGU, diffusion des données
- Respecter le RGPD : obligations et bonnes pratiques

Prévenir et réagir face aux cyberattaques

- Techniques de piratage courantes et comment s'en prémunir.
- Logiciels malveillants et solutions de protection.
- Actions en cas de compromission et interlocuteurs privilégiés (ANSSI, CNIL, CERT-FR, banques)

Évaluation et conclusion

- QCM final.
- Synthèse des bonnes pratiques à retenir.

Objectifs pédagogiques

- Comprendre les enjeux de la cybersécurité et le cadre réglementaire
- Identifier les principaux risques informatiques et adopter les bonnes pratiques pour sécuriser les équipements, les données et les échanges numériques
- Utiliser des outils simples pour renforcer la sécurité.
- Développer des réflexes sécuritaires adaptés à son activité quotidienne.

Public visé

Tout public salarié des 54 branches professionnelles et l'interprofession du champ de OPCO EP.

Prérequis

Maîtrise de la langue française
Maîtrise de l'outil et de l'environnement informatique et Internet

Modalités pédagogiques

Ateliers pratiques (simulations, analyse de mails ,paramétrage téléphone pro..)
Témoignages vidéo
Formation interactive basée sur les échanges entre participants et formateur
QCM final

Durée de formation en heures et en jours

1 journée de 7H

Contact Organisme de formation

GIPAL Formation
Ouafa ADDALA
Gipal-fao@ac-lyon.fr
04 72 40 43 37