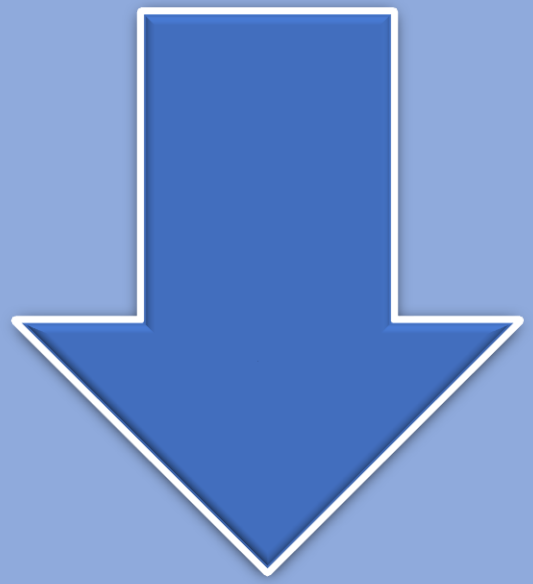
Sécurité Android

Secure Your Android

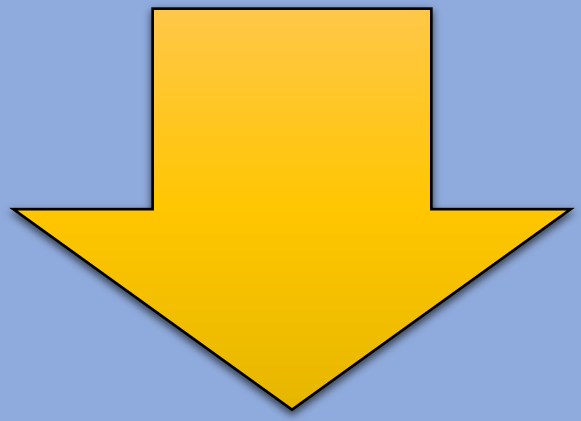
Comment savoir si quelqu’un nous espionne Sinon, qu’est-ce que je peux y faire?

Voici une liste de choses qui peuvent être piratées.

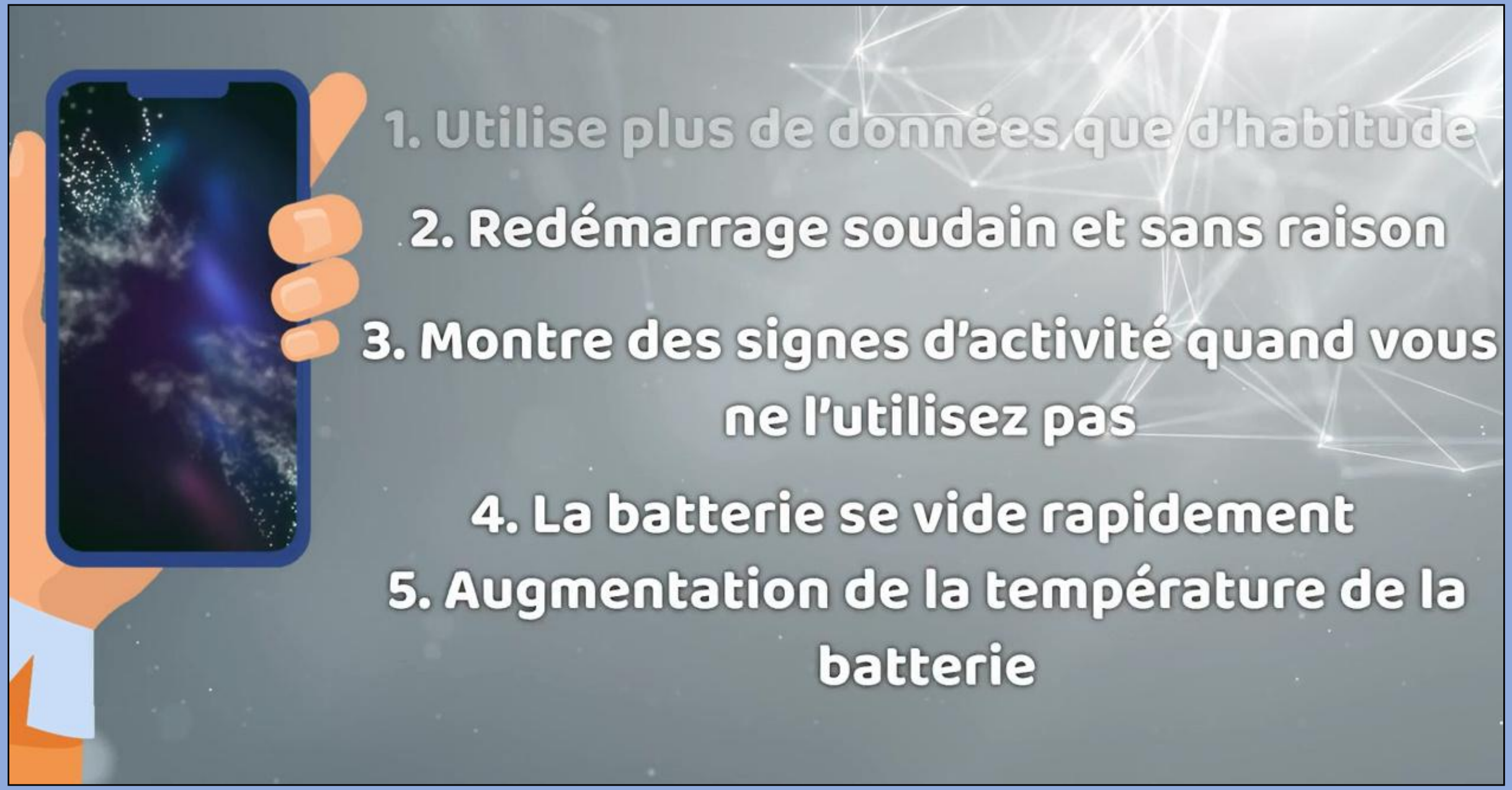


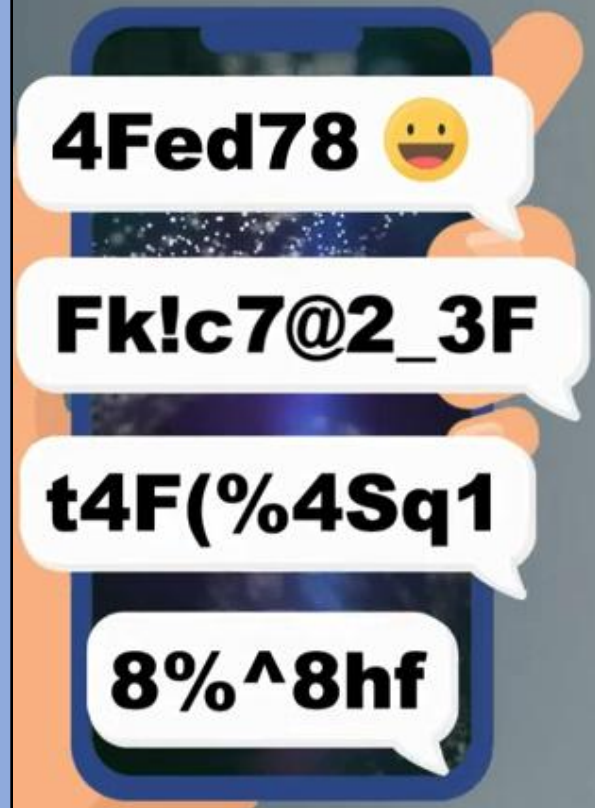

SMS
EMAILS
RÉPONDEUR
PHOTOS
COMPTES RÉSEAUX SOCIAUX
HISTORIQUE DE NAVIGATION
DONNÉES DE TRANSACTIONS BANCAIRES

Il faut être attentif et identifier ces signes ci-dessous.




