

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



Intitulé du module : « Sécuriser ses pratiques numériques (Cybersécurité, RGPD) »

Contenu du programme

Les enjeux liés à la Cybersécurité (1 heure)

- Définition et importance de la cybersécurité.
- Enjeux pour les entreprises : données, réputation, continuité d'activité.
- État des lieux sur les dernières cybermenaces
- L'impact multiple d'une cyberattaque sur les entreprises

Cadre réglementaire et RGPD (1 heure)

- Présentation du RGPD : principes, droits et obligations.
- Impact du RGPD sur les pratiques numériques.
- Obligations des entreprises et droits des individus
- Sanctions en cas de non-conformité.

Identification des risques informatiques (1,5 heure)

- Hameçonnage (phishing) : techniques et exemples.
- Rançongiciels (ransomwares) : fonctionnement et prévention.
- Failles humaines : erreurs et négligences.
- Autres risques : malwares, attaques par déni de service, etc.

Les bonnes pratiques de sécurité (1,5 heure)

- Gestion des mots de passe : création, stockage, renouvellement.
- Sécurisation des équipements : antivirus, pare-feu, mises à jour.
- Reconnaissance et prévention du phishing.
- Protection des données sensibles : chiffrement, sauvegarde.
- Gestion des accès : principe du moindre privilège.
- Sécurité du travail nomade : VPN, Wi-Fi sécurisé.

Les outils de sécurité et échanges numériques (1 heure)

- Présentation et utilisation d'outils de sécurité simples et efficaces.
- Sécurisation des échanges : messagerie chiffrée, partage de fichiers sécurisé.
- Navigation sécurisée : extensions de navigateur, VPN.

La prévention et la gestion des attaques numériques (1 heure)

- Identification des acteurs : attaquants, autorités, experts.
- Procédures en cas d'attaque : signalement, isolation, restauration.
- Communication de crise et gestion de l'image
- Sensibilisation des équipes à la sécurité dans ses routines professionnelles



Objectifs pédagogiques

- Comprendre les enjeux de la cybersécurité dans les entreprises
- Sensibiliser au cadre réglementaire (RGPD)
- 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

Public visé :

Professionnels de tous secteurs souhaitant renforcer leur sécurité numérique.

Prérequis

Aucun prérequis n'est nécessaire. Néanmoins, une évaluation de début de stage sera réalisée pour obtenir une photographie du niveau de départ

Modalités pédagogiques

Une présentation théorique est exposée par le formateur, suivie d'échanges d'expériences avec les apprenants. Des cas pratiques sont effectués sous forme d'études de cas, jeux de rôle, et d'exercices basés sur les objectifs de chacun et sont corrigés de manière individuelle et collective. Une alternance d'apports théoriques, d'études de cas, de mises en situation sont faits tout au long de la formation. La méthode active est largement utilisée afin de favoriser l'assimilation.

Le formateur propose des organisations adaptées à chacun puis évalue les acquis.

Durée de formation en heures et en jours
7 heures – 1 jour

Organisme de formation – contact de l'OF
Fabrice LEROY
Laboratoire LM
182 Quai Cavaignac
46000 CAHORS
Tel : 05 65 24 55 55
Mail : labolm@wanadoo.fr