Fiche Pratique N°69 : Récupérez un compte piraté V1.0

11 nov, 2026 · @Gabriel

Objectif : *reprendre la main sur un compte de messagerie, de réseau social ou de boutique en ligne dont quelqu'un s'est emparé, limiter les dégâts autour de vous, puis le protéger pour que cela ne se reproduise pas.*

- ***Public visé :*** *débutant*
- ***Temps estimé :*** *1 heure pour les premiers gestes ; parfois plusieurs jours si le service doit vérifier votre identité*
- ***Difficulté :*** ★★☆☆☆ *(Facile)*
- ***Prérequis :*** *un appareil sain (de préférence celui que vous utilisez d'habitude pour ce compte), l'accès à votre téléphone et à votre adresse de secours si vous en avez une*
- ***Fiches associées :*** *N°16 (mots de passe), N°18 (double authentification), N°47 (reconnaître et déjouer les arnaques en ligne), N°58 (réagir à une fuite de données), N°65 (clés d'accès), N°56 (alias de courriel), N°70 (sécuriser ses démarches en ligne)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : quelqu'un d'autre a les clés

Un compte piraté se reconnaît vite : votre mot de passe ne marche plus, vos amis reçoivent des messages que vous n'avez pas écrits, une commande apparaît que vous n'avez pas passée, ou le service vous écrit qu'une « nouvelle connexion » ou un « changement d'adresse » a eu lieu. Le plus souvent, le pirate a obtenu le mot de passe par un faux message (hameçonnage), par une fuite de données d'un autre site où vous utilisiez le même mot de passe, ou par un logiciel malveillant.

Situation	Conséquence
Le pirate est dans votre messagerie	Il peut réinitialiser les mots de passe de tous vos autres comptes
Il est dans votre compte Facebook, Instagram ou WhatsApp	Il écrit à vos proches en votre nom pour leur soutirer de l'argent
Il est dans un compte de boutique ou de paiement	Il passe des commandes avec votre carte enregistrée
Il a changé l'adresse et le téléphone de secours	Vous ne recevez plus les codes de récupération
Vous attendez	Chaque heure lui laisse le temps de verrouiller le compte davantage

Une image pour comprendre : on vous a volé les clés de la maison. Il faut d'abord récupérer le trousseau (le compte), puis changer les serrures (mot de passe et double authentification), vérifier qu'aucun double n'a été fait (sessions, appareils, transferts automatiques) et prévenir les voisins (vos contacts).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°69 : Récupérez un compte piraté V1.0

Le risque : perdre définitivement vos courriels, vos photos et vos contacts, voir vos proches escroqués en votre nom, ou subir des achats frauduleux.

Le bénéfice : dans la plupart des cas, un compte se récupère si l'on agit vite et dans le bon ordre. Et la double authentification empêche presque toujours que cela recommence.

2. Comprendre l'ordre des gestes

L'ordre compte. Le dispositif national Cybermalveillance.gouv.fr recommande cette suite :

Ordre	Geste	Pourquoi
1	Vérifier que votre appareil est sain	Sinon, le pirate lira aussi votre nouveau mot de passe
2	Récupérer le compte par la procédure officielle du service	Seul le service peut vous rendre l'accès
3	Changer le mot de passe et activer la double authentification	Le pirate ne peut plus revenir avec l'ancien
4	Vérifier les réglages de récupération et les appareils connectés	Le pirate a pu laisser une « porte de derrière »
5	Changer le mot de passe des autres comptes qui l'utilisaient	Il essaiera le même mot de passe ailleurs
6	Prévenir vos contacts	Ils ne répondent pas aux demandes d'argent
7	Vérifier commandes, publications et banque	Annuler, signaler, faire opposition
8	Garder les preuves et porter plainte	Indispensable en cas d'escroquerie ou de chantage

⚠️ **N'utilisez jamais un lien reçu par message pour « récupérer votre compte »** : les faux services de récupération sont une arnaque courante. Tapez vous-même l'adresse du service, ou passez par son application officielle. Personne ne vous demandera de payer pour récupérer un compte Google, Meta ou Microsoft.

