

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



**Intitulé du module : Sécuriser ses pratiques numériques (cyber sécurité / RGPD)**

**Contenu du programme**

**Demi-journée 1 : Enjeux, risques et bonnes pratiques de base (3,5 heures)**

**Séance 0 : Bienvenue et mise en route (30 minutes)**

Accueillir les participants et créer une atmosphère conviviale et propice à l'apprentissage. Présentation du formateur et des stagiaires  
Présenter le programme de la formation, ses objectifs et son déroulement.  
Instaurer une dynamique de groupe positive et encourager l'interaction entre les participants

*ICE BREAKER : activité courte et ludique pour favoriser la détente et l'échange (ex : "deux vérités, un mensonge", "le plus grand point commun").*

Identifier les attentes et les besoins individuels des participants.

Présenter les modalités pratiques de la formation (horaires, lieux, supports, etc.).

Évaluation des acquis

**Séance 1 : introduction à la cyber sécurité (1 heure)**

Les enjeux de la cyber sécurité pour les entreprises artisanales et commerciales.

Impact des cyberattaques sur les entreprises : exemples concrets.

*Exercice : Echange et partage d'expérience sur les risques perçus en matière de cyber sécurité.*

**Séance 2 : Identification des risques informatiques (1 heure)**

Présentation des principaux risques :

Hameçonnage (phishing) et attaques par ingénierie sociale.

Rançongiciels (ransomwares) et autres logiciels malveillants.

Faillles humaines (erreurs, négligences, etc.).

Risques liés aux mots de passe faibles et à la non-mise à jour des logiciels.

*Exercice : Analyse de scénarios d'attaques et identification des risques.*

**Séance 3 : Mise en place des bonnes pratiques de sécurité de base (1 heure)**

Utilisation de mots de passe forts et gestionnaires de mots de passe.

Sécurisation des équipements (antivirus, pare-feu, mises à jour, etc.).

Reconnaissance et prévention du phishing (analyse d'emails suspects, liens, etc.).

*Exercice : Atelier pratique de création de mots de passe forts et sécurisation d'un appareil.*

**Demi-journée 2 : RGPD, outils et gestion des incidents (3,5 heures)**

**Séance 4 : Introduction au RGPD et protection des données sensibles (1 heure)**

Présentation des principes fondamentaux du RGPD et des droits des personnes.

Identification des données personnelles et de leurs différents types.

Protection des données sensibles : chiffrement, limitation des accès, etc.

Sécurisation des données lors du travail nomade (VPN, Wi-Fi sécurisé, etc.).

*Exercice : Étude de cas sur la mise en conformité RGPD d'une petite entreprise.*

**Séance 5 : Outils et gestion des incidents (1 heure)**

Présentation d'outils simples et efficaces pour sécuriser les échanges (messageries chiffrées, gestionnaires de mots de passe, etc.).

Prévention et gestion des risques liés aux attaques numériques :

Identification des acteurs (internes, externes, etc.).

Bons réflexes à avoir en cas d'attaque (alerte, isolation, restauration).

*Exercice : Simulation d'un incident de sécurité et mise en pratique des réflexes à adopter.*

**Séance 6 : Réflexes sécuritaires et bilan (1 heure)**

Développement de réflexes sécuritaires adaptés à l'activité quotidienne.

Conseils pour sensibiliser les collaborateurs à la cyber sécurité et au RGPD.

**Séance 7 : Bilan de la formation et évaluation (30 minutes)**

Révision des points clés de la formation.

Questions/réponses.

Évaluation de la satisfaction et des acquis

Clôture de la formation.

**Objectifs pédagogiques**

Appréhender les enjeux de la cyber sécurité dans les entreprises

Identifier les principaux risques informatiques (hameçonnage, rançongiciels, failles humaines, etc.)

Mettre en place les bonnes pratiques de sécurité (utiliser des mots de passe forts, sécuriser les équipements, reconnaître et éviter le phishing, protéger les données sensibles, limiter les accès en fonction des besoins, sécuriser le travail nomade, etc.)

Utiliser des outils simples et efficaces pour sécuriser les équipements et les échanges numériques

Prévenir et gérer les risques liés aux attaques numériques (identifier les acteurs et les bons réflexes à avoir en cas d'attaque)

Développer des réflexes sécuritaires adaptés dans son activité quotidienne

Connaître le cadre réglementaire RGPD

**Public visé**

**Salariés des 54 branches professionnelles et l'interprofession relevant du champ de l'OPCO EP**

**Prérequis**

**Aucun**

**Modalités pédagogiques**

*Atelier participatif en petit groupe*

*Animation par des consultants experts*

*Apports théoriques interactifs*

*Exercices pratiques et jeux de rôle*

*Études de cas et exemples concrets*

*Brainstorming et discussions de groupe.*

*Utilisation de supports visuels (PowerPoint, vidéos)*

*Feedback individualisé et collectif*

**Durée de formation en heures et en jours**

**7 heures**

**1 jour**

**Organisme de formation – contact de l'OF à renseigner mail et Tel**

**CMA FORMATION**

**formationcontinuepaca@cmar-paca.fr**

**04 84 31 00 00**