9 Signes
faciles à identifier


1. Utilise plus de données que d'habitude
2. Redémarrage soudain et sans raison
3. Montre des signes d'activité quand vous ne l'utilisez pas
4. La batterie se vide rapidement
5. Augmentation de la température de la batterie

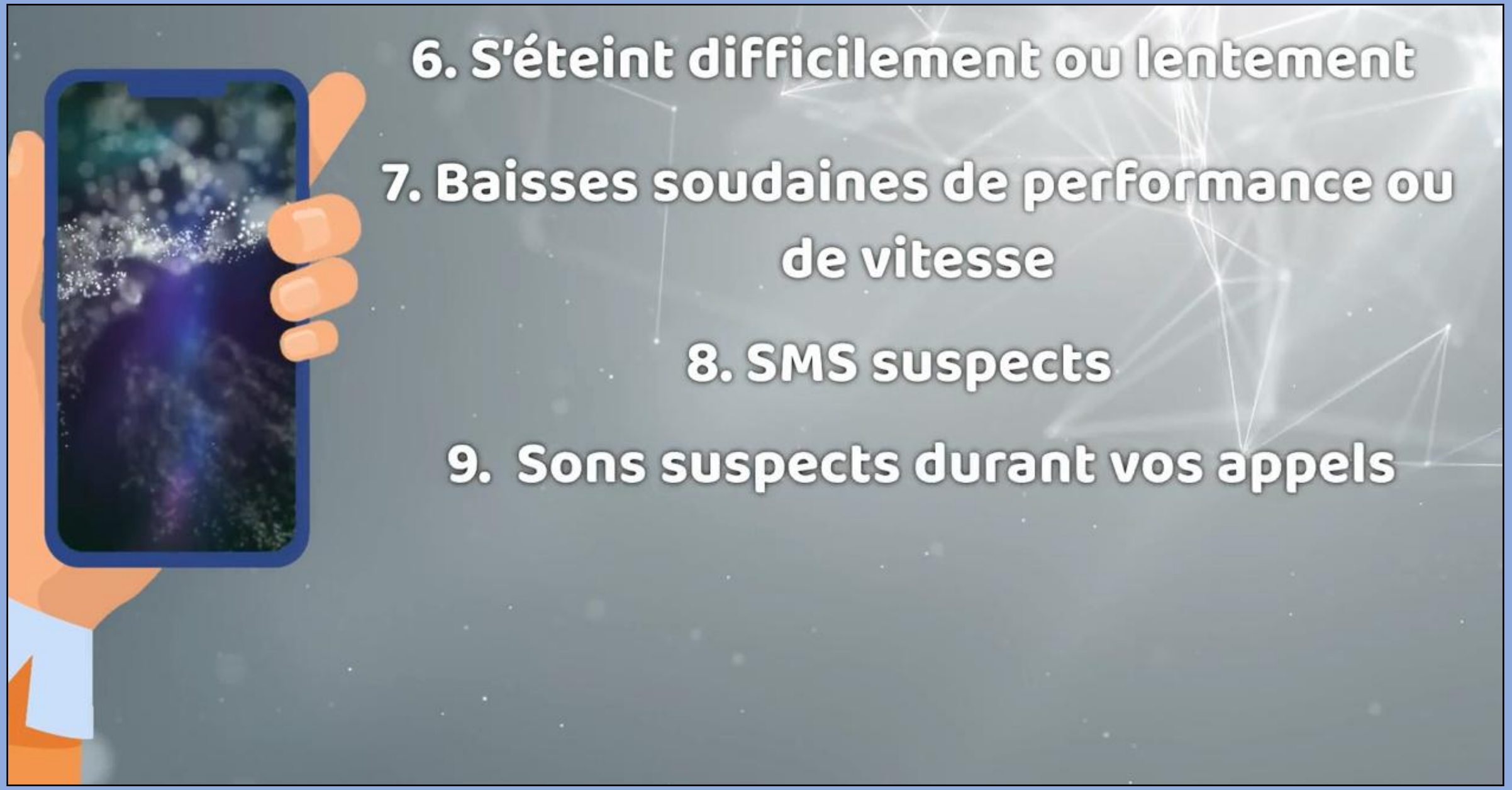


6. S'éteint difficilement ou lentement

7. Baisses soudaines de performance ou de vitesse

8. SMS suspects

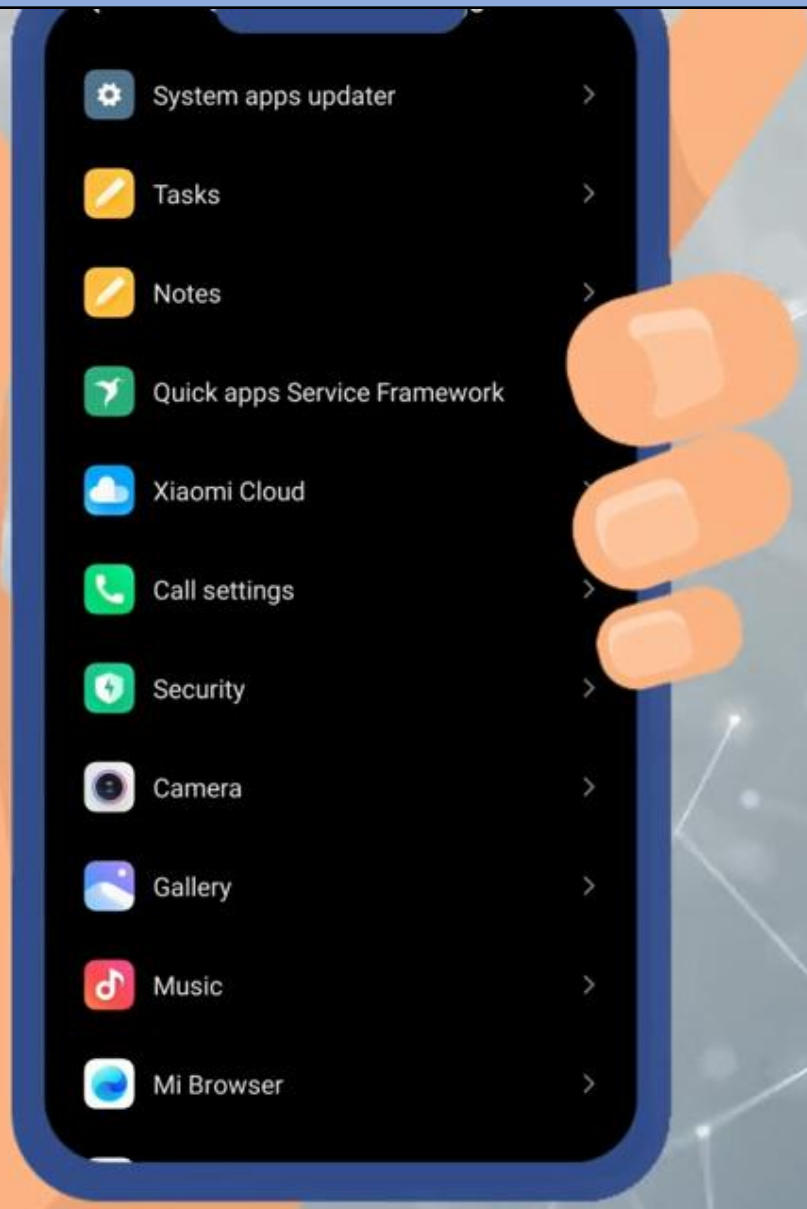
On parle de Smishing, ou la combinaison des SMS et du phishing, quand un arnaqueur vous envoie un message vous redirigeant vers un site frauduleux ou vous demandant d'entrer des informations sensibles. Ne cliquez pas sur des liens dans les SMS ou emails si vous ne connaissez pas l'expéditeur ou s'il parait suspect. Faites confiance à votre instinct.


