Cybersécurité pour les TPE/PME et associations

Version 1 jour — Découverte • Catalogue NTech Conseil

Une journée très concrète pour comprendre les risques numériques du quotidien et mettre en place un socle d'hygiène simple : mots de passe, authentification renforcée, mises à jour, sauvegardes, et réflexes face aux messages frauduleux. L'objectif est de repartir avec une check-list et un plan d'action réaliste sur 30 jours.

Objectifs pédagogiques

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

- Identifier les menaces courantes (hameçonnage, mots de passe compromis, rançongiciel, fraude au président).
- Adopter les bons réflexes de sécurité au quotidien (mises à jour, verrouillage, droits, partage).
- Mettre en place un socle d'authentification (gestionnaire de mots de passe, double facteur).
- Sécuriser ses données avec une stratégie de sauvegarde simple et testée.
- Construire un plan d'action priorisé sur 30 jours, adapté à la structure.

Durée

1 jour (7h)

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 « Découverte » : 140€ HT/stagiaire
Forfait intra : nous consulter
Sur-mesure : nous consulter

Public concerné

Dirigeants, responsables d'équipe, fonctions support, salariés, bénévoles associatifs, référents numériques.

Aucun prérequis technique ; savoir utiliser un navigateur web et la messagerie.

Programme de la formation

- Panorama des risques actuels et vocabulaire simple (sans jargon).
- Reconnaître un message frauduleux (signaux d'alerte) et réagir correctement.
- Mots de passe : bonnes pratiques, gestionnaire, règles d'équipe.
- Authentification renforcée : activer le double facteur sur les services clés.
- Mises à jour et sécurisation des postes (PC/Mac), du navigateur et du téléphone.
- Sauvegardes : principe 3-2-1, choix des supports, test de restauration.
- Données sensibles : classement rapide, partages, stockage cloud, précautions RGPD de base.
- Atelier guidé : diagnostic express + check-list "socle d'hygiène".
- Plan d'action 30 jours : 3 à 5 mesures prioritaires, responsables, échéances.

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

La formation s'appuie sur une démarche pédagogique active et progressive, centrée sur la mise en pratique.
Elle combine :

- Apports théoriques simples et illustrés (cas réels).
- Démonstrations d'outils et réglages clés (mots de passe, double facteur, sauvegarde).
- Atelier guidé : [illegible]

- Études de cas adaptées aux usages des participants (TPE/PME, associations).

- Échanges interactifs et réponses personnalisées aux besoins.

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.

- En présentiel :

- Salle équipée (écran ou vidéoprojecteur).

- Accès Internet.

Encadrement

La formation est animée par un formateur spécialisé en cybersécurité et en sensibilisation des publics débutants. Les exemples et ateliers sont adaptés à votre contexte (outils utilisés, contraintes, niveau).

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 (quiz court + recueil des usages et points sensibles).
- Évaluations formatives en continu (exercices guidés, repérage de messages frauduleux).
- Évaluation sommative : restitution d'un plan d'action cybersécurité 30 jours.
- Check-list "socle d'hygiène" et charte de bonnes pratiques (modèles fournis).
- Fiche réflexe "Que faire en cas de suspicion d'attaque ?".
- 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