



# Comment survivre à un compte de réseau social piraté

Des publications que vous n'avez pas faites, des messages envoyés à vos contacts, un mot de passe qui ne fonctionne plus. Sur les réseaux sociaux, **tout se joue sur l'adresse e-mail associée au compte** : c'est la première chose qu'un attaquant modifie, et souvent la seule qui permette de tout récupérer.



## Dans l'heure qui suit

URGENCE

### 1 Ouvrez d'abord votre boîte mail.

Cherchez le message « votre adresse e-mail a été modifiée ». Il contient presque toujours un lien « ce n'était pas moi » qui annule le changement — il n'est valable que quelques jours.

### 2 Changez le mot de passe.

Si vous avez encore accès au compte, faites-le depuis un appareil sain.

### 3 Si vous êtes exclu, utilisez le parcours « compte piraté ».

Pas le simple « mot de passe oublié » : chaque réseau a un formulaire dédié, qui peut demander une pièce d'identité ou une courte vidéo de vérification. Répondez avec précision : date de création, anciens mots de passe, appareils utilisés.

### 4 Déconnectez toutes les sessions actives.

Révoquez également les applications tierces connectées au compte.

### 5 Activez l'authentification multifacteur.

De préférence par application d'authentification plutôt que par SMS.

### 6 Prévenez publiquement vos contacts.

Depuis un autre réseau ou un autre compte : « mon compte est piraté, ne répondez à aucune demande d'argent ni à aucun lien envoyé de ma part ».



- **Supprimez les publications, stories et commentaires** diffusés en votre nom, puis vérifiez la liste de vos abonnements : les attaquants en ajoutent pour monétiser le compte.
- **Vérifiez les moyens de paiement et les campagnes publicitaires** si le compte est professionnel ou lié à une page — c'est le motif le plus fréquent de piratage de comptes suivis.
- **Signalez à la plateforme les messages frauduleux** envoyés à vos contacts, et demandez à ceux qui les ont reçus de les signaler également : cela accélère le traitement.
- **Changez le mot de passe partout où vous l'aviez réutilisé**, en commençant par votre messagerie.
- **Vérifiez les administrateurs** des pages et groupes que vous gérez : un compte ajouté à votre insu garde la main même après votre reprise en main.



### À ne pas faire

- ✗ Payer un « service de récupération de compte » proposé en commentaire ou en message privé. Ce sont des arnaques sans exception : personne ne peut débloquent un compte à la place de la plateforme.
- ✗ Créer immédiatement un compte de remplacement : cela complique la vérification d'identité et sème la confusion chez vos contacts.
- ✗ Négocier avec l'attaquant ou répondre à ses messages.
- ✗ Communiquer un code de vérification reçu par SMS, même à quelqu'un qui se présente comme le support de la plateforme.



### Pour éviter que cela recommence

- **Authentification multifacteur par application** sur chaque réseau, et codes de secours conservés hors ligne.
- **Une adresse e-mail dédiée** à vos réseaux sociaux, elle-même protégée par un facteur d'authentification.
- **Un tri régulier des applications connectées** : les jeux, filtres et outils de statistiques autorisés il y a des années restent des portes d'entrée.
- **De la méfiance envers les messages de « partenariat »** et les liens envoyés par des comptes amis : c'est le principal vecteur de propagation.