6. S'éteint difficilement ou lentement
7. Baisses soudaines de performance ou de vitesse
8. SMS suspects
9. Sons suspects durant vos appels


Secure Your
Android
2

Pour vérifier s’il n’y a pas de logiciels malveillants.
Allez dans les applications installées en passant par les paramètres

Vérifiez s’il n’y a pas de noms bizarres comme ce qui suit.



FLEXISPY
SPYERA
IKEYMONITOR
XNSPY
TRACKER
MOBISTEALTH
HOVERWATCH
MESSAGE AND CALL
MOBILE TRACKER FOR ANDROID

Être prudents en téléchargeant des applications

L’une des choses les plus amusantes à faire avec un nouveau Smartphone est d’explorer toutes les formidables applications que vous pouvez télécharger. En commençant à explorer, assurez-vous de télécharger responsablement.

Téléchargez seulement les applications à partir de sites de confiance, vérifiez l’évaluation de l’application et lisez les commentaires pour vous assurer qu’elle soit largement utilisée et respectée.

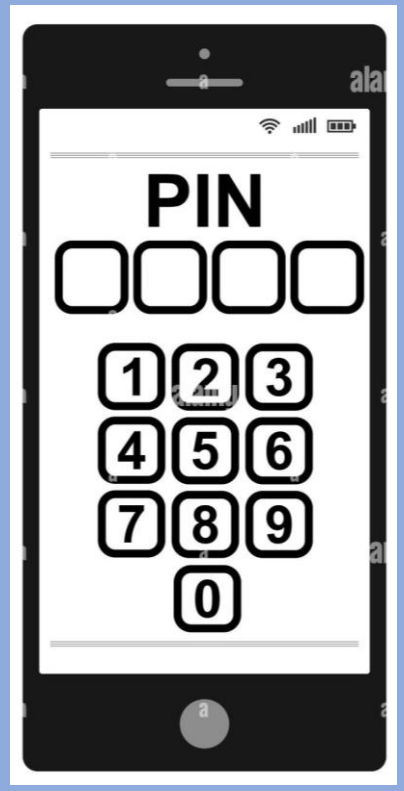

Secure Your
Android
3

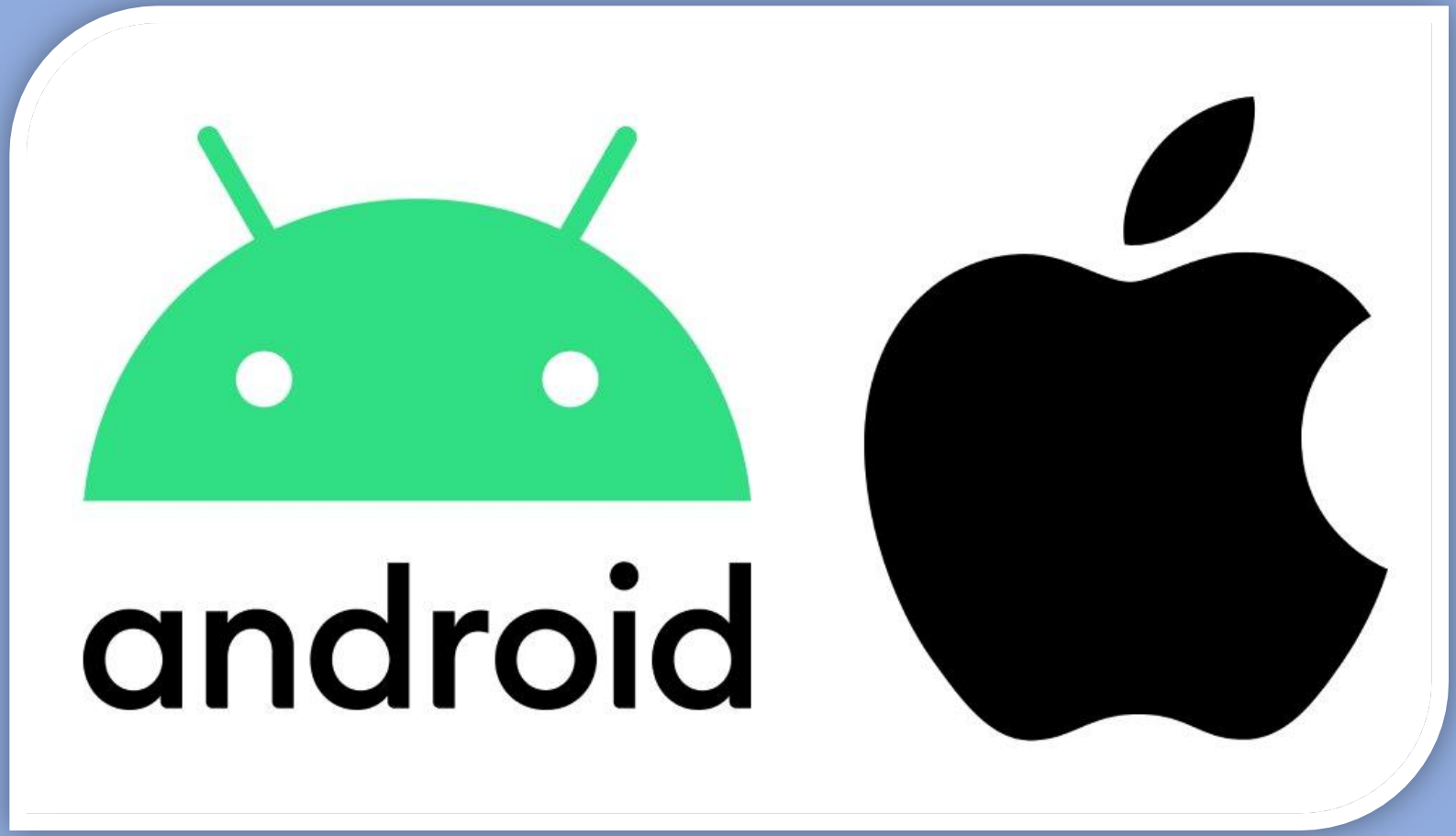
1ere règle pour se protéger efficacement
Le mot de passe, le code PIN, et le code d'acces

Code d’accès et code pin, deux protections complémentaires

Mot de passe, signe, combinaison de touches ou biométrie : le code de verrouillage empêche de pouvoir se servir de l’appareil si on ne le connaît pas.

