Vytalx

Checklist de sécurité : Office 365

Réduire le risque de compromission, sécuriser les accès, renforcer la détection (30 minutes)

Vytalx

Comment utiliser cette checklist ?

Cochez chaque point selon votre situation.
L'objectif étant d'identifier rapidement les zones à risque
et de prioriser les actions urgentes.

Mode d'emploi

1. **Choisissez un périmètre :**
   commencez par vos services les plus critiques (ex: tenant + identités + messagerie + SharePoint/OneDrive/Teams).

2. **Cochez chaque point :**
   - ✅ Oui = mis en place et fonctionnel
   - ⚠️ Partiel = mis en place mais incomplet / pas fiable / pas systématique
   - ❌ Non = absent

3. **Notez une preuve (si possible) :**
   ex. capture, export, rapport, paramètre, log.

Exemple

"Tests de restauration mensuels"
- ✅ : test daté et documenté
- ⚠️ : test fait "de temps en temps"
- ❌ : aucun test effectué

Scoring simple

Barème
- ✅ = 2 points
- ⚠️ = 1 point
- ❌ = 0 point

Les 5 preuves attendues

1. MFA/Conditional Access (captures/politiques)
2. Export des logs d'audit / alertes
3. Paramètres anti-phishing/anti-spam (ou équivalent)
4. Revue des admins & rôles
5. Procédure de réponse incident (même simple)

Objectif : Passer d'un tenant "configuré" à une posture "vérifiable" : accès, protection des données, détection, preuves.

Vytalx

Périmètre de revue

**Avant de parcourir la checklist,
identifiez les zones qui concentrent le risque sur Microsoft 365 :
comptes à privilèges, accès externes, partages, et applications tierces.**

Votre périmètre

Identités & accès

☐ Comptes administrateurs (Global Admin, rôles clés)
☐ Comptes à privilèges “métiers/IT” (helpdesk, sécurité, échanges)
☐ Comptes “service” / automatisations
☐ Comptes invités (Guests / externes)

Messagerie

☐ Boîtes aux lettres utilisateurs
☐ Boîtes partagées
☐ Groupes / listes de distribution
☐ Règles de transfert / redirections externes

Collaboration & stockage

☐ SharePoint
☐ OneDrive
☐ Teams (équipes, canaux, apps)
☐ Partage externe (liens, invités)

Applications & terminaux

☐ Applications tierces (OAuth / consentements)
☐ Terminaux (BYOD, postes gérés/non gérés)
☐ Accès mobiles

Zone (Admins / Guests / Partage externe / Apps OAuth / Messagerie / Logs)	**Propriétaire** (qui gère ?)	**Politique en place ?**	**Dernière revue** (date / jamais)

Les 6 zones qui “font basculer” le risque

1. Comptes à privilèges : trop nombreux, mal protégés, non surveillés
2. Accès conditionnel & MFA : coverage incomplet, exceptions non maîtrisées
3. Authentification héritée : protocoles faibles encore autorisés (si applicable)
4. Partage externe : liens trop permissifs, invités non gouvernés
5. Applications tierces : consentements OAuth accordés sans contrôle
6. Règles de messagerie : transferts externes / règles suspectes non détectées

Vytalx

Checklist : Identités & accès

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
MFA activé pour tous les comptes à privilèges (admins, rôles sensibles)	☐	☐	☐	☐	
MFA largement déployé sur les utilisateurs (exceptions justifiées et tracées)	☐	☐	☐	☐	
Accès conditionnel en place (au minimum : MFA renforcé + blocage des accès à risque)	☐	☐	☐	☐	
Blocage / restriction des authentifications héritées (protocoles faibles, si applicable)	☐	☐	☐	☐	
Revue périodique des rôles administrateurs (moindre privilège, rôles temporaires si possible)	☐	☐	☐	☐	
Comptes “break-glass” définis et sécurisés (accès d’urgence, usage encadré)	☐	☐	☐	☐	
Réinitialisation en libre-service (SSPR) encadrée (méthodes, sécurité, supervision)	☐	☐	☐	☐	
Comptes “service” / automatisations identifiés et maîtrisés (usage, droits, rotation si pertinent)	☐	☐	☐	☐	
Invités (Guests) gouvernés (qui invite, approbation, expiration, revue)	☐	☐	☐	☐	
Consentement aux applications tierces maîtrisé (OAuth) : restrictions/approbations	☐	☐	☐	☐	
Inventaire des applications OAuth et revue des permissions (régulière)	☐	☐	☐	☐	
Politiques de session adaptées (durée, réauthentification, restrictions appareils non gérés)	☐	☐	☐	☐	
Détection/alertes sur connexions à risque (impossible travel, pays atypiques, etc.)	☐	☐	☐	☐	
Journalisation des actions admin activée et consultable.	☐	☐	☐	☐	

Priorité immédiate : Si MFA + accès conditionnel ne sont pas robustes sur les comptes à privilèges, le reste est secondaire.

