

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



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

Module 2 : 7h (2 parties de 3h30)

Partie 1 : Comprendre et Identifier les Risques Cyber (3h30)

Introduction (10 min)

- Présentation du formateur
- Objectifs pédagogiques et déroulé

Module 1 : Comprendre les enjeux de la cybersécurité dans les entreprises (40 min)

- Définitions clés : cybersécurité, cyberattaque
- Pourquoi les entreprises sont-elles ciblées ?
- Conséquences économiques, opérationnelles et réputationnelles
- Étude de cas pratiques

Module 2 : Cadre réglementaire RGPD (30 min)

- Rappel des principes fondamentaux du RGPD
- Obligations des entreprises
- Risques liés à la non-conformité
- Bonnes pratiques en matière de protection des données

> **Pause (10 min)**

Module 3 : Identifier les principales menaces informatiques (2h)

- L'hameçonnage
Démonstration par le formateur : réalisation d'une attaque en direct.
- **Atelier : identifier des courriels frauduleux**
- Le piratage de compte
- Les rançongiciels
- L'arnaque aux faux support Technique
- Fuite et violation de donnée personnelles
- Qu'est-ce que le DarkWeb ?
Atelier : identifier la présence d'informations personnelles sur le Dar Web

Bilan intermédiaire (10 min)

Partie 2 : Mettre en place les bonnes pratiques et développer les réflexes (3h30)

Module 4 : Mettre en place les bonnes pratiques de sécurité (2h)

- Sécurité des mots de passe : bonnes pratiques
Atelier : démonstration de l'usage de KeePass
- Usages professionnels et personnels
- Les bonnes pratiques en télétravail et en déplacement
- Protéger son identité numérique
- Sécuriser son réseau WIFI
- Chiffrer ses données
- Sauvegarde et restauration des données
- Mise à jour et gestion proactive des systèmes

Pause (10 min)

Module 5 : Prévenir, gérer les attaques et développer les bons réflexes (1h)

- Sensibilisation continue : Quelles sources d'informations utiliser ?
Communication interne - Bonnes pratiques à adopter
- Faire face à une attaque : procédure d'urgence - Qui contacter, comment réagir ?
- Scénario d'incident : gestion et analyse en groupe

Conclusion et évaluation (20 min)

- Synthèse des apprentissages
- Évaluation des acquis par quiz interactif
- Ressources complémentaires

Objectifs pédagogiques

- Identifier les risques Cyber
- Identifier les menaces
- Comprendre les principes de la RGPD
- Adopter et mettre en place les bonnes pratiques.
- Prévenir les cyberattaques.
- Développer les bons réflexes en cas de cyberattaque.

Public visé

Salariés des entreprises relevant du champ de l'OPCO EP

Prérequis

- Ordinateur avec connexion Internet haut débit, webcam, micro et haut-parleurs et/ou casque fonctionnels
- Familiarité avec la navigation internet et les outils numériques de base (courriel, téléchargement, création de comptes, etc..).

Modalités et moyens pédagogiques

- Présentations interactives
- Suite de démonstrations par le formateur, d'apports théoriques, d'expérimentation pratiques sur des travaux collectifs et individuels, d'échanges entre apprenants et de quizz
- Adaptation et accompagnement au projet des apprenants sur les temps dédiés
- Mise à disposition d'un support PDF

Durée de formation en heures et en jours
7 heures en 2 sessions de 3h30 réparties sur 2 journées

Contact : AFPA
Sandy BEZAULT
sandy.bezault@afpa.fr
06 33 86 28 91