Composé de 4 chiffres, le code PIN bloque quant à lui l’accès à votre carte SIM et empêche donc de pouvoir s’en servir dans un autre appareil si on ne le connaît pas.





Vous devez changer les mots de passe de votre compte et celui de vos comptes

COMMENT CRÉER UN MOT DE PASSE SOLIDE

- Évitez les évidences
- Utilisez plus de 12 caractères
- Utilisez majuscules et minuscules
- Utilisez des chiffres et des symboles
- N'utilisez pas de mots du dictionnaire

Et comment je vais me souvenir de tous ces mots de passe compliqués

Une autre solution, c'est de passer par les gestionnaires de mots de passe, comme..

Un gestionnaire de mots de passe est un type de logiciel ou de service en ligne qui permet à un utilisateur de gérer ses mots de passe, soit en centralisant l'ensemble de ses identifiants et mots de passe dans une base de données (portefeuille), soit en les calculant à la demande. Le gestionnaire de mots de passe est protégé par un mot de passe unique — appelé *mot de passe maître* —, le seul que l'utilisateur se doit de retenir.

Un gestionnaire de mots de passe peut prendre la forme d'un logiciel autonome, ou d'un module d'extension pour un navigateur web. Les mots de passe peuvent être stockés en local (sur un disque dur, sur un support amovible tel qu'une clé USB), en utilisant les technologies de l'informatique en nuage, ou bien sur un site web[2].


Secure Your
Android
4

Évitez les réseaux publics Wifi publics ou inconnus

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutile- ment.


Secure Your
Android
5

Bluetooth

Contrairement à de nombreuses atteintes a la cyber sécurité où les pirates mènent leurs attaques à distance, les hackers qui exploitent le Bluetooth pour se servir dans vos données doivent se trouver à faible distance de vos appareils Bluetooth. Pour fonctionner, l'appairage en Bluetooth exige que les appareils soient à proximité les uns des autres.

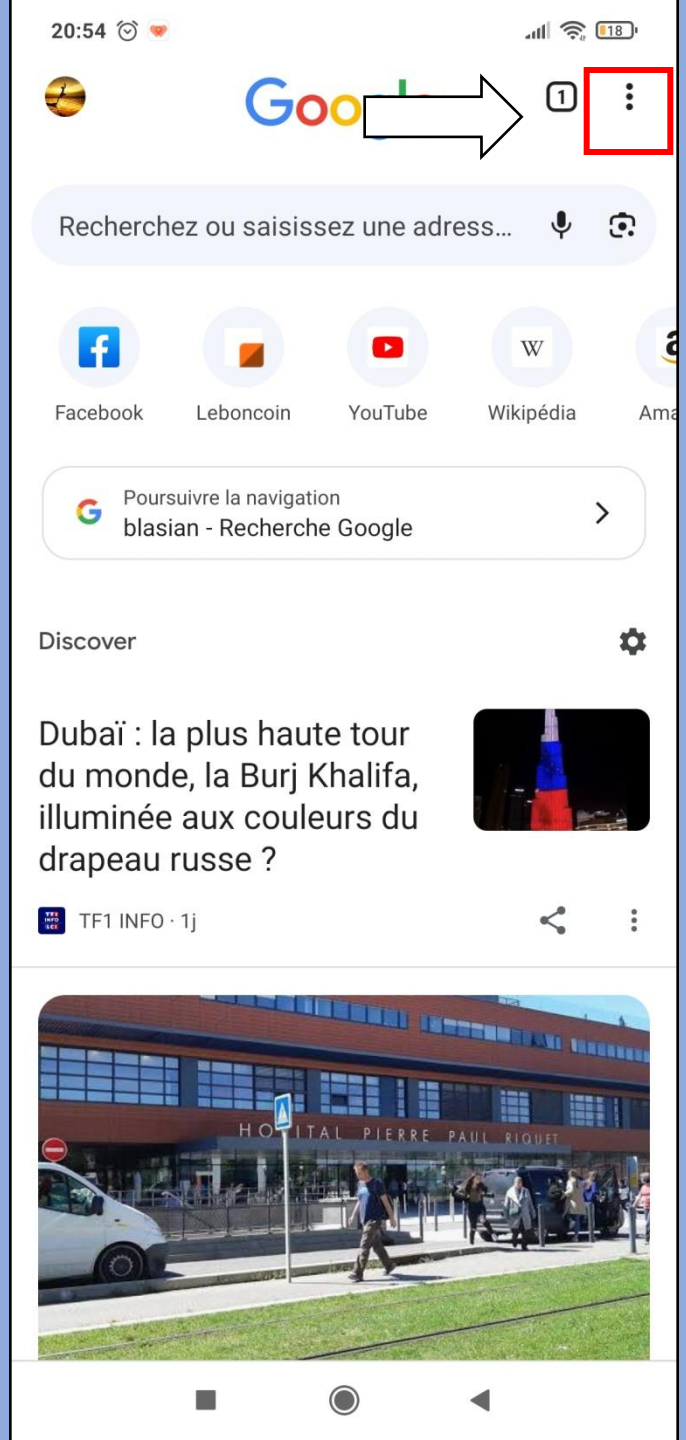
En résumé : pour neutraliser la plupart des problèmes de sécurité évoqués dans cet article, il vous suffit de désactiver votre Bluetooth lorsque vous ne l'utilisez pas.

