Cybersécurité - Découverte

Introduction à la cybersécurité pour les TPE et collectivités

Cette formation de 2 jours de **découverte de la cybersécurité** est destinée aux **dirigeants, gestionnaires et employés des petites structures et collectivités** ayant peu de connaissances préalables en cybersécurité.

Elle vise à **sensibiliser sur les menaces**, comprendre le fonctionnement mais surtout à **adopter des pratiques de sécurité de base** et à **réagir efficacement** en cas d'incidents.

L'objectif est d'inculquer les **bonnes pratiques de sécurité** de base adaptées aux **petites structures et collectivités**, en proposant des **solutions accessibles**, des **plans d'action** en cas d'incidents et en encourageant le **développement d'une culture de sécurité** au sein des entreprises de petite taille.

Objectifs

Appréhender les risques spécifiques aux petites entreprises (TPE)	Maîtriser les bases pour protéger l'entreprise des cyberattaques	Apprendre à réagir face à des incidents de sécurité	Sélectionner des outils de protection accessibles et efficaces	Instaurer une culture de vigilance au sein de l'équipe

Publics cibles

Ce parcours est ouvert aux dirigeants, gestionnaires et employés de petites structures (TPE) et collectivités ayant peu de connaissances en cybersécurité et souhaitant se sensibiliser.

Pré-requis et objectifs pédagogiques

Aucune connaissance préalable spécifique en cybersécurité n'est nécessaire pour aborder les objectifs pédagogiques suivants :

- Comprendre les Menaces
- Appliquer les bonnes pratiques
- Réagir aux Incidents
- Choisir des Solutions Adaptées
- Cultiver une Culture de Sécurité

Programme

Cette formation se démarque par son approche pratique et opérationnelle.

Elle est proposée en présentiel, dure 14 heures, et est déployée sur deux journées consécutives.

Axée sur les enjeux spécifiques aux petites entreprises, elle combine des présentations interactives et des études de cas concrets pour offrir une vision approfondie des menaces cybernétiques.

Ce programme débutera par une contextualisation de la cybersécurité et son importance dans l'environnement numérique actuel, puis sera fait un aperçu rapide des normes majeures avec une brève mention de leur application, ainsi qu'une présentation succincte sur l'importance de la conformité intersectorielle.

1. Panorama des menaces et des risques cybernétiques pour les petites structures et collectivités

> Introduction aux menaces courantes
Rappel sur les systèmes d'information d'une entreprise
Présentation des types de menaces

> Identification des risques spécifiques aux petites structures et collectivités
Analyse des vulnérabilités propres aux petites structures
Exemples concrets

> Illustration des conséquences financières et opérationnelles
Mise en lumière des impacts financiers et opérationnels des attaques

2. Sensibilisation aux attaques courantes : phishing, ransomware, etc.

> Exploration des techniques d'attaque fréquentes
Découverte des méthodes et analyse

> Études de cas : Illustration de scénarios réels et de leurs impacts

> Mécanismes de propagation des menaces
Compréhension des mécanismes appuyés sur des exemples concrets

3. Bonnes pratiques de sécurité de base pour les entreprises de petite taille :

> Bonnes pratiques de sécurité
Mots de passe robustes, mises à jour, sauvegardes, etc…

> Conseils pratiques pour sécuriser les périphériques et les données
Mesures simples pour renforcer la sécurité

> Stratégies simples de protection et de prévention adaptées aux petites structures et collectivités
Application de mesures de sécurité proportionnées

4. Plan d'action en cas d'incident cybernétique spécifique aux petites structures et collectivités :

> Définition d'un plan de réponse aux incidents
Élaboration d'un plan adapté, mise en pratique

> Méthodologie pour identifier, isoler et résoudre les incidents rapidement
Processus d'intervention rapide, exemples concrets

> Sensibilisation à la communication et à la notification des incidents aux autorités compétentes

5. Solutions de protection accessibles aux petites entreprises et collectivités :

> Présentation des outils et logiciels accessibles
Sélection d'outils abordables pour renforcer la sécurité (Annuaire, poste de travail, messagerie, accès, réseaux et Cloud)

> Choix des solutions en fonction des besoins et des budgets des petites structures et collectivités
Sélection judicieuse des solutions selon les ressources disponibles

6. Développement d'une culture de sécurité au sein des petites entreprises et collectivités :

> Formation du personnel aux bonnes pratiques de sécurité
Sensibilisation des employés, renforcer la vigilance de son personnel

> Sensibilisation continue et programmes de formation adaptés aux petites structures et collectivités
Mise en place de processus pour maintenir une culture de sécurité

> Mise en place de Processus internes
Signalisation des incidents et réaction rapide

Compétences ciblées

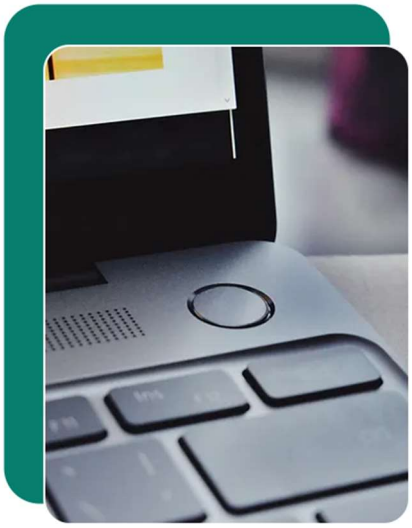
- Appréhender les risques spécifiques aux petites entreprises (TPE)
- Maîtriser les bases pour protéger l'entreprise des cyberattaques
- Apprendre à réagir face à des incidents de sécurité
- Sélectionner des outils de protection accessibles et efficaces
- Instaurer une culture de vigilance au sein de l'équipe

Moyens pédagogiques

Cette formation s'appuie sur des **études de cas**, des **démonstrations pratiques**, et des discussions stimulantes pour offrir une **expérience d'apprentissage immersive**.

Elle fournit aux participants une **connaissance approfondie** des défis concrets de la cybersécurité, des **compétences pratiques** pour renforcer la sécurité des petites entreprises, et une **expertise opérationnelle** pour réagir efficacement aux incidents.

Cette formation vise à **autonomiser les participants** en les dotant des connaissances pratiques nécessaires pour **sécuriser les systèmes d'information** des TPE et à **instaurer une culture de sécurité durable** au sein de ces entreprises.



Moyens d'encadrement

La formation est assurée par un formateur.rice expert.e en cybersécurité, disposant d'une expérience professionnelle significative sur la thématique et une expérience en techniques

Modalités d’évaluation

Les évaluations se dérouleront à travers des tests pratiques simplifiés évaluant la compréhension des principes de sécurité fondamentaux.

Le dispositif d’évaluation est composé de :

- Questionnaires à choix multiples pour évaluer les connaissances théoriques sur les menaces et les pratiques de sécurité.
- De simulations d'attaques simples pour évaluer la réaction des participants face à des scénarios d'attaques basiques

Ces méthodes d'évaluation permettront de mesurer la compréhension, la réactivité et l'application des connaissances acquises lors de la formation.

Une attestation de réalisation est remise à chaque participant à l’issue de la formation. Une attestation de réussite est remise aux participants satisfaisant les critères de réussite de la formation.

Prix et modalités d'accès

La formation est commercialisée en inter-entreprise et en intra-entreprise pour des groupes de 6 à 12 personnes.

Prix HT : à partir de 1550€