

3.1.4 - SÉCURISER SES PRATIQUES NUMÉRIQUES (CYBER SÉCURITÉ /RGPD) (1 JOUR)

Objectif général

En une journée vous serez initié à la cybersécurité et au respect du Règlement Général sur la Protection des Données (RGPD). L'objectif de cette formation est de vous permettre d'identifier les risques informatiques, d'adopter de bonnes pratiques de sécurité au quotidien, et de savoir comment prévenir et gérer les cyberattaques.

Objectif pédagogique

- 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.

Prérequis

- Aucun

Les + de votre CMA FORMATION :

Nos experts formations vous accompagnent dans :

- La définition de vos besoins,
- L'établissement de votre parcours formation,
- L'étude des modalités de prise en charge.

Nos formations sont adaptées aux particularités des TPE & PME :

- Accessibles quel que soit votre niveau,
- Directement opérationnelles en entreprise.

Durée : 7h

Public : Salariés des 54 branches professionnelles et l'interprofession relevant du champ de l'OPCO EP, Chefs d'entreprise, artisan et leur conjoint, l'ensemble des salariés, créateurs d'entreprises et demandeurs d'emploi.

Plages horaires : De 8h à 12h30 et de 13h à 17h30

Formateur.trice : Expert(e) du domaine, formateur (trice) numérique à la CMA PACA

Effectif : 5 à 12 personnes

Suivi et évaluation :

- Acquis mesurés en entrée et en fin de formation.
- Attestation de formation.

Moyens et méthodes pédagogiques :

- Atelier participatif en petit groupe.
- 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).
- Utilisation de WOOLAP régulière comme Ice Breaker, respiration ou évaluation formative.
- Feedback individualisé et collectif.

Modilité d'inscription :

Pour les chefs d'entreprise, artisan, salarié, hors opco ep, toute l'année, jusqu'à 1 semaine avant le début de la formation, après entretien préalable et signature d'une convention de formation simplifiée. Pour les salariés de l'OPCO EP inscription via la plateforme de l'OPCO EP, consulter nos conseillers !

Séquence 1 :

Enjeux, risques et bonnes pratiques de base

Matin

Bienvenue et mise en route

- 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.
- Introduction à la cyber sécurité.
- 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.
- Identification des risques informatiques.

Présentation des principaux risques :

- Hameçonnage (phishing) et attaques par ingénierie sociale.
- Rançongiciels (ransomwares) et autres logiciels malveillants.
- Faillies 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.
- Mise en place des bonnes pratiques de sécurité de base.
- 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.

Séquence 2 :

RGPD, outils et gestion des incidents

Après-midi

Introduction au RGPD et protection des données sensibles

- 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.
- Outils et gestion des incidents.
- 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.
- Réflexes sécuritaires et bilan.
- Développement de réflexes sécuritaires adaptés à l'activité quotidienne.
- Conseils pour sensibiliser les collaborateurs à la cyber sécurité et au RGPD.
- Bilan de la formation et évaluation.
- Révision des points clés de la formation.
- Questions/réponses.

Partout présents

LA CHAMBRE
DE MÉTIERS ET DE L'ARTISANAT PROVENCE-ALPES-CÔTE D'AZUR

ALPES-DE-HAUTE-PROVENCE
formationcontinue04@cmar-paca.fr

HAUTES-ALPES
formationcontinue05@cmar-paca.fr

ALPES-MARITIMES
formationcontinue06@cmar-paca.fr

BOUCHES-DU-RHÔNE
formationcontinue13@cmar-paca.fr

VAR
formationcontinue83@cmar-paca.fr

VAUCLUSE
formationcontinue84@cmar-paca.fr

**CHAMBRE DE MÉTIERS ET DE L'ARTISANAT
PROVENCE-ALPES-CÔTE D'AZUR**

Direction Régionale Formation - 5 boulevard Pèbre, 13008 Marseille
N° SIRET : 130.020.878.00240
Déclaration d'activité enregistrée sous le n° 93.13.15755.13 auprès du
préfet de région PACA

Notre centre de contact :

04 84 31 00 00 - contact@cmar-paca.fr



Pour plus d'informations

Rdv sur cmar-paca.fr/catalogues-des-formations