

Réflexes en cas de compromission

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 intervention de l'utilisateur ;
- connexions inconnues ;
- e-mails inhabituels ;
- données modifiées ou supprimées ;
- comportement anormal de l'application.

Que faire immédiatement en cas de suspicion de piratage ?

Les premiers réflexes recommandés sont :

1. Modifier immédiatement le mot de passe du compte.
2. Se déconnecter des autres sessions actives si cette fonctionnalité est disponible.
3. Vérifier les informations du compte et les dernières actions effectuées.
4. Contacter rapidement le support Gesti'up Verde via la bulle d'aide.
5. Activer la double authentification (2FA, si elle n'est pas activée).

Que faire si des données semblent avoir été modifiées ?

Il est recommandé :

- de vérifier les modifications effectuées ;
- d'identifier les éléments concernés ;
- de contacter rapidement le support Gesti'up Verde via la bulle d'aide ;
- et de documenter les actions suspectes observées.

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

Les accès suspects sont-ils surveillés ?

Des mécanismes de sécurité et de surveillance peuvent être utilisés afin :

- de détecter des comportements anormaux ;
- de limiter les accès non autorisés ;
- et de protéger les comptes utilisateurs.

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

Des mesures techniques et organisationnelles sont mises en œuvre afin de limiter les risques ; de sécuriser les accès ; et de 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.