Cybersécurité pour le dirigeant TPE-PME

Une cyberattaque coute en moyenne 25 000 euros a une TPE-PME et 60 % d entre elles ne s en relevent pas. En 1 jour, mettez en place les 10 mesures qui protegent votre entreprise.

ESSENTIEL CYBERSÉCURITÉ 1 jour (7h)

INFORMATIONS PRATIQUES

Référence	**LEX-CYB-001**
Formacode	**31006**
Durée	**1 jour (7h)**
Version	**LEX-CYB-001_v1.0 · MAJ**

Une question ?
Contenu, financement, organisation — réponse sous 24h.

contact@lexora-formation.fr
05 54 07 30 33

LE CONSTAT

En 2025, 43 % des cyberattaques ciblent les TPE-PME (rapport ANSSI 2024). Le cout moyen d une attaque pour une petite structure est de 25 000 euros, et 60 % des entreprises victimes deposent le bilan dans les 18 mois (etude Hiscox 2024).

NOTRE RÉPONSE

En 1 jour, vous identifiez vos vulnerabilites, mettez en place les protections essentielles et formez vos reflexes face aux menaces les plus courantes.

Source : ANSSI - Panorama de la cybermenace 2024, publie fevrier 2025 · Hiscox - Rapport annuel sur la gestion des cyber-risques 2024

POUR QUI

PUBLIC CIBLE

Dirigeants de TPE-PME, auto-entrepreneurs, gerants et responsables souhaitant proteger leur activite contre les cybermenaces sans expertise technique prealable.

PRÉREQUIS

Aucun prerequis technique. Savoir utiliser un ordinateur et une messagerie email.

Délai d'accès : 14 jours ouvres avant la session

LES BÉNÉFICES DE LA FORMATION

Concrètement, après cette formation

- ✓ Vous evaluez le niveau de securite de votre entreprise grace a un audit simplifie que vous realisez vous-meme
- ✓ Vous detectez les emails de phishing et les tentatives d arnaque avant qu ils ne causent des degats
- ✓ Vous mettez en place les 10 protections essentielles sans avoir besoin d un prestataire informatique
- ✓ Vous repartez avec un plan de continuite d activite pret a deployer en cas d incident

OBJECTIFS PÉDAGOGIQUES

À l'issue de cette formation, vous serez capable de

1. Identifier les principales cybermenaces ciblant les TPE-PME et evaluer le niveau de vulnerabilite de son entreprise
2. Mettre en oeuvre les 10 mesures de securite essentielles recommandees par l ANSSI pour proteger son activite
3. Detecter une tentative de phishing ou d ingenierie sociale et appliquer les reflexes de protection adaptes
4. Elaborer un plan de continuite d activite simplifie integrant les procedures de sauvegarde et de reprise apres incident

PROGRAMME DÉTAILLÉ

Le programme sur 1 jour (7h)

MOD-CYB-001 — MOD-CYB-001 - Comprendre les cybermenaces en TPE-PME — 2h

- Panorama des menaces 2025-2026 : phishing, ransomware, compromission de messagerie. Pourquoi les TPE-PME sont des cibles privilegiees. Analyse de 3 cas reels d attaques sur des petites structures. Les consequences financieres, juridiques et reputationnelles.

MOD-CYB-002 — MOD-CYB-002 - Auditer et proteger son environnement — 2h

- Les 10 mesures ANSSI pour les TPE-PME. Audit de securite simplifie : mots de passe, sauvegardes, mises a jour. Configuration des protections : double authentification, gestionnaire de mots de passe. Securisation de la messagerie et du Wi-Fi.

MOD-CYB-003 — MOD-CYB-003 - Detecter et reagir face aux menaces — 1h30

- Reconnaitre un email de phishing : les 7 signaux d alerte. Ingenierie sociale : techniques et parades. Que faire en cas d incident : les 5 premieres minutes. Simulation de phishing en temps reel.

MOD-CYB-004 — MOD-CYB-004 - Construire son plan de continuite — 1h30

- Strategie de sauvegarde 3-2-1. Plan de continuite d activite simplifie. Assurance cyber : ce qu il faut savoir. Plan d action individuel a 30 jours avec checklist.

MODALITÉS PÉDAGOGIQUES

Notre approche

MÉTHODE
Cas réels
Ateliers pratiques : audit de securite simplifie, simulation de phishing, configuration de protections. Cas reels d attaques sur des TPE-PME. Format 8 max.

FORMAT
8 max
Interaction garantie avec le formateur

MOYENS
Support + outils
Presentiel : salle equipee videoprojecteur, paperboard, WiFi. Distanciel : Zoom, support partage en temps reel. Chaque participant recoit : support PDF, checklist securite, plan d action.

RATIO
75% pratique
Vérifié sur scénario minuté

75% Pratique — cas réels, QCM, échanges — 25% Théorie

Moyens techniques — Presentiel : salle equipee videoprojecteur, paperboard, WiFi. Distanciel : Zoom, support partage en temps reel. Chaque participant recoit : support PDF, checklist securite, plan d action.

FORMATEUR RÉFÉRENT

Sebastien Hurstel
Consultant digital - Specialiste securite et transformation numerique
Entrepreneur et consultant digital, Sebastien accompagne les dirigeants de TPE-PME dans la securisation de leur environnement numerique. Il traduit les enjeux techniques en actions concretes et accessibles.

Cette formation peut également être animée par tout formateur qualifié par LEXORA.

ACCESSIBILITÉ

Formation accessible PSH
Adaptation sur demande.
Référent : William Bigot
accessibilite@lexora-formation.fr
0612225849

ÉVALUATION

Comment nous mesurons vos acquis

AVANT
Questionnaire de positionnement

PENDANT
Exercices pratiques + QCM par bloc

APRÈS
Evaluation a chaud + attestation de competences

Suivi de l'exécution — Feuilles d emargement signees par demi-journee, attestation d assiduite, certificat de realisation remis en fin de formation.

☆ PARCOURS PRÉ & POST-FORMATION

J+7	J+14 - J+42	J+30	J+60
Email recapitulatif + checklist securite	1 action securite / semaine pendant 4 semaines	Evaluation a froid + feedback formateur	Webinaire Q&A Retour terrain

TARIFS

MODALITÉ	FORMAT	TARIF
Sur-mesure		*Cette formation est disponible en intra-entreprise sur mesure.*