Avant de commencer

- ☐ Je fais une capture d'écran de tout ce qui prouve le piratage (messages envoyés en votre nom, courriels d'alerte, commandes)
- ☐ J'utilise un appareil que j'utilise d'habitude pour ce compte : le service le reconnaît, ce qui facilite la récupération
- ☐ J'ai fait une analyse antivirus complète de cet appareil (Microsoft Defender sous Windows), ou j'utilise un autre appareil sain
- ☐ J'ai mon téléphone sous la main et l'accès à mon adresse de secours, si j'en ai une

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°69 : Récupérez un compte piraté V1.0

- ☐ Je ne supprime pas les cookies et je ne me déconnecte pas si une session est encore ouverte quelque part
- ☐ Je cherche dans ma messagerie le courriel du service annonçant le changement (mot de passe, adresse, téléphone) : il contient souvent un lien pour annuler

3. Pas à pas : reprendre le compte

1. **Si vous êtes encore connecté quelque part** (sur votre téléphone, par exemple), changez tout de suite le mot de passe depuis cette session, puis passez à l'étape 4.
    - Vous devez voir : un message confirmant le changement et, souvent, la déconnexion des autres appareils.
2. **Si vous avez reçu un courriel du service** signalant un changement que vous n'avez pas fait, utilisez le lien qu'il contient pour annuler la modification, après avoir vérifié que l'expéditeur est bien le service (adresse de l'expéditeur, aucune faute, aucune urgence inventée).
    - Vous devez voir : une page du vrai site (adresse exacte dans la barre du navigateur) qui vous propose de sécuriser le compte.
3. **Sinon, lancez la procédure officielle de récupération** en tapant vous-même l'adresse :
    - Google (Gmail, YouTube) : `g.co/recover`, ou le lien **Mot de passe oublié ?** sur la page de connexion.
    - Facebook : `facebook.com/hacked` ; Instagram : `instagram.com/hacked`.
    - Microsoft (Outlook, Hotmail, Windows) : le lien **Mot de passe oublié ?** sur la page de connexion, puis l'**assistant de connexion** du support Microsoft.
    - Proton : le lien **Mot de passe oublié ?** sur `account.proton.me`.
    - Vous devez voir : le service vous demande un code envoyé à votre téléphone ou à votre adresse de secours, ou vous pose des questions sur le compte.
4. **Répondez aux questions de vérification** le plus précisément possible : ancien mot de passe, date approximative de création du compte, contacts fréquents. Si vous ne savez pas, donnez votre meilleure estimation plutôt que de passer.
    - Vous devez voir : un nouveau mot de passe demandé, ou l'annonce d'une vérification qui prendra du temps.
5. **Si le pirate a changé l'adresse et le téléphone de secours**, le service propose une vérification d'identité. Chez Meta, il peut s'agir d'un **selfie vidéo** (proposé à certains comptes seulement) ou d'une photo de pièce d'identité, toujours **dans le parcours officiel**, jamais par message privé.
    - Vous devez voir : un délai annoncé. Patientez et ne multipliez pas les demandes, cela ralentit le traitement.
6. **Choisissez un mot de passe neuf**, long et jamais utilisé ailleurs, de préférence généré par votre gestionnaire de mots de passe (fiche N°16).
    - Vous devez voir : vous êtes de nouveau connecté à votre compte.

4. Fermer toutes les portes laissées par le pirate

Une fois le compte repris, le pirate a pu laisser des moyens de revenir. Vérifiez dans cet ordre :

1. **Déconnectez tous les autres appareils.** Google : **Sécurité** › **Vos appareils**. Facebook et Instagram : **Espace comptes** › **Mot de passe et sécurité** › **Où vous êtes connecté(e)**.