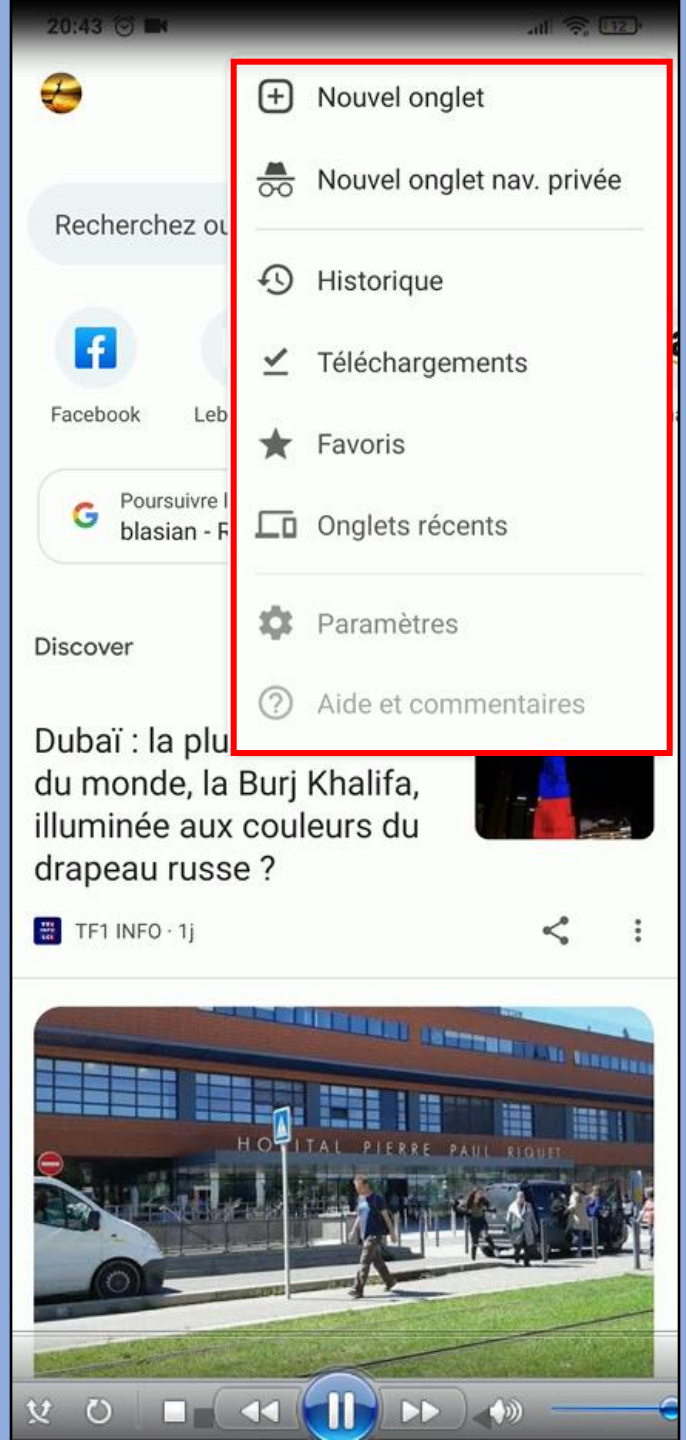
Rejetez les demandes de jumelage provenant d'appareils inconnus

