UMiH FORMATiON

Patricia LARCHER
Tél : 07 88 11 38 20
patricia.larcher@umihformation.fr
contact@travelproformations.fr

PROGRAMME

# CYBERSECURITE

PUBLIC : **Cette formation s'adresse aux dirigeants de TPE/PME/CHR, toutes les personnes membre de l'organisation qui manipulent des données à caractère personnel.**

PRÉ REQUIS : PRESENTIEL : Aucun
VISIO : Connexion internet et PC ou tablette avec Webcam.

À L'ISSUE DE CETTE FORMATION, les participants seront capables de :

- Comprendre les enjeux de la cybersécurité pour déployer une démarche et une culture de cybersécurité dans son entreprise.

## FORMATION **7 HEURES**

INTER OU INTRA ENTREPRISES - 6 À 12 PARTICIPANTS

**INTERVENANTS**
Spécialisés dans les techniques de négociation

**METHODE**
Apports théoriques animés en formation à distance en salle virtuelle -Support formateur partagé - Support de formation envoyé par mail Pédagogie active et participative. Exercices collectifs de mise en application et jeux de rôle débriefés et corrigés avec le formateur.

### ■ SENSIBILISATION AUX BONNES PRATIQUES EN MATIERE DE RGPD

1. PRESENTATION DU RGPD, DE LA CNIL ET DES ENJEUX.
2. U'EST-CE QU'UNE DONNEE PERSONNELLE, UNE DONNEE SENSIBLE ?
3. IMPACT DU RGPD SUR L'ENTREPRISE, SES COLLABORATEURS, SES CLIENTS ET SA GESTION DES DONNEES PERSONNELLES.
4. QUI SONT LES ACTEURS DE LA CONFORMITE DANS L'ENTREPRISE [RP, DPO, CIL] ?
5. COMMENT L'ENTREPRISE DEMONTRE SA CONFORMITE A LA CNIL ?
6. INTRODUCTION AUX BONNES PRATIQUES EN MATIERE DE RGPD :
   - RECENSER & CARTOGRAPHIER LES DONNEES A CARACTERE PERSONNEL.
   - GERER LES ACCES AUX DONNEES PERSONNELLES & LIMITER LES ACCES AUX SEULES DONNEES DONT UN UTILISATEUR A BESOIN. .
   - IDENTIFIER LES SOUS-TRAITANTS QUI MANIPULENT LES DONNEES A CARACTERE PERSONNEL DE L'ENTREPRISE.
   - RECUEIL DU CONSENTEMENT.
   - MINIMISATION DE LA COLLECTE.
   - ASSURER LA SECURITE DES DONNEES PERSONNELLES.
   - L'INFORMATION DU PERSONNEL ET DU CSE.
   - RESPECTER LES DUREES DE CONSERVATION DES DONNEES.
   - RESPECTER LE DROIT D'ACCES DES PERSONNES CONCERNEES.
   - DECLARER TOUTE VIOLATION DE DONNEES.
   - UTILISATION DE LA MESSAGERIE ET RGPD.
   - TELETRAVAIL ET RESPECT DU RGPD.
   - FAIRE VIVRE LA CONFORMITE EN INFORMANT LE RESPONSABLE DE TRAITEMENT ET LE DPO DE MISE EN OEUVRE DE TOUT NOUVEAU TRAITEMENT, INFORMATISE OU NON IMPLIQUANT DES DONNEES A CARACTERE PERSONNEL.
7. LES BIENFAITS DE LA CONFORMITE ?
8. JE NE RESPECTE PAS LE RGPD, QUELS SONT LES RISQUES CAS DE PLAINTE, D'EXERCICE DE DROITS D'ACCES OU DE CONTROL ?

Patricia LARCHER
Tél : 07 88 11 38 20
patricia.larcher@umihformation.fr
contact@travelproformations.fr

## ■ SENSIBILISATION AUX BONNES PRATIQUES EN MATIERE D'INFORMATIQUE, DE PROTECTION DES DONNEES ET DE CYBERSECURITE.

1. POURQUOI SECURISER SON INFORMATIQUE ?
2. LES ACTEURS DE LA CYBERSECURITE EN FRANCE.
3. ET SI VAUBAN AVAIT POSE LES FONDEMENTS DE LA SECURITE INFORMATIQUE ?
4. CONNAITRE LE SYSTEME D'INFORMATION ET IDENTIFIER LE PATRIMOINE INFORMATIONNEL DE SON SYSTEME D'INFORMATION.
5. INVENTAIRE DES MENACES ET DES PARADES :
   - RANÇONGICIEL.
   - HAMEÇONNAGE.
   - PIRATAGE DE COMPTE.
   - INTRUSION DANS LE SI ET VOL DE DONNEES.
   - USURPATION D'IDENTITE ET ARNAQUE AU PRESIDENT.
   - FRAUDE AU VIREMENT.
   - DENI DE SERVICES.
   - DEFIGURATION DE SITE INTERNET.
6. LA MENACE NE VIENT PAS FORCEMENT DE L'EXTERIEUR…
7. UTILISER LES BONNES PRATIQUES RECOMMANDEES PAR L'ANSII :
   - CHOISIR AVEC SOIN SES MOTS DE PASSE.
   - METTRE A JOUR REGULIEREMENT VOS LOGICIELS.
   - BIEN CONNAITRE SES UTILISATEURS ET SES PRESTATAIRES.
   - UTILISER UN ANTIVIRUS.
   - EFFECTUER DES SAUVEGARDES REGULIERES.
   - SECURISER L'ACCES WI-FI DE VOTRE ENTREPRISE.
   - ÊTRE AUSSI PRUDENT AVEC SON ORDIPHONE OU SA TABLETTE QU'AVEC SON ORDINATEUR.
   - PROTEGER SES DONNEES LORS DE SES DEPLACEMENTS.
   - ÊTRE PRUDENT LORS DE L'UTILISATION DE SA MESSAGERIE.
   - TELECHARGER SES PROGRAMMES SUR LES SITES OFFICIELS DES EDITEURS.
   - ÊTRE VIGILANT LORS D'UN PAIEMENT SUR INTERNET.
   - SEPARER LES USAGES PERSONNELS DES USAGES PROFESSIONNELS.
   - PRENDRE SOIN DE SES INFORMATIONS PERSONNELLES, PROFESSIONNELLES ET DE SON IDENTITE NUMERIQUE.
8. TELETRAVAIL ET BYOD.
9. COMMENT REAGIR EN CAS CYBERATTAQUE ?
10. JE SUIS CYBER VICTIME QUE FAIRE ?
    - ECHANGES AVEC LES PARTICIPANTS ET REPONSES AUX QUESTIONS

VALIDATION DE LA FORMATION : Remise d'une attestation de formation.