FORMASUITE

PROGRAMME DE LA FORMATION

Cybersécurité pour les PME : Prévenir et Réagir face aux Menaces

Le 22/11/2026

OBJECTIFS DE LA FORMATION

À l'issue de la formation, le participant sera capable de mettre en œuvre les compétences suivantes :

- Identifier les menaces liées aux systèmes d'information
- Maîtriser les conséquences des menaces cyber sur les organisations et leurs collaborateurs
- Comprendre les outils pour protéger les échanges de mails et éviter les dangers
- Adopter les bonnes pratiques pour sécuriser les données de l'entreprise
- Identifier les comportements à risque lors de la navigation sur le web
- Détecter les principaux dangers dans l'utilisation d'une messagerie électronique

CONTENU

AVANT LA FORMATION
Entretien téléphonique avec le formateur afin de personnaliser votre formation.
Le programme de formation ci-dessous pourra donc être modifié gratuitement en fonction de vos attentes.

Jour 1 : Comprendre les Menaces et Identifier les Risques
Matin : Identifier les menaces liées aux systèmes d'information

- Présentation des principales menaces cybernétiques ciblant les PME
- Explication des termes clés : phishing, ransomware, malware et autres attaques
- Identification des points faibles des systèmes d'information et des réseaux
- Analyse des risques liés à l'utilisation d'outils numériques non sécurisés
- Présentation des comportements à risque pouvant compromettre la sécurité

Après-midi : Maîtriser les conséquences des menaces cyber

- Impact des cyberattaques sur les entreprises, leurs données et leur activité
- Conséquences financières, juridiques et réputationnelles des incidents cyber
- Effets sur les collaborateurs, leurs performances et leur confiance
- Obligations légales et réglementaires en matière de cybersécurité pour les PME
- Présentation des scénarios fréquents d'attaques et de leurs impacts concrets

Jour 2 : Protéger les Données et Adopter les Bonnes Pratiques
Matin : Protéger les échanges de mails et détecter les dangers

- Présentation des outils pour sécuriser les échanges de mails et les pièces jointes
- Importance du chiffrement et de l'authentification multifactorielle pour les emails
- Détection des emails frauduleux et des pièces jointes malveillantes

CONTACTEZ NOUS

Du Lundi au Vendredi
de 9h00 à 12h30 et de 13h30 à 17h00
Par téléphone au **05 31 60 07 07**
Par email : serviceclient@formasuite.fr
Responsable Pédagogique : Yannick Lacave

FORMASUITE
12 rue Courbet 82000 Montauban
SIRET : 842 016 594 00017
N° de déclaration d'activité : 76820087382

- Analyse des risques liés à l'utilisation de messageries électroniques non sécurisées
- Adoption de bonnes pratiques pour éviter les erreurs humaines dans la gestion des emails

Après-midi : Adopter les bonnes pratiques pour protéger les données

- Sensibilisation à la gestion des accès et à la limitation des privilèges utilisateurs
- Importance des sauvegardes régulières pour prévenir les pertes de données critiques
- Mises à jour des logiciels et systèmes pour corriger les failles de sécurité
- Encourager une politique de cybersécurité continue et adaptée aux PME
- Sensibilisation des collaborateurs à l'importance de leur rôle dans la protection des données

FIN DE LA FORMATION

Débrief de la formation avec le formateur pour consolider vos connaissances.

PREREQUIS

Aucun

PUBLIC VISE

Tout public

- Formation individuelle ou collective (garantie à partir du premier inscrit)
- Formation assurée au sein de vos locaux ou dans une salle de formation dans la ville de votre choix
- Dates de votre choix sans surcoût
- Entretien téléphonique préalable avec notre formateur afin de personnaliser votre formation
- Inscription à réaliser 15 jours avant le démarrage de la formation
- Horaires : de 9h à 12h30 et de 13h30 à 17h
- Nombre de participants : de 1 à 20 participants (au delà nous consulter)
- **Formation accessible à toutes personnes porteuses de handicap. Locaux adaptés.**

DUREE

14 heures

PEDAGOGIE

Montée en compétence assurée par l'association d'un contenu théorique et pratique. Etude de cas concrets en rapport avec votre quotidien professionnel.

Suivi de l'exécution :

- Feuilles de présences signées des participants et du formateur par demi-journée
- Attestation de fin de formation mentionnant les objectifs, la nature et la durée de l'action et les résultats de l'évaluation des acquis de la formation.

Appréciation des résultats :

- Recueil individuel des attentes du stagiaire
- Questionnaire d'auto-évaluation des acquis en début et en fin de formation
- Évaluation continue durant la session
- Remise d'une attestation de fin de formation
- Questionnaire d'évaluation de la satisfaction en fin de formation

Moyens et supports pédagogiques :

- Evaluation des besoins et du profil du participant
- Apport théorique et séquences pédagogiques regroupées en différents modules
- Cas pratiques
- Questionnaire et exercices
- Tests de contrôle de connaissances et validation des acquis à chaque étape
- Retours d'expériences
- Séquences pédagogiques regroupées en différents modules,
- Remise d'un support pédagogique
- Echanges interactifs
- Intervention d'un formateur expert dans son domaine

Modalités d'évaluation et de suivi :

- Grille d'évaluation (test de positionnement)
- Entretien téléphonique avec le formateur avant la formation
- Travaux pratiques
- Tests de contrôle de connaissances et validation des acquis à chaque étape
- Echange avec le formateur par visioconférence (webinar), téléphone et mail
- Exercices corrigés, études de cas réels, mise en application concrète et utile
- Évaluation pour valider vos acquis en fin de formation

Profil du formateur :

- Chaque formation est sous la responsabilité du directeur pédagogique de l'organisme de formation.
- Le bon déroulement est assuré par le formateur désigné par l'organisme de formation.
- Formateur référent : M.Lacave Téléphone : 05 31 60 07 07

Une attestation de formation sera délivrée au stagiaire.