Mettez régulièrement à jour vos firmwares

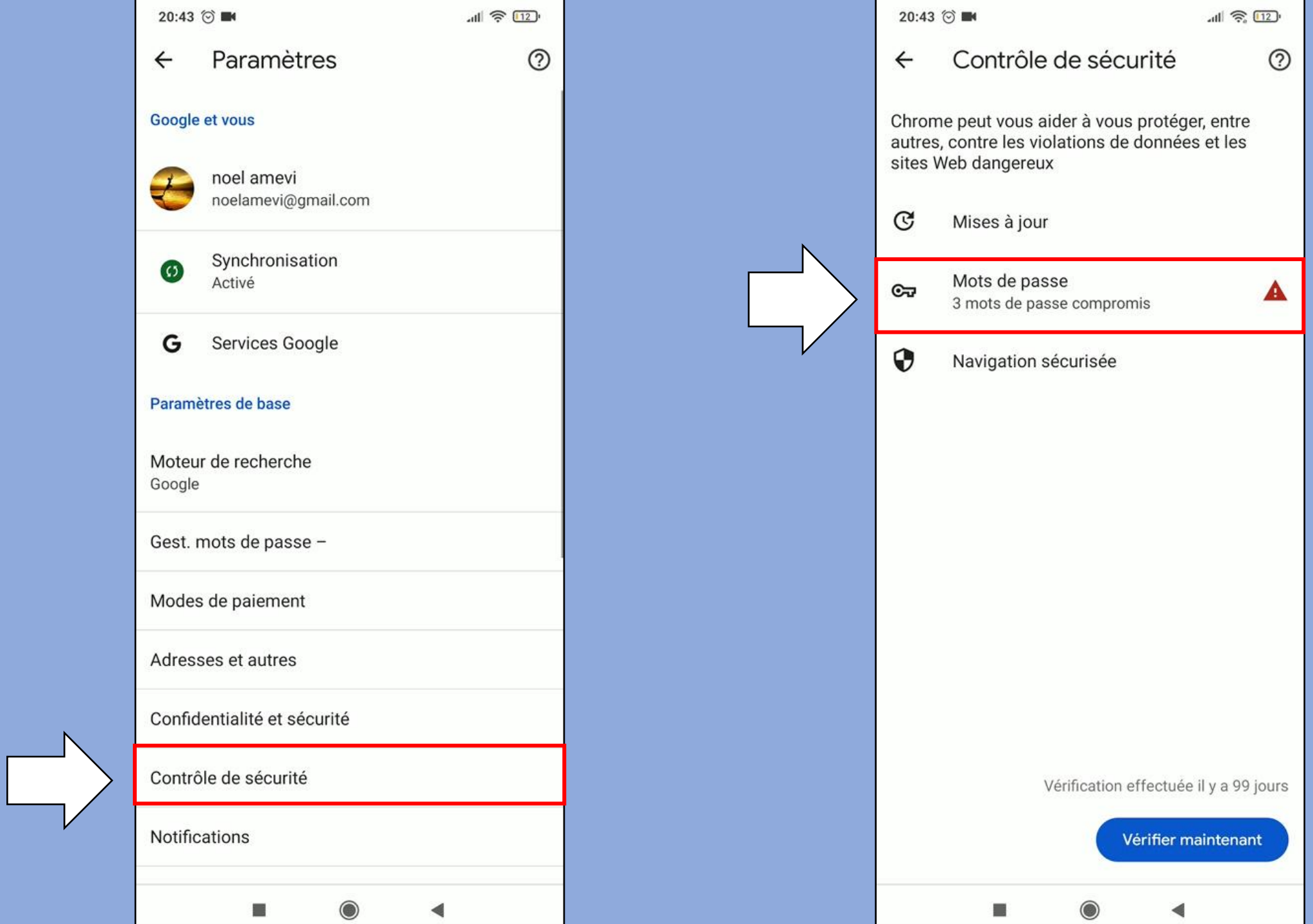

Secure Your
Android
6


ANDROID
PIRATAGE
EMAIL / MOT DE PASSE
LES MEILLEURES ASTUCES ANDROID

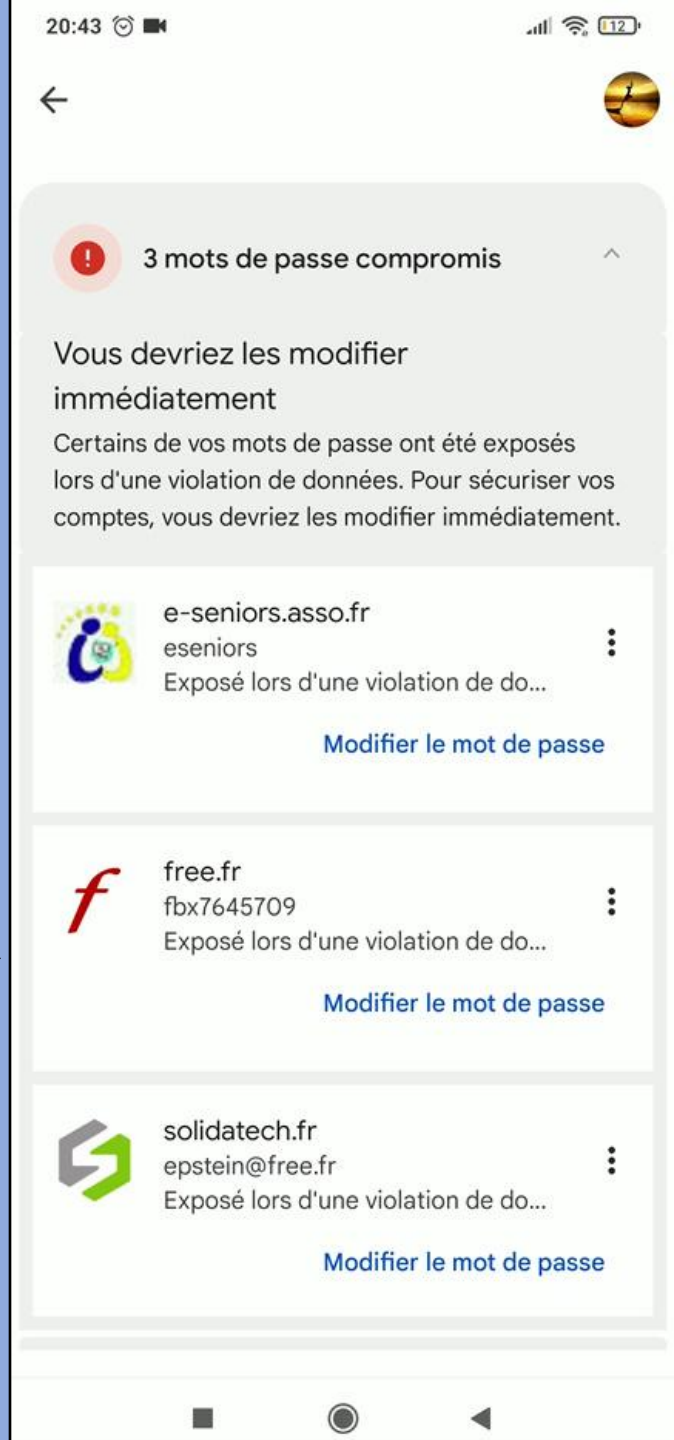

20:54
Recherchez ou saisissez une adress...
Facebook
Leboncoin
YouTube
Wikipédia
Poursuivre la navigation
blasian - Recherche Google
Discover
Dubaï : la plus haute tour du monde, la Burj Khalifa, illuminée aux couleurs du drapeau russe ?
TF1 INFO · 1j
HOPITAL PIERRE PAUL RIQUET


20:43
Nouvel onglet
Nouvel onglet nav. privée
Historique
Téléchargements
Favoris
Onglets récents
Paramètres
Aide et commentaires
Facebook
Discover
Dubaï : la plu
du monde, la Burj Khalifa, illuminée aux couleurs du drapeau russe ?
TF1 INFO · 1j
HOPITAL PIERRE PAUL RIQUET

Pour savoir si vos mots de passe enregistrés sont compromis, cliquez sur chrome et non sur Google. Ensuite sur les trois petits points en haut a droite, puis sur paramètres.
Dans la fenêtre qui s'ouvre, cliquez sur contrôle de sécurité, puis sur mots de passe. Dans la fenêtre du check-up, vous verrez les mots de passe de tous les comptes corrompus.


20:43
Paramètres
Google et vous
noel amevi
noelamevi@gmail.com
Synchronisation
Activé
Services Google
Paramètres de base
Moteur de recherche
Google
Gest. mots de passe –
Modes de paiement
Adresses et autres
Confidentialité et sécurité
Contrôle de sécurité
Notifications
20:43
Contrôle de sécurité
Chrome peut vous aider à vous protéger, entre autres, contre les violations de données et les sites Web dangereux
Mises à jour
Mots de passe
3 mots de passe compromis
Navigation sécurisée
Vérification effectuée il y a 99 jours
Vérifier maintenant


20:43
Check-up Mots de passe
Mots de passe vérifiés pour 25 sites ou applis
3 mots de passe compromis
Vous devriez les modifier immédiatement
24 mots de passe réutilisés
Créez des mots de passe uniques
14 mots de passe peu sécurisés
Créez des mots de passe sécurisés


20:43
3 mots de passe compromis
Vous devriez les modifier immédiatement
Certains de vos mots de passe ont été exposés lors d'une violation de données. Pour sécuriser vos comptes, vous devriez les modifier immédiatement.
e-seniors.asso.fr
eseniors
Exposé lors d'une violation de do...
Modifier le mot de passe
free.fr
fbx7645709
Exposé lors d'une violation de do...
Modifier le mot de passe
solidatech.fr
epstein@free.fr
Exposé lors d'une violation de do...
Modifier le mot de passe

