

LES RECOMMANDATIONS

- 1 Mettez en place un **code d'accès**
- 2 **Chiffrez** les données de l'appareil
- 3 Appliquez les **mises à jour** de sécurité
- 4 Faites des **sauvegardes**
- 5 Utilisez une solution de sécurité contre les **virus** et autres attaques
- 6 N'installez des applications que depuis les **sites** ou magasins **officiels**
- 7 Contrôlez les **autorisations** de vos applications
- 8 Ne laissez pas votre appareil sans **surveillance**
- 9 Évitez les réseaux **Wi-Fi** publics ou inconnus
- 10 Ne stockez pas d'informations confidentielles sans protection



CONSEILS



POUR LES MOTS DE PASSE

➔ **Si vous protégez avec ...**
... un code d'accès :
Utilisez au moins 6 chiffres

... un schéma
Ne pas dessiner une lettre ou de schéma trop simple

➔ **Utilisez également la biométrie.**
Visage ou empreinte digitale
À activer en complément du code, afin d'éviter les regards indiscrets

AUTRES CONSEILS

➔ **Carte SIM**
Définissez un code d'accès

➔ **Code IMEI**
Conservez ce code lié au terminal, en cas de perte de vol

=> Pour le récupérer, appeler le *#06#

➔ **Mises à jour**
Mettez régulièrement à jour les applications **ET** le système Android ou iOS

POUR VOS SAUVEGARDES

- ➔ Faites vos **sauvegardes** via un cloud, une carte SD, ou en utilisant un câble et votre ordinateur.
- ➔ Vous pouvez utiliser également une **application tierce** (avec précautions).
- ➔ Réalisez vos sauvegardes de **manière régulière** !