Cybersécurité, de la sensibilisation à l'action concrète pour les TPE et PME

Un parcours conçu pour ancrer les réflexes cybersécurité dans le quotidien de vos collaborateurs

Objectifs pédagogiques

- Comprendre le contexte et les enjeux de la cybersécurité.
- Revoir les bases informatiques utiles à la sécurité.
- Identifier les principales menaces.
- Reconnaître des cas concrets d'attaques.
- Adopter les bons réflexes au quotidien.

Participants et prérequis

- Tous les collaborateurs d'une entreprise
- Dirigeants, membres du CODIR, les responsables de sites et managers opérationnels

Pré-requis :

- Connaître les bases informatiques
- Utiliser les outils informatiques de l'entreprise

Méthode pédagogique :

Formation en présentiel.

Cette formation interactive de 3 heures combine théorie et pratique pour sensibiliser les collaborateurs aux enjeux de la cybersécurité et du RGPD.

Les points forts

- Comprendre les menaces numériques qui ciblent les TPE/PME sans jargon technique.
- Adopter les bonnes pratiques d'hygiène numérique au quotidien, expliquées de manière claire et vulgarisée.
- Reconnaître et réagir face à un phishing ou une tentative d'arnaque grâce à des exemples concrets.

Durée

2 demi-journées (7 h)

Délais d'accès : de 7 jours à 3 mois selon le mode de financement.

Programme

1ère demi-journée

- Introduction et contexte : la cybersécurité aujourd'hui
- Back-to-Basic : l'informatique d'entreprise c'est quoi ?
- Enjeux cybersécurité pour votre entreprise
- Panorama non exhaustif des menaces
- Cas concrets & mise en situation
- Synthèse : devenez la 1ère défense de votre entreprise

2ème demi-journée

Grâce à un jeu pédagogique, les participants découvrent de façon ludique les risques numériques, testent leurs réflexes face à des incidents et identifient les bonnes pratiques à adopter au quotidien.

Déroulé en 4 étapes :

- Introduction : contexte, enjeux cyber et RGPD.
- Mise en jeu : découverte des règles et constitution des équipes.
- Partie collective : chaque équipe fait face à des scénarios (phishing, vol de données, incidents techniques) et choisit ses stratégies de protection.
- Débrief : analyse des décisions, mise en perspective avec la réalité de l'entreprise et rappel des bons réflexes.

Bénéfices :

- Une sensibilisation engageante et mémorable.
- Une meilleure appropriation des enjeux de cybersécurité.
- Le développement d'une culture commune de la vigilance au sein de l'entreprise.