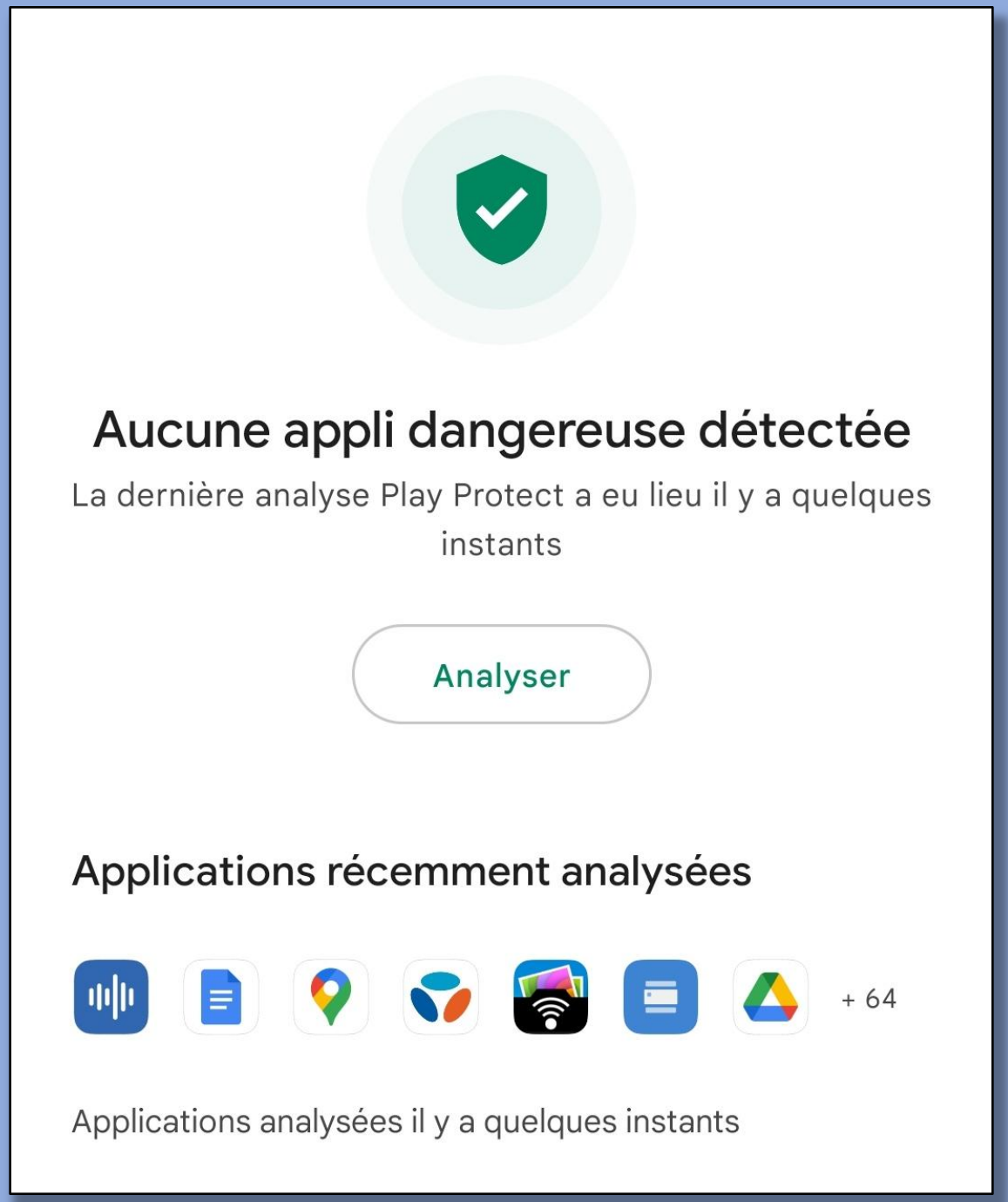

Secure Your
Android
7

Pour savoir si vous n’avez aucune applications dangereuses installées.

Allez sur Play store

Saisir Play Protect, validez et voyez le rapport.

Le rapport doit apparaitre comme ceci.




Secure Your
Android

Un numéro que tout le monde se doit de connaitre le code IMEI

Composé de 15 à 17 chiffres, le code IMEI est le numéro de série de votre appareil mobile. Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.
Notez le soigneusement et, si vous l'avez égaré, vous pouvez le récupérer en tapant ce numéro.

EN APPUYANT DESSUS, TU PEUX DÉCOUVRIR TON NUMÉRO D'IDENTIFICATION D'ÉQUIPEMENT MOBILE INTERNATIONAL, OU, COMME APPELÉ PLUS COMMUNÉMENT TON IM

Pour savoir si vos appels ne sont pas transférés vers un autre numéro

SAISIR *#21#

et appuyez sur appel

Le service doit être désactivé.

Pour savoir si vous n’êtes pas sur écoute

Faites *#62#

et appuyez sur appel

Doit apparaitre une fenêtre qui indique que le transfert est désactivé.

Et si jamais vous avez un numéro suspect, voici comment faire pour désactiver cet espionnage en faisant simplement ce code, puis faire appel

Vous aurez une fenêtre, qui indiquera que tout transfert a été désactivé.


Secure Your
Android
9

Faut-il mettre un antivirus sur son smartphone Android / iPhone ?

Ce n’est pas nécessaire.

Car le risque d’infection est très faible

Il y a des solutions de protections déjà dans Android.

La consommation de la ressource est élevée.

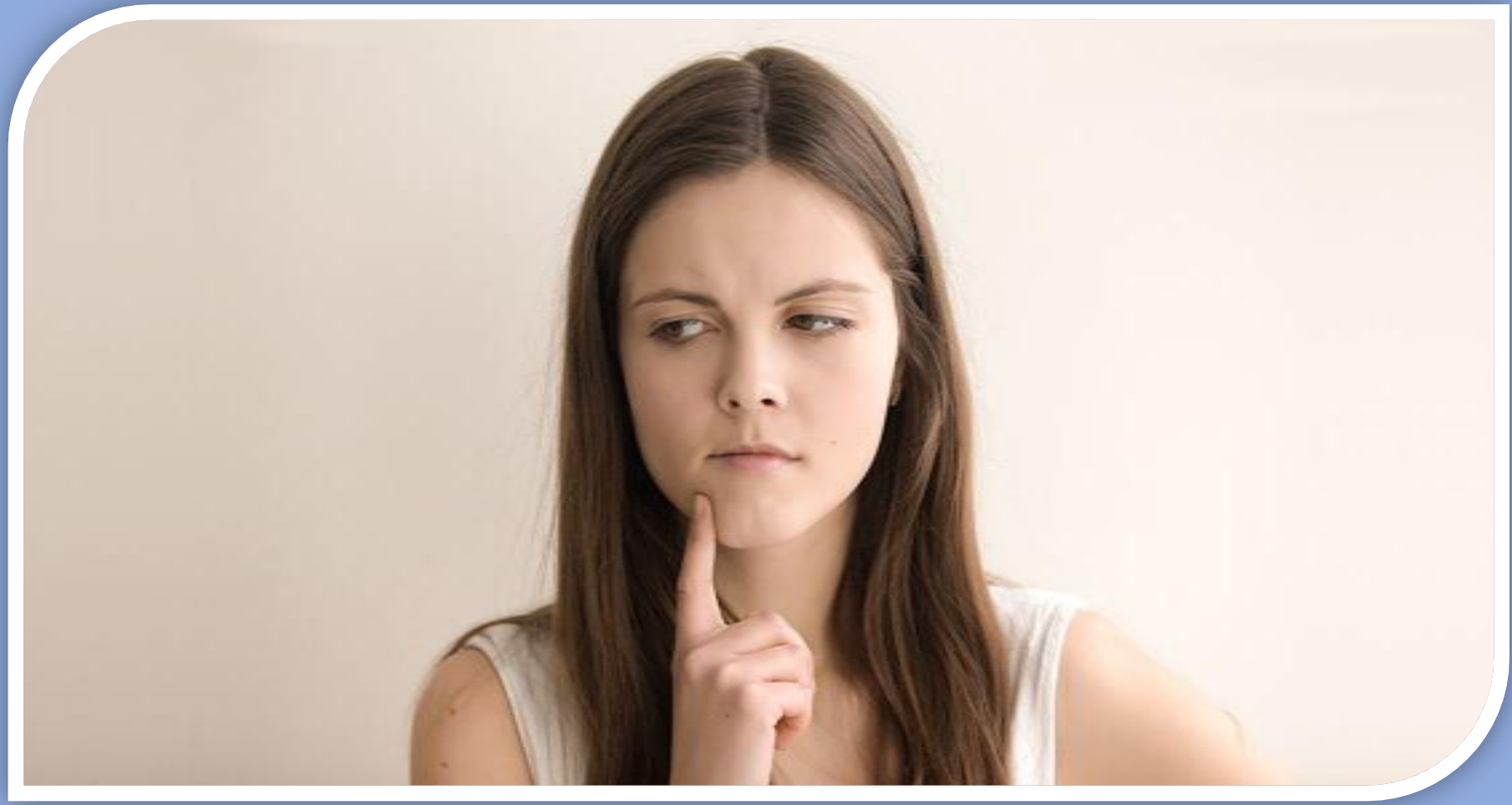
Vous êtes le meilleur antivirus

Mais si jamais vous voulez mettre plus de sécurité, sachez que cela ne dépendra que de la puissance de votre Smartphone, et la configuration idéale requise est celle ci en dessous.

