

Boîte mail piratée : reprendre le contrôle, réparer les dégâts

La messagerie est la clé de tout le reste. Détecter l'intrusion, expulser l'intrus, et couper les portes dérobées qu'il a laissées.

8 min de lecture · Niveau Essentiel · cyberionis.fr/ressources/boite-mail-piratee

La boîte mail est le compte maître : elle réinitialise tous les autres, connaît vos contacts, vos factures, vos habitudes. C'est pourquoi sa compromission est à la fois si courante et si grave — et pourquoi l'attaquant qui y entre s'installe discrètement plutôt que de tout casser : il lit, il attend, il prépare une fraude au virement ou une usurpation. Détecter, expulser, et surtout fermer les portes dérobées : le protocole complet.

1. Les signes d'une boîte compromise

- Des messages envoyés que vous n'avez pas écrits (vérifiez aussi les éléments envoyés... et supprimés)
- Des contacts qui reçoivent « de vous » des demandes étranges
- Des connexions inconnues dans l'historique du compte (lieu, appareil, heure — toutes les messageries l'affichent)
- Des emails qui « disparaissent » ou marqués lus sans vous : le signe de règles de tri pirates
- Une alerte de connexion ou un changement de paramètres que vous n'avez pas fait
- Parfois rien : l'attaquant en mode lecture pure est invisible — d'où l'intérêt des vérifications périodiques

2. Reprendre le contrôle (dans cet ordre)

- Depuis un appareil sûr : changer le mot de passe — long, unique, générés par le gestionnaire
- Déconnecter TOUTES les sessions actives (option « se déconnecter partout ») : le changement de mot de passe seul ne chasse pas les sessions ouvertes
- Activer ou vérifier la MFA — et vérifier que l'attaquant n'a pas enregistré SON appareil ou SON numéro comme second facteur
- Vérifier les informations de récupération : email et téléphone de secours détournés = porte de retour garantie
- En entreprise : l'administrateur Microsoft 365/Workspace fait tout cela centralement, et vérifie les journaux d'accès

3. Chasser les portes dérobées — l'étape que tout le monde oublie

- Les règles de boîte pirates : transferts automatiques vers l'extérieur, suppression des alertes, déplacements discrets — LE grand classique, à purger règle par règle
- Les délégations et partages accordés : qui peut lire ou envoyer « en votre nom » ?
- Les applications tierces autorisées : révoquer tout accès inconnu ou inutile (consent phishing)

- Les appareils connectés au compte : supprimer les inconnus
- La signature et les réponses automatiques : parfois modifiées pour porter des liens piégés

ATTENTION

L'attaquant expulsé par le nouveau mot de passe revient par la règle de transfert qu'il a laissée : chaque email continue de lui parvenir en silence, y compris vos réinitialisations de mots de passe. Après TOUT piratage de boîte, l'inspection des règles, délégations et applications autorisées n'est pas optionnelle — c'est là que se joue la vraie éviction.

4. Réparer et prévenir la suite

- Évaluer ce qui a été lu/pris : la boîte contient RIB, contrats, données clients — selon le cas, la notification RGPD s'impose
- Prévenir contacts et collègues si des messages frauduleux sont partis : votre alerte tue la fraude en cours
- Chercher la porte d'entrée : phishing, mot de passe réutilisé fuité, poste infecté — et la traiter
- Changer les mots de passe des comptes rattachés à cette adresse (l'attaquant a pu les réinitialiser)
- Tirer la leçon d'équipe : MFA généralisée, alertes de connexion activées, et la vérification trimestrielle des règles de boîte au rituel du référent

L'essentiel à retenir

- 01 Changer le mot de passe ET déconnecter toutes les sessions
- 02 Vérifier MFA et informations de récupération (numéros, emails)
- 03 Purger règles de transfert, délégations et applications tierces
- 04 Évaluer les données exposées et notifier si nécessaire
- 05 Prévenir les contacts si des messages frauduleux sont partis
- 06 Identifier et corriger la porte d'entrée

Questions fréquentes

J'ai la MFA : ma boîte est-elle impirable ?

Presque — mais pas tout à fait : le phishing en temps réel qui relaie le code, la fatigue MFA, et surtout le vol de cookies de session par infostealer contournent le second facteur. La MFA élimine l'écrasante majorité des attaques ; les clés physiques (FIDO2) et l'hygiène du poste ferment le reste. Et les vérifications périodiques de connexions et de règles restent pertinentes, MFA ou pas.

L'attaquant a changé le mot de passe et je suis dehors. Comment récupérer ?

Via les procédures de récupération du fournisseur : informations de secours si elles vous restent, formulaires de récupération (préparez preuves d'identité et éléments d'historique). En entreprise, l'administrateur reprend le compte en minutes — un argument de plus pour la messagerie professionnelle administrée plutôt que les comptes gratuits isolés (voir notre guide). Agissez vite : l'attaquant utilise ce temps pour verrouiller davantage.

Compromission d'une boîte : faut-il le dire aux clients ?

Si des messages frauduleux leur sont partis ou peuvent partir : oui, vite et sobrement — votre transparence les protège et préserve la confiance (voir notre guide usurpation). Si l'analyse montre une intrusion en lecture sur des échanges contenant leurs données personnelles, l'évaluation RGPD (notification CNIL/ personnes) s'impose. Le silence espéré coûte toujours plus cher que l'information maîtrisée.

Pour aller plus loin

Cybermalveillance.gouv.fr — piratage de compte — www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/piratage-compte

CNIL — notifier une violation de données — www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

Un doute, une urgence, un incident ?

Cyberionis évalue votre exposition, prépare vos défenses et vous épaula pour réagir vite en cas d'attaque.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr