



Comment survivre à un compte piraté

Quelqu'un s'est connecté à votre compte à votre place : boîte mail, espace client, plateforme de travail. **Commencez par votre adresse e-mail** — c'est elle qui permet de réinitialiser tous vos autres comptes. Tant qu'elle est compromise, le reste l'est aussi.



Dans l'heure qui suit

URGENCE

- 1 Utilisez un autre appareil, sain.**
Si l'appareil habituel est infecté, tout nouveau mot de passe saisi dessus sera capté à son tour.
- 2 Changez le mot de passe.**
Un mot de passe long, unique, qui ne ressemble pas au précédent. Si l'accès vous est refusé, lancez la procédure « mot de passe oublié ».
- 3 Déconnectez toutes les sessions ouvertes.**
Dans les paramètres de sécurité du service : « appareils connectés » ou « sessions actives ». Sans cela, l'attaquant reste connecté malgré le changement de mot de passe.
- 4 Activez l'authentification multifacteur.**
C'est ce qui empêchera une nouvelle intrusion, même si le mot de passe fuit à nouveau.
- 5 Vérifiez les paramètres détournés.**
Adresse e-mail et numéro de secours, question de sécurité, règles de transfert automatique des messages, applications tierces autorisées, signature. Un attaquant modifie ces réglages pour garder un accès après votre reprise en main.
- 6 Prévenez vos contacts.**
Dites-leur d'ignorer tout message reçu de votre part récemment, en particulier les demandes d'argent ou les liens.



- **Changez le mot de passe partout où vous l'aviez réutilisé.** C'est le point le plus souvent négligé : les attaquants testent le couple identifiant / mot de passe volé sur des dizaines d'autres services.
- **Vérifiez les comptes liés** — tous ceux où vous vous connectez « avec Google », « avec Facebook » ou « avec Apple » via le compte compromis.
- **Relisez vos messages envoyés et votre corbeille** pour mesurer ce qui a été consulté ou expédié en votre nom.
- **Surveillez vos relevés bancaires** pendant au moins un mois si le compte contenait des informations de paiement.
- **Analysez l'appareil habituel** avec un antivirus à jour : le vol de mot de passe vient parfois d'un logiciel espion installé localement.
- **Conservez les traces** (captures d'écran, e-mails d'alerte de connexion) si vous envisagez un signalement.



À ne pas faire

- ✗ Reprendre l'ancien mot de passe avec une simple variante (un chiffre en plus, une majuscule).
- ✗ Cliquer sur les liens des e-mails « alerte de sécurité » reçus juste après l'incident : les attaquants profitent du moment de panique pour envoyer un second hameçonnage.
- ✗ Attendre de voir « si ça se calme ». Chaque heure d'accès supplémentaire élargit la compromission aux comptes liés.
- ✗ Changer le mot de passe depuis l'appareil suspect avant de l'avoir analysé.



Pour éviter que cela recommence

- **Un mot de passe différent par compte**, mémorisé par un gestionnaire de mots de passe plutôt que par vous.
- **L'authentification multifacteur sur la messagerie en priorité**, puis sur les comptes bancaires et les réseaux sociaux.
- **Une revue trimestrielle** des appareils connectés et des applications autorisées sur vos comptes principaux.
- **Une adresse de secours à jour**, sur un service différent de votre adresse principale.