Cybersécurité pour les TPE/PME et associations

Version 3 jours — Approfondissement • Catalogue NTech Conseil

Un parcours complet pour passer du “socle d’hygiène” à une organisation de sécurité opérationnelle. Les participants construisent une feuille de route à 3 mois, mettent en place des réglages essentiels, et apprennent à réagir en cas d’incident, avec des outils et des procédures simples.

Objectifs pédagogiques

À l’issue de la formation, le stagiaire sera en mesure de :

- Évaluer les principaux risques d’une structure et prioriser les actions de sécurité.
- Mettre en place des pratiques d’authentification et de gestion des accès robustes.
- Sécuriser les postes, les téléphones et les services cloud utilisés au quotidien.
- Structurer la sauvegarde, la continuité et la réaction à incident (procédure simple).
- Construire une feuille de route cybersécurité sur 3 mois (jalons, responsables, indicateurs).

Durée

3 jours (21h)

Nombre de participants

- Minimum : 6
- Maximum : 15

Tarifs

Les tarifs ci-dessous sont fournis à titre indicatifs et seront adaptés selon le programme pédagogique défini.
Prix inter « Approfondissement » : 2 100€ HT/stagiaire
Forfait intra : nous consulter
Sur-mesure : nous consulter

Public concerné

Dirigeants, responsables d’équipe, référents numériques, salariés impliqués dans l’administration, bénévoles associatifs responsables.

structure (messagerie, cloud, outils de travail).

Programme de la formation

- Jour 1 — Sensibilisation avancée : menaces, hameçonnage, fraude, rançongiciel, erreurs humaines.
- Cartographie rapide des actifs : comptes, appareils, services, données sensibles.
- Gestion des accès : rôles, droits, partages, comptes génériques, départ d'un salarié/bénévole.
- Mots de passe : gestionnaire d'équipe, règles, récupération, bonnes pratiques.
- Double facteur : stratégie de déploiement (services prioritaires) et accompagnement des utilisateurs.
- Jour 2 — Sécurisation des postes et mobiles : mises à jour, navigateur, extensions, antivirus, sauvegardes locales.
- Réseau et Wi-Fi : bonnes pratiques, séparation invités, mots de passe, routeur/box.
- Sauvegardes : 3-2-1, choix des supports, fréquence, tests de restauration, stockage hors ligne.
- Jour 3 — Procédures : gestion d'incident (qui fait quoi), premières actions, preuves, communication.
- Prévention continue : routine mensuelle, check-list, sensibilisation interne.
- Ateliers : simulation de scénarios (mail suspect, compte compromis, perte de téléphone).
- Feuille de route 3 mois : priorités, budget, responsabilités, calendrier.

Modalités et délais d'accès

Toute demande de renseignement et d'inscription est traitée sous 48h.
Délai moyen d'accès selon financement et disponibilités : 3 à 6 semaines.

Modalités pédagogiques et techniques

- Apports théoriques et retours d'expérience (cas concrets).
- Démonstrations et réglages pas-à-pas sur les outils utilisés par les participants.
- Ateliers pratiques : check-lists, exercices guidés, simulations.
- Travail sur les procédures et l'organisation interne (adaptée à la structure).
- Restitution collective et plan d'action finalisé.

Suivi

- Une feuille d'émargement permet de suivre la présence des participants.
- Les supports pédagogiques sont remis au fil de la formation, et une synthèse des ressources est fournie en fin de session.
- La session débute par un recueil des attentes pour adapter le déroulé si nécessaire, et se termine par un bilan de fin de formation.
- Les modalités d'accessibilité sont rappelées en amont afin de garantir des conditions d'accueil adaptées à chacun.

Modalités techniques

- En distanciel :
- Visioconférence (Teams/Zoom).
- Partage d'écran, chat et tableau collaboratif.
- PC individuel obligatoire avec une connexion Internet stable.

- Salle équipée (écran ou vidéoprojecteur).
- Accès Internet.
- Supports fournis en version numérique.

Encadrement

La formation est animée par un formateur spécialisé en cybersécurité, sensibilisation et bonnes pratiques d'hygiène numérique. Le contenu est ajusté selon votre environnement (outils, effectif, contraintes).

Évaluation des acquis & livrables

Les acquis des stagiaires sont évalués tout au long de la formation à travers des questions, des échanges et des exercices pratiques.
Dans le cadre de la formation, plus spécifiquement :

- Diagnostic d'entrée (questionnaire + échanges sur les usages et incidents passés).
- Évaluations formatives en continu (exercices, réglages, simulations).
- Évaluation sommative : feuille de route cybersécurité 3 mois + procédures essentielles.
- Check-lists (accès, postes, mobiles, sauvegardes, incident) et modèles de documents.
- Mini-audit guidé des comptes et services (liste des actions à appliquer).
- Attestation de réalisation.

Taux de satisfaction

Indicateurs calculés sur l'ensemble de nos actions de formation, toutes thématiques confondues (pas de statistiques individuelles par formation). Mise à jour : 07/01/2026.
• Satisfaction globale : 4,47/5
• Taux d'abandon : 0 %
• Taux de réponse : 100 %

Accessibilité aux personnes en situation de handicap

Adaptations possibles (rythme, supports pas-à-pas, police lisible, assistance technique).
Référent accessibilité : Sylvain Buthaud – sylvain.buthaud@ntechconseil.fr