



GUIDE PRATIQUE · 7IT CYBERSECURITY

Sécuriser Microsoft 365

La checklist essentielle pour protéger vos comptes, vos e-mails et vos données

● SECURE

Microsoft 365 concentre l'essentiel de la vie d'une entreprise : messagerie, documents, réunions, partages. Un seul compte piraté peut ouvrir l'accès à des années d'échanges. Cette checklist rassemble les mesures qui protègent vraiment, classées par thème. Certaines dépendent de vos licences : nous l'indiquons.

1. Comptes et identités

- ☐ L'authentification multifacteur (MFA) est activée pour tous les utilisateurs, direction comprise.
- ☐ Les administrateurs utilisent un compte dédié à l'administration, distinct de leur compte de travail quotidien.
- ☐ Le nombre d'administrateurs globaux est limité à quelques personnes clairement identifiées.
- ☐ Les protocoles d'authentification hérités, qui ne gèrent pas la MFA, sont désactivés.
- ☐ Les comptes des personnes qui quittent l'entreprise sont bloqués le jour même de leur départ.
- ☐ Un gestionnaire de mots de passe est mis à disposition des équipes.

2. Messagerie

- ☐ Les enregistrements SPF, DKIM et DMARC de votre nom de domaine sont configurés : ils limitent l'usurpation de vos adresses.
- ☐ Le transfert automatique des e-mails vers des adresses externes est bloqué.
- ☐ Un avertissement signale les messages venant de l'extérieur de l'entreprise.
- ☐ La protection contre l'hameçonnage et les pièces jointes dangereuses est activée (Microsoft Defender pour Office 365, selon vos licences).

3. Données et partages

- ☐ Les liens de partage « accessibles à toute personne » sont désactivés ou limités dans le temps.
- ☐ Les partages avec l'extérieur sont revus régulièrement, et supprimés quand ils ne servent plus.
- ☐ Les documents importants sont enregistrés dans OneDrive, SharePoint ou Teams, pas sur les postes.
- ☐ Les documents sensibles sont identifiés et protégés par des étiquettes de confidentialité (selon vos licences).

4. Appareils

- ☐ Les ordinateurs sont chiffrés (BitLocker) et reçoivent automatiquement les mises à jour.
- ☐ Les appareils sont gérés avec Microsoft Intune : ils peuvent être verrouillés ou effacés à distance en cas de perte.
- ☐ L'accès aux données est réservé aux appareils conformes, grâce à l'accès conditionnel (Microsoft Entra ID P1, inclus dans Microsoft 365 Business Premium).

5. Sauvegarde et reprise

- ☐ Une sauvegarde indépendante couvre les messageries, OneDrive, SharePoint et Teams.
- ☐ Une restauration est testée au moins deux fois par an.
- ☐ Un plan de réponse aux incidents précise qui fait quoi en cas de piratage ou de rançongiciel.

Bon à savoir : Microsoft garantit la disponibilité du service, mais la protection de vos données contre une suppression accidentelle, un départ de collaborateur ou un rançongiciel reste de votre responsabilité.

6. Utilisateurs et surveillance

- ☐ Les collaborateurs sont sensibilisés à l'hameçonnage, avec des simulations régulières.
 - ☐ Chacun sait comment signaler un message suspect, et le fait sans crainte.
 - ☐ Le journal d'audit est activé et les alertes de sécurité sont suivies.
 - ☐ Le Microsoft Secure Score est consulté chaque mois pour mesurer les progrès.
-

Par où commencer ?

Délai	Priorités
Cette semaine	MFA pour tous, comptes administrateurs dédiés, désactivation de l'authentification héritée.
Ce mois-ci	SPF, DKIM et DMARC, sauvegarde indépendante, limitation des partages anonymes.
Ce trimestre	Gestion des appareils avec Intune, accès conditionnel, programme de sensibilisation.

Parlons de votre projet

Besoin d'aide ? 7IT Cybersecurity réalise une revue de sécurité de votre environnement Microsoft 365 et vous remet un plan d'action clair, par ordre de priorité.

contact@7itgroup.com [WhatsApp +237 671 59 84 67](https://www.whatsapp.com/channel/0029va333333333333333333) www.7itgroup.com