Vytalx

Checklist : Messagerie, collaboration & données

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Protections anti-phishing/anti-spam configurées (niveau adapté, politiques appliquées)	☐	☐	☐	☐	
Protection des liens et pièces jointes activée (si disponible selon licences) ou alternative documentée	☐	☐	☐	☐	
DMARC/DKIM/SPF configurés pour les domaines (si périmètre mail concerné)	☐	☐	☐	☐	
Transferts automatiques vers l'externe maîtrisés (bloqués ou strictement contrôlés)	☐	☐	☐	☐	
Détection/revue des règles de boîte aux lettres (règles suspectes, redirections, suppressions)	☐	☐	☐	☐	
Boîtes partagées et comptes "service" sécurisés (accès, MFA si applicable, propriétaire)	☐	☐	☐	☐	
Partage externe OneDrive/SharePoint encadré (types de liens, durée, domaines, invités)	☐	☐	☐	☐	
Gouvernance Teams en place (création d'équipes, invités, apps, cycle de vie)	☐	☐	☐	☐	
Gestion du cycle de vie des contenus (rétention/archivage) définie pour les données critiques	☐	☐	☐	☐	
DLP / classification / étiquetage déployés (si applicable) ou plan défini	☐	☐	☐	☐	
Audit des activités M365 activé et conservé (accès, partages, actions admin)	☐	☐	☐	☐	
Processus de restauration/recouvrement des données défini (mail, fichiers, sites)	☐	☐	☐	☐	
La stratégie de sauvegarde M365 est clarifiée (ce qui est couvert, limites, preuves)	☐	☐	☐	☐	

Erreurs fréquentes :

- Redirections externes tolérées "au cas par cas" sans contrôle
- Partage externe trop permissif (liens "anyone", pas d'expiration)
- Audit activé mais sans exploitation ni conservation exploitable
- "Sauvegarde implicite" supposée, sans test ni preuve de restauration

Vytalx

Checklist : Détection & réponse

Point de contrôle	Oui ✅	Partielle ⚠️	Non ❌	N/A	Preuve ? (oui/non) rapport / capture / procédure / ticket / test daté
Les alertes de sécurité sont activées et routées vers les bonnes personnes (astreinte si besoin)	☐	☐	☐	☐	
Un seuil de traitement est défini (ex. critique < 1h, élevé < 4h)	☐	☐	☐	☐	
Surveillance des connexions à risque (pays atypiques, impossible travel, risques élevés)	☐	☐	☐	☐	
Surveillance des actions sensibles (création d'admins, changements de politiques, consentement d'apps)	☐	☐	☐	☐	
Détection des règles de boîte suspectes (transferts externes, suppressions)	☐	☐	☐	☐	
Détection des consentements OAuth et apps à risque (nouveaux consentements, permissions élevées)	☐	☐	☐	☐	
Un runbook "compte compromis" existe (révocation sessions, reset, MFA, nettoyage règles)	☐	☐	☐	☐	
Un runbook "phishing" existe (analyse, purge, recherche, communication interne).	☐	☐	☐	☐	
Conservation et export des preuves (logs/audit) pour analyse et reporting	☐	☐	☐	☐	
Capacité de recherche/audit : vous savez répondre à "qui a fait quoi, quand"	☐	☐	☐	☐	
Revue périodique sécurité du tenant (mensuelle/trimestrielle)	☐	☐	☐	☐	
Exercice de gestion d'incident (tabletop ou simulation légère) au moins 1×/an	☐	☐	☐	☐	
Intégration avec un dispositif de détection plus large (XDR/SIEM/SOC si existant)	☐	☐	☐	☐	

La configuration ne suffit pas : la différence se fait sur la capacité à détecter vite, agir, et conserver des preuves.

Vytalx

Synthèse & plan d'action

Votre résultat

Score total : ____ / ____

Niveau : ☐ Risque élevé (0%-49%) ☐ À consolider (50%-74%) ☐ Structuré (75%-100%)

Barème :	Calcul :
✅ Oui = 2 pts ⚠️ Partiel = 1 pt ❌ Non = 0 pt	**Score obtenu** = somme des points **Score Max** = 2 × (nb de lignes évaluées)

Zones rouges

Vos 5 écarts prioritaires :

_____

_____

_____

_____

_____

Points bloquants

☐ MFA non généralisé sur les comptes à privilèges
☐ Absence d'accès conditionnel (ou règles trop faibles / trop d'exceptions)
☐ Transferts externes non maîtrisés (ou règles de boîte non surveillées)
☐ Partage externe trop permissif (sans gouvernance)
☐ Alertes / logs non exploitables (pas de routage, pas de runbook)

Plan d'action

Phase 1 : Verrouiller les identités

- Déployer MFA en priorité sur les comptes à privilèges (+ revue des rôles admin)
- Mettre en place / renforcer l'accès conditionnel (accès à risque, appareils non gérés, pays)
- Réduire les exceptions et sécuriser les comptes d'urgence (break-glass)

Phase 2 : Réduire l'exposition messagerie

- Durcir les politiques anti-phishing/anti-spam
- Encadrer / bloquer les transferts externes
- Mettre en place une revue des règles de boîte (détection règles suspectes)

Phase 3 : Encadrer la donnée & les partages

- Revoir les paramètres de partage OneDrive/SharePoint (liens, expiration, domaines)
- Mettre à plat la gouvernance Teams (invités, création, apps)
- Clarifier la stratégie de restauration (ce qui est couvert + comment prouver)

Phase 4 : Industrialisation

- Mettre en place un routage des alertes + un seuil de traitement
- Rédiger 2 runbooks : compte compromis + phishing
- Organiser une revue trimestrielle tenant sécurité (rituel + preuves)

contact/vytalx.fr contact@vytalx.fr