

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



Intitulé du module :

Module 2 : Sécuriser ses pratiques numériques (Cybersécurité / RGPD)

Contenu du programme

1 : Comprendre les enjeux de la cybersécurité

- Cybersécurité : définitions, état des lieux actuel, enjeux pour les entreprises
- Chiffres clés et exemples marquants d'attaques récentes (entreprises, collectivités...)
- Impacts humains, économiques, juridiques et d'image liés aux incidents numériques

2 : Sensibilisation au cadre réglementaire RGPD

- Rappel des grands principes du RGPD : données personnelles, obligations légales
- Les implications concrètes pour l'entreprise : consentement, registre des traitements, droit des personnes, etc.

3 : Identifier les principaux risques informatiques

- Types de menaces : phishing/hameçonnage, ransomware/rançongiciel, virus, ingénierie sociale, faille humaine
- Analyse de cas concrets d'attaques récentes : comment les reconnaître ?

4 : Mettre en place les bonnes pratiques de sécurité

Les bonnes pratiques essentielles :

- Gestion des mots de passe forts (gestionnaires, bonnes pratiques)
- Sécurisation des équipements (ordinateurs, smartphones, tablettes...)
- Identification et évitement du phishing
- Protection des données sensibles
- Gestion des accès selon les besoins (principe du moindre privilège)
- Sécurité lors du télétravail et en déplacement (VPN, Wi-Fi sécurisé...)

5 : Outils simples et efficaces pour sécuriser les pratiques numériques

- Présentation et démonstrations : antivirus gratuits (Avast, Bitdefender), gestionnaires de mots de passe, VPN gratuits (ProtonVPN), outils de chiffrement (VeraCrypt), stockage sécurisé (Cryptomator), messagerie sécurisée...

6 : Prévenir et gérer une crise cyber

- Prévention : sensibilisation des collaborateurs, vigilance permanente
- En cas d'incident : Identifier rapidement les bons réflexes, actions prioritaires, les acteurs clés à contacter (référent cybersécurité, CNIL, prestataire IT...)

7 : Développer des réflexes sécuritaires au quotidien

- Récapitulatif des bons réflexes quotidiens à adopter
- Construction collective d'une "check-list des réflexes sécurité" à diffuser dans les équipes.

8 : Conclusion - Evaluation

Objectifs pédagogiques

À l'issue du module, les participants seront capables de :

- Comprendre les enjeux fondamentaux liés à la cybersécurité en entreprise.
- Connaître le cadre réglementaire du RGPD et ses implications pratiques.
- Identifier clairement les principaux risques informatiques (hameçonnage, rançongiciel, faille humaine, etc.).
- Mettre en place des bonnes pratiques efficaces pour sécuriser leur environnement numérique professionnel.
- Utiliser des outils simples et adaptés pour sécuriser leurs équipements et échanges numériques.
- Prévenir les attaques numériques et gérer efficacement une crise liée à une cyberattaque.
- Développer des réflexes sécuritaires concrets dans leurs pratiques quotidiennes.

Public visé

Toute personne souhaitant comprendre les enjeux de la cybersécurité et acquérir les bonnes pratiques numériques

Prérequis

La lecture
L'écriture
L'expression en langue française
L'usage courant des outils bureautiques
Être muni d'un ordinateur avec connexion internet et doté d'une caméra et d'un micro

Modalités pédagogiques

Distanciel – synchrone – Teams

Formation opérationnelle qui alterne les apports théoriques, la mise en pratique concrète sur le projet des apprenants et les échanges entre stagiaires.

Durée de formation en heures et en jours

7 heures (1 jour)

Horaires : 9h – 17h

Organisme de formation

EME PME

contact@eme-pme.com

Tél : 03 44 06 27 14