gabriel.ananda@mailo.com
CC BY SA

   - Vous devez voir : seul l'appareil que vous tenez reste connecté.
2. **Vérifiez l'adresse et le téléphone de récupération.** Supprimez ceux que vous ne reconnaissez pas, remettez les vôtres.
   - Vous devez voir : uniquement vos coordonnées.
3. **Activez la double authentification** (fiche N°18), de préférence par une application ou une clé de sécurité plutôt que par SMS.
   - Vous devez voir : la double authentification indiquée comme activée.
4. **Dans une messagerie, vérifiez les transferts et les filtres.** Un pirate ajoute souvent un transfert automatique vers son adresse, ou un filtre qui supprime les alertes de votre banque. Gmail : **Paramètres** › **Voir tous les paramètres** › onglets **Comptes et importation** (délégation), **Filtres et adresses bloquées** et **Transfert et POP/IMAP**. Outlook : règles, transferts et réponses automatiques.
   - Vous devez voir : aucun transfert, aucun filtre ni délégué que vous n'avez pas créé.
5. **Retirez les applications tierces inconnues** qui ont accès au compte (Google : **Sécurité** › **Vos connexions à des applications et services tiers**).
   - Vous devez voir : uniquement les applications que vous utilisez.
6. **Examinez l'activité récente** : courriels envoyés, publications, messages privés, commandes, modes de paiement ajoutés. Google propose **Sécurité** › **Activité récente liée à la sécurité** : si une action ne vient pas de vous, cliquez sur **Non, sécuriser mon compte**.
   - Vous devez voir : la liste de ce que le pirate a fait, à garder en capture d'écran.

5. Limiter les dégâts autour de vous

- **Prévenez vos contacts** par un autre canal (SMS, appel, message depuis un autre compte) : « Mon compte a été piraté, ne répondez à aucune demande d'argent venant de moi. »
- **Changez le mot de passe de tous les comptes** qui utilisaient le même, en commençant par la messagerie et la banque.
- **Si une carte bancaire était enregistrée** ou si des achats ont eu lieu : appelez votre banque et faites opposition (numéro au dos de la carte), puis contestez les opérations.
- **Si le pirate vous fait chanter** (photos, données) : ne payez pas, ne répondez pas, gardez les preuves.
- **Faites-vous aider** : la plateforme **17Cyber** (`17cyber.gouv.fr`) établit un diagnostic en ligne, à toute heure, donne les bons gestes et, si l'atteinte est grave, vous met en relation par tchat avec un policier ou un gendarme.
- **Portez plainte** au commissariat, à la gendarmerie ou par écrit au procureur de la République, avec vos captures d'écran, dès qu'il y a escroquerie, usurpation d'identité ou chantage.

6. À quoi s'attendre et dépannage

Symptôme	Cause possible	Action
Le code de récupération arrive sur un numéro que vous ne connaissez pas	Le pirate a remplacé votre téléphone de secours	Choisissez l'option « Je n'ai plus accès » et suivez la vérification d'identité

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°69 : Récupérez un compte piraté V1.0

Symptôme	Cause possible	Action
Google dit qu'il ne peut pas vérifier que le compte vous appartient	Trop peu d'informations ou appareil inconnu	Réessayez depuis un appareil et un lieu habituels, en répondant au plus grand nombre de questions
Le compte Google a été supprimé par le pirate	Suppression récente	Lancez la récupération au plus vite : un compte supprimé n'est récupérable que pendant un temps limité
Facebook ne propose pas le selfie vidéo	L'option n'est pas offerte à tous les comptes	Utilisez la pièce d'identité dans le parcours officiel
Proton vous oblige à changer de mot de passe	Proton a détecté une connexion suspecte et verrouillé le compte	Saisissez l'ancien mot de passe, puis le nouveau deux fois : les autres sessions sont fermées
Le pirate revient quelques jours plus tard	Une porte est restée ouverte (transfert, appli tierce, appareil infecté)	Reprenez la section 4 et analysez vos appareils
Quelqu'un vous propose de récupérer le compte contre paiement	C'est une arnaque	Ne payez rien, signalez le profil

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

7. Se préparer avant que cela arrive

La récupération est d'autant plus simple que le compte a été bien préparé.

Précaution	Où la régler	Pourquoi
Adresse et téléphone de secours à jour	Réglages de sécurité de chaque service	C'est par là que passe la récupération
Double authentification par application ou clé	Fiche N°18	Un mot de passe volé ne suffit plus
Codes de secours imprimés	Réglages de la double authentification	Récupérer l'accès sans téléphone
Phrase de récupération (Proton)	Paramètres › Récupération	Sans elle, les courriels chiffrés peuvent être perdus après une réinitialisation
Un mot de passe différent par compte	Gestionnaire de mots de passe (fiche N°16)	Une fuite ne touche qu'un seul compte

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°69 : Récupérez un compte piraté V1.0

Précaution	Où la régler	Pourquoi
Clé d'accès (passkey)	Fiche N°65	Un moyen de plus de prouver que c'est vous

