Famille : Réagir correctement

Fiche 16 — Que faire si un compte a été piraté

Réagir vite pour reprendre le contrôle et limiter les dégâts

1 Pourquoi cette fiche est utile

- Un compte piraté peut servir à voler des données, contacter vos proches ou lancer d’autres attaques.
- Une réaction rapide limite les dégâts.
- La messagerie est souvent le premier compte à sécuriser.
- Chaque minute compte lorsque l’accès a été compromis.

2 Ce qu’il faut savoir

- Les signes possibles sont des connexions inhabituelles, des messages envoyés à votre insu ou des informations modifiées.
- Les paramètres de récupération du compte sont essentiels.
- La messagerie principale et les comptes liés doivent être vérifiés.
- Il faut agir dans un ordre logique pour éviter d’aggraver la situation.

3 Signaux d’alerte

- Connexion non reconnue.
- Message ou publication envoyée à votre insu.
- Mot de passe qui ne fonctionne plus.
- Adresse de récupération ou numéro de téléphone modifié sans votre accord.

4 Erreurs à éviter

- Attendre en espérant que le problème disparaisse.
- Ne traiter qu’un seul compte alors que plusieurs sont liés.
- Oublier la messagerie principale.
- Ne pas prévenir les contacts qui auraient pu recevoir des messages frauduleux.

Bon réflexe : La priorité est de reprendre le contrôle de la messagerie principale et de sécuriser les accès liés.

Fiche 16 —

Que faire si un compte a été piraté

Les bons gestes à appliquer

1 Les bons réflexes immédiats

- Changez immédiatement le mot de passe si l’accès est encore possible.
- Déconnectez les appareils inconnus ou les sessions ouvertes.
- Activez la double authentification.
- Vérifiez les adresses de récupération, redirections et paramètres de sécurité.
- Traitez ensuite les autres comptes liés au compte compromis.

2 Si l’erreur a déjà été commise

- Lancez la procédure officielle de récupération si vous ne pouvez plus entrer.
- Prévenez vos contacts si des messages frauduleux ont pu partir.
- Contrôlez vos moyens de paiement si le compte est lié à des achats.
- Conservez les preuves utiles de la compromission.
- Signalez l’incident au service concerné si nécessaire.

3 Mémo express

- Messagerie d’abord.
- Changer, vérifier, sécuriser.
- Informer rapidement les personnes exposées.

4 Pour aller plus loin

- cybermalveillance.gouv.fr
- service-public.fr
- cnil.fr
- anssi.gouv.fr