CYBERSECURITE – LES BONNES PRATIQUES

Durée	1/2 jour	Référence Formation	4-SE-DEF1

Objectifs
Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques

Participants
Responsable, technicien, correspondant informatique

Pré-requis
Il est nécessaire d'avoir une réelle connaissance informatique.

Moyens pédagogiques
Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME
Accueil et introduction
Accueil des participants
Présentation de l'objectif du cours
Brève introduction à la cybersécurité

Les menaces en ligne pour les TPM et PME
Les principales menaces en ligne : phishing, ransomware, malware, etc.
Les menaces venant de l'intérieur : virus, vol de données, destruction de données…
Exemples de cas réels de cyberattaques contre les petites entreprises
Les conséquences financières et de réputation des cyberattaques

Bonnes pratiques en Cybersécurité
Utilisation de mots de passe forts et uniques
Cryptage de fichiers
Mises à jour régulières des logiciels
Sensibilisation à l'email et aux pièces jointes suspectes
Sensibilisation aux bonnes pratiques : usb, échanges de documents, gestion des comptes…
Travail à distance et prestataires extérieurs
Accès au réseau en inter, Wi-Fi…

Comment sécuriser mon environnement Windows et Microsoft ?
Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11…)
Conseils pour sécuriser mon domaine et Active Directory
Outils et conseils pour sécuriser mon serveur de fichiers
Conseils pour la gestion du réseau et des serveurs applicatifs