8. Cas particuliers

- **WhatsApp volé par un code SMS** : réinstallez WhatsApp avec votre numéro et saisissez le code reçu par SMS ; le pirate est déconnecté. Activez ensuite la **validation en deux étapes** (code PIN) dans **Paramètres** › **Compte**.
- **Compte de messagerie professionnelle ou associative** : prévenez tout de suite l'administrateur ; il peut couper les sessions et vérifier les règles de transfert.
- **Votre adresse figure dans une fuite** : vérifiez sur Have I Been Pwned (fiche N°58) quels sites sont concernés et changez ces mots de passe en priorité.
- **Plusieurs comptes piratés en même temps** : l'appareil lui-même est probablement infecté. Sauvegardez vos fichiers personnels, réinstallez le système, puis changez les mots de passe depuis un appareil sain.

À savoir avant de se lancer

Crainte fréquente	La réalité
« C'est fichu, je ne le récupérerai jamais. »	La plupart des comptes se récupèrent par la procédure officielle, surtout si l'on agit vite.
« Il faut payer quelqu'un pour le récupérer. »	Non : les procédures officielles sont gratuites. Les « récupérateurs » payants sont des escrocs.
« J'ai été naïf, j'ai honte. »	Les arnaques sont conçues par des professionnels. Prévenir vos proches les protège.
« Porter plainte ne sert à rien. »	La plainte est souvent exigée par la banque pour rembourser, et elle aide les enquêteurs.
« La double authentification, c'est compliqué. »	Cinq minutes de réglage, puis un code de temps en temps : c'est la meilleure protection.

Challenge 7 jours

- **Jour 1 :** récupérez le compte et changez son mot de passe.
- **Jour 2 :** fermez les portes : appareils, transferts, applications tierces, adresse et téléphone de secours.
- **Jour 3 :** activez la double authentification sur ce compte et sur votre messagerie principale.
- **Jour 4 :** changez le mot de passe de tous les comptes qui utilisaient le même.
- **Jour 5 :** imprimez les codes de secours et rangez-les avec vos papiers importants.
- **Jour 6 :** vérifiez votre adresse sur Have I Been Pwned.

gabriel.ananda@mailo.com
CC BY SA

- **Jour 7 :** expliquez à un proche comment reconnaître un faux message de récupération.

Vous allez constater : le compte est de nouveau à vous, il est mieux protégé qu'avant, et vous savez exactement quoi faire si cela recommence.

En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Récupérer le compte par la voie officielle	Vos données et vos contacts	Section 3
Fermer les portes laissées par le pirate	Il ne revient pas	Section 4
Prévenir vos contacts et votre banque	Personne d'autre n'est escroqué	Section 5
Double authentification et mots de passe uniques	Le prochain vol de mot de passe ne suffira pas	Fiches N°16 et N°18

À retenir absolument

- Tapez vous-même l'adresse de récupération du service : jamais un lien reçu par message.
- Après la récupération, fermez toutes les portes : appareils, transferts, applications, coordonnées de secours.
- Prévenez vos contacts par un autre canal et gardez les preuves.
- La double authentification et un mot de passe unique par compte évitent presque toujours la rechute.

Test final :

1. Je suis de nouveau connecté et le mot de passe a été changé.
2. Aucun appareil, transfert ou application inconnu n'a accès au compte.
3. La double authentification est activée et mes codes de secours sont imprimés.
4. Mes contacts sont prévenus et ma banque aussi si une carte était enregistrée.
5. Je sais où trouver 17Cyber et comment porter plainte. ✅

Références

- Cybermalveillance.gouv.fr – Fiche réflexe : piratage de compte (PDF)
- Google – Sécuriser un compte Google piraté ou compromis
- Microsoft – Procédure de récupération d'un compte Microsoft piraté ou compromis
- Microsoft – Protéger votre compte de messagerie Outlook.com
- Proton – Proton a verrouillé temporairement mon compte pour des raisons de sécurité
- Proton – La récupération du compte Proton expliquée
- Lebigdata – Facebook piraté sans e-mail ni téléphone : les démarches pour récupérer votre compte (5 novembre 2026)
- IT-Connect – La France lance 17Cyber, sa nouvelle plateforme pour aider les victimes de cyberattaque (18 décembre 2024)

gabriel.ananda@mailo.com
CC BY SA