


## Quelques conseils pour mieux se protéger avec SNAP

### Modifier les paramètres de confidentialité (d'après le support Snapchat)...

- Appuie sur le bouton  sur ton écran de profil, va jusqu'à l'option "Qui peut... », sélectionne une option, puis appuie sur le bouton Retour pour enregistrer ton choix.
  - Qui peut me trouver dans Ajout rapide : sélectionne qui peut te trouver.
  - M'envoyer des notifications : choisis de recevoir des notifications de tout le monde ou uniquement de tes amis.
  - Me contacter : règle qui peut te contacter directement via un Snap, un Chat, un appel, etc.
  - Qui peut voir ma Story : sélectionne qui peut voir ta Story. Appuie sur "Personnalisé" pour bloquer des amis en particulier et les empêcher de voir ta Story. *(Si ton profil est un profil public, tu devra te rendre dans votre profil pour paramétrer les réglages de confidentialité de la rubrique Ma Story.)*

### Ne plus apparaître dans la carte de géolocalisation

- Active le mode fantôme :
  - Pince sur l'écran principal
  - Clique sur paramètres en haut à droite
  - Active fantôme
  - Maintenant tu es en privé et ton bitmoji est n'apparaît plus sur la carte
- Une fois en mode fantôme, plus personne ne peut savoir où tu te trouves en temps réel. C'est important de te protéger.
- Si tu y tiens absolument avec tes amis proches (et connus dans la vie réelle), tu peux limiter l'affichage de ton bitmoji à ces amis uniquement.

### Se désinscrire d'un groupe s'il y a un problème

- Va sur les Paramètres du groupe, là tu peux te désinscrire du groupe.
- C'est important que tu te le fasse si tu penses avoir des problèmes de cyberharcèlement. N'oublie pas de prendre d'abord des captures d'écran des preuves des contenus qui te font du mal.

### Eviter les applications externes avec Snap

- En octobre 2014, des dizaines de milliers de contenus ont été volés à des utilisateurs de Snap qui utilisaient une application externe. Les conditions générales d'utilisation l'interdisent d'ailleurs formellement. Ce qui veut dire qu'en plus tu n'aurais aucun recours.
- Si tu n'es pas certain du résultat et des conséquences possibles, ne fais rien qui pourrait mettre en cause ta sécurité sur le réseau.