Cybersécurité pour TPE/PME & associations — du socle d'hygiène au plan d'action

Version 3 jours — approfondissement & déploiement (non-technique) • Catalogue NTech Conseil

Intitulé & contexte

Sensibilisation et mise en pratique **sans jargon technique** : hygiène numérique, cartographie des données, premières mesures concrètes (mots de passe, MFA, sauvegardes, mises à jour, phishing), organisation interne, et garde-fous **RGPD & IA Act**. La version 3 jours approfondit les pratiques et met en place des mesures opérationnelles (gestionnaire de mots de passe, politiques simples, checklists), **sans analyse SOC ni techniques expertes**.

Public visé & prérequis

Public visé	**Dirigeants, administratifs, référents numériques, responsables associatifs, équipes support.**
Prérequis	Aucun prérequis technique. Venir avec ses usages (messagerie, stockage, outils métier).

Objectifs opérationnels (fin des 3 jours)

- Disposer d'un **plan de cybersécurité** réaliste : politique mots de passe, MFA, sauvegardes, mises à jour, phishing.
- Déployer un **gestionnaire de mots de passe** d'équipe (structure, partages, politique).
- Mettre en place un **kit incidents** (qui alerter, quoi couper, que garder), sans outillage expert.
- Formaliser une **feuille de route 3 mois** & les responsabilités (RACI simple).

Compétences visées

- Concevoir des **politiques simples** (mots de passe, mises à jour, sauvegardes, messagerie).
- Paramétrer un gestionnaire de mots de passe (coffres, groupes/collections, partage sécurisé).
- Organiser la **réaction à incident** (phishing, vol d'équipement, compte compromis).
- Piloter l'adoption (indicateurs, rituels, sensibilisation continue).

Programme détaillé (3 × 7 h)

Jour 1 — Version 1 jour (intégrale)

09h00–09h30	**Tour de table & **icebreaker** : incidents vécus, représentations des risques.**
09h30–10h30	**Grand quiz cybersécurité** : menaces, mythes & bonnes pratiques (vote & débrief).
10h30–10h45	Pause
10h45–12h15	Atelier — **Phishing** : reconnaître, signaler, simuler ; premiers réflexes (messagerie & navigateur).
12h15–13h45	Déjeuner
13h45–14h30	Atelier — **Mots de passe & MFA** : choisir un gestionnaire (Bitwarden/KeePassXC), créer & partager en équipe.
14h30–15h15	Atelier — **Sauvegardes 3-2-1** : support externe, versioning cloud, test de restauration.
15h15–15h30	Pause
15h30–16h15	**Cartographie des données** & **registre RGPD light** (où/qui/quoi).
16h15–16h45	**IA Act & RGPD** : principes utiles, données sensibles, minimisation & traçabilité.
16h45–17h00	Restitution + **plan d'action 30 jours** (gabarit fourni).

Jour 2 — Pratiques & politiques simples

09h00–09h15	**Récap J1, objectifs J2 ; sélection des chantiers prioritaires.**
09h15–10h00	Gestionnaire de mots de passe (équipe) : coffres, collections, partage ; politique de complexité.
10h00–10h30	MFA : périmètre de déploiement, supports de secours, cas particuliers (comptes partagés).
10h30–10h45	Pause
10h45–11h30	Sauvegardes 3-2-1 : matrice des périmètres (poste, cloud, serveur), fréquence & test de restauration.
11h30–12h15	Mises à jour & durcissement léger : OS, applications, navigateur ; extensions utiles.
12h15–13h45	Déjeuner
13h45–14h30	Messagerie & navigateur : filtres anti-phishing, signatures, gestion des liens/pièces jointes.
14h30–15h15	Kit **réaction à incident** (fiche réflexe, contacts, isolement du poste, changement de mots de passe).
15h15–15h30	Pause
15h30–16h30	Consolidation & documentation : modèles de chartes/procédures, preuves (captures).
16h30–17h00	**Matrice des opportunités (Impact × Effort)** + **plan d'inter-session (15 jours)**.

Jour 3 — REX & déploiement

09h00–10h30	****Retours d'expérience (REX)** inter-session : déploiement réel (gestionnaire, MFA, sauvegardes), difficultés & solutions.**
10h30–10h45	Pause
10h45–11h30	Affinage des politiques : exceptions, cas métiers, procédures de sortie (offboarding).
11h30–12h15	Sensibilisation continue : micro-formations, quiz, rituels d'équipe (5 min/semaine).
12h15–13h45	Déjeuner
13h45–14h30	Tableau de bord **light** : quelques indicateurs (MFA activé, sauvegardes testées, incidents signalés).
14h30–15h15	Conduite du changement : rôles & RACI simple, communication interne, support de 1er niveau.
15h15–15h30	Pause
15h30–16h30	Plan de continuité **basique** : listes de contacts, accès essentiels, procédures minimales.
16h30–17h00	Restitutions finales : **politiques + kit incidents + plan 3 mois**.

Modalités pédagogiques

Apports courts, quiz interactif, ateliers guidés, inter-session accompagnée, co-construction.

Évaluation des acquis & livrables

- Diagnostic d'entrée (usages, incidents vécus, priorités).
- Évaluations formatives en continu (ateliers guidés, revues).
- Évaluation sommative : plan d'action minimal viable + preuves (captures, checklist).
- Bilan de sortie + plan d'action 30 jours (modèle fourni).
- Dossier final : politiques + kit incidents + feuille de route 3 mois.
- Modèles : **politique mots de passe**, **charte d'usage**, **fiche incident** (premiers réflexes).
- Checklists : sauvegardes 3-2-1, mises à jour, MFA, **phishing** (signaux d'alerte).
- Cartographie des données (où/qui/quoi) + registre RGPD light.
- Plan d'action 30 jours + **kit de déploiement** du gestionnaire de mots de passe.
- Attestation de réalisation.

Moyens techniques & organisation

Modalités	**Présentiel (intra/inter) ou distanciel • Groupe 6–15 • PC individuel recommandé.**
Outils mobilisés	Gestionnaire de mots de passe (ex. **Bitwarden/KeePassXC**), application d'authentification (MFA), navigateur web, suite bureautique, support externe pour sauvegardes. Outils d'auto-diagnostic et modèles fournis.

Accessibilité

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

Délais d'accès & financement

Délais d'accès	**Réponse sous 48 h. Délai moyen d'accès : 3 à 6 semaines selon calendrier et financement.**
Financement & tarifs	Éligible financeurs publics/OPCO ; devis personnalisé selon format et contexte.

Satisfaction & réclamations

Indicateurs disponibles sur demande. Réclamations : contact@ntechconseil.fr

Traçabilité

Traçabilité	**Émargements J1/J2/J3, supports, productions (politiques, checklists, captures), bilan de sortie.**
Adaptation	Recueil des attentes, ajustements par équipe, modalités d'accessibilité appliquées.
Évaluation	Diagnostic J1, évaluations formatives, dossier final + soutenance courte.