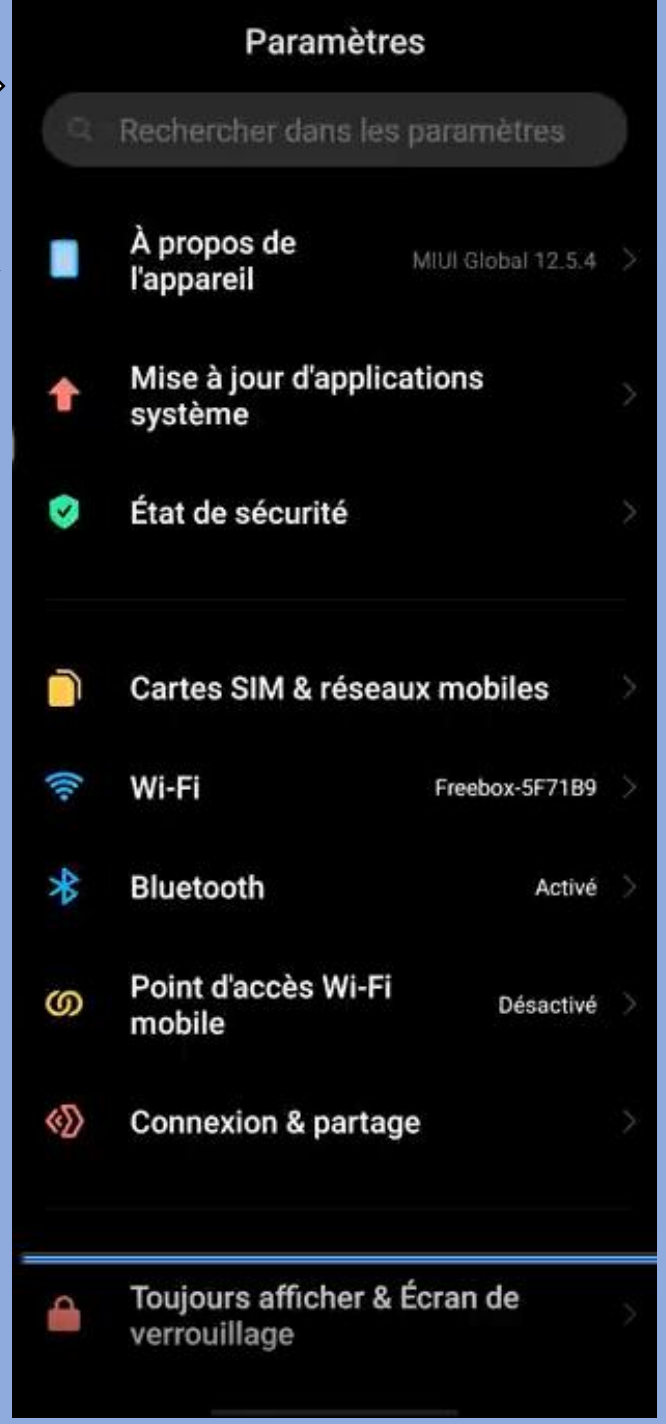
Processeur Qualcomm Snapdragon 898.

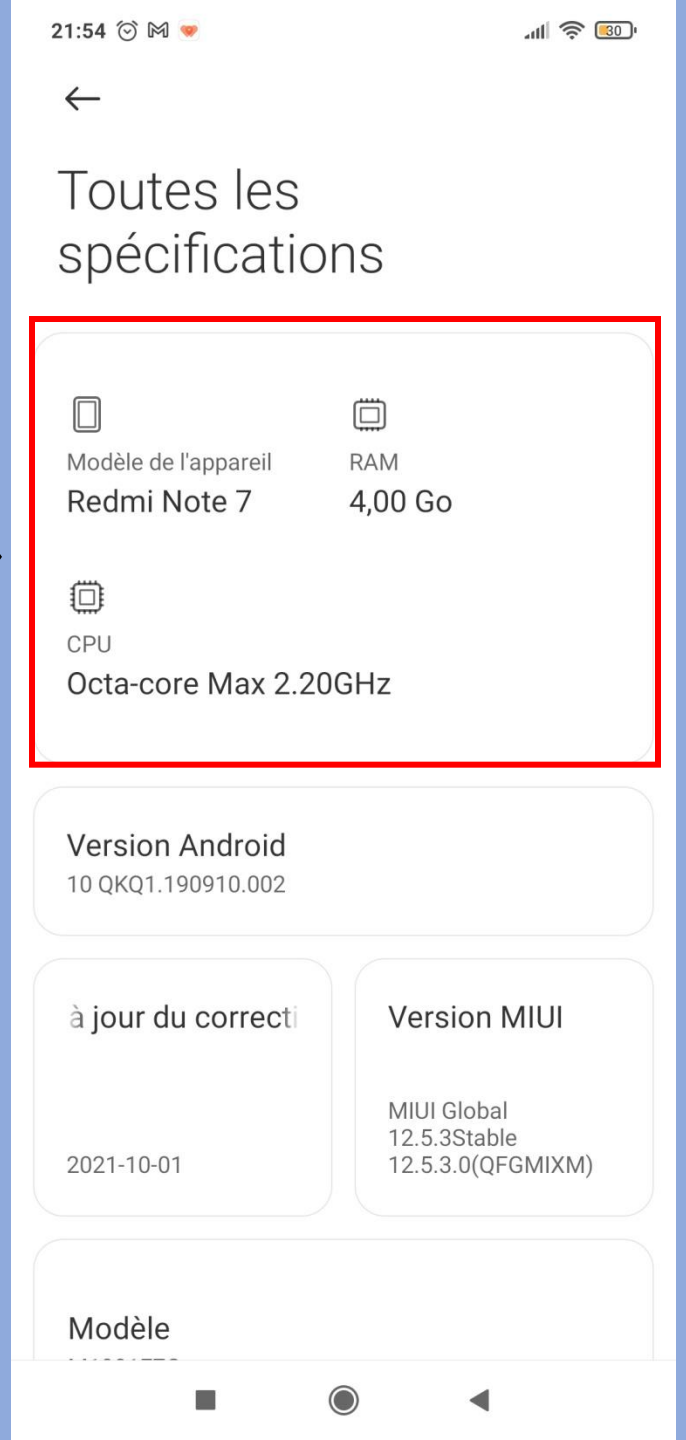
Ou 2.20 Ghz en processeur et 4ghz en mémoire ram, minimum.

Comment savoir ou se trouve ces spécifications?

