

Réflexes en cas de compromission

LANGUE Français

AUDIENCE Tous les utilisateurs

Ce qu'il faut repérer et ce qu'il faut faire, dans l'ordre, si vous pensez que votre compte Gesti'up a été utilisé par quelqu'un d'autre.

01 Comment reconnaître une activité suspecte sur son compte ?

Plusieurs éléments peuvent indiquer une activité inhabituelle.

Impossibilité de se connecter

Changement de mot de passe non autorisé

Actions réalisées sans votre intervention

Connexions inconnues

E-mails inhabituels

Données modifiées ou supprimées

Comportement anormal de l'application

02 Que faire immédiatement en cas de suspicion de piratage ?

Les premiers réflexes recommandés, dans cet ordre. Si vous ne pouvez plus vous connecter, voyez la section 03. Le détail des gestes figure dans les documentations « Réinitialiser ou modifier son mot de passe » et « Utiliser la double authentification ».

- 1 **Modifiez immédiatement le mot de passe** du compte, depuis Paramètres → Mon compte → Sécurité.
- 2 **Vérifiez les informations du compte** et les dernières actions effectuées.
- 3 **Prévenez rapidement Gesti'up** : écrivez à securite@gestiup.fr, ou contactez le support via la bulle d'aide.
- 4 **Activez la double authentification (2FA)**, si elle n'est pas déjà activée.

03 Que faire si je ne peux plus me connecter ?

La marche à suivre dépend de votre situation.

SITUATION	QUE FAIRE
Vous avez accès à votre adresse e-mail de connexion	Réinitialisez votre mot de passe avec « Mot de passe oublié ? », sur la page de connexion. Cela vaut pour un utilisateur comme pour un administrateur.
Votre adresse e-mail n'est plus valide, et vous êtes utilisateur	Demandez à un administrateur de votre compte de modifier votre adresse e-mail.
Votre adresse e-mail n'est plus valide, et vous êtes l'administrateur	Contactez le support via la bulle d'aide, accessible depuis la page de connexion, ou par e-mail à support@gestiup.fr , avec une preuve d'identité au nom du compte utilisateur.



Besoin d'aide ?

Bulle d'aide · FAQ · Ticket support · Vidéos tutorielles

04 Que faire si des données semblent avoir été modifiées ?

Selon la situation, une restauration ou des mesures correctives peuvent être mises en œuvre.

- 1 Vérifiez les modifications effectuées.
- 2 Identifiez les éléments concernés.
- 3 Contactez rapidement Gesti'up : securite@gestiup.fr, ou le support via la bulle d'aide.
- 4 Documentez les actions suspectes observées.

05 Les accès suspects sont-ils surveillés ?

Oui. Des mécanismes de sécurité et de surveillance détectent les comportements anormaux, limitent les accès non autorisés et protègent les comptes utilisateurs.

- **Limitation des connexions simultanées** sur un même compte.
- **Surveillance du trafic**, pour repérer les comportements anormaux.
- **Journalisation** de certains événements de sécurité.
- **Double authentification (2FA)**, que l'administrateur peut rendre obligatoire pour tous les utilisateurs.
- **Exigences de sécurité du mot de passe** : longueur minimale, majuscule, minuscule, chiffre et caractère spécial.
- **Lien de réinitialisation** du mot de passe valable 24 heures.
- **Traçabilité des suppressions** : la corbeille indique la date et l'auteur de chaque suppression.
- **Chiffrement** des connexions (HTTPS) et des mots de passe stockés.
- **Sauvegardes régulières** des données.

06 Les données personnelles sont-elles protégées en cas d'incident ?

- ⚠ Des mesures techniques et organisationnelles sont mises en œuvre pour limiter les risques, sécuriser les accès et protéger les données traitées par l'application. En cas d'incident majeur impliquant des données personnelles, les procédures réglementaires applicables peuvent être mises en œuvre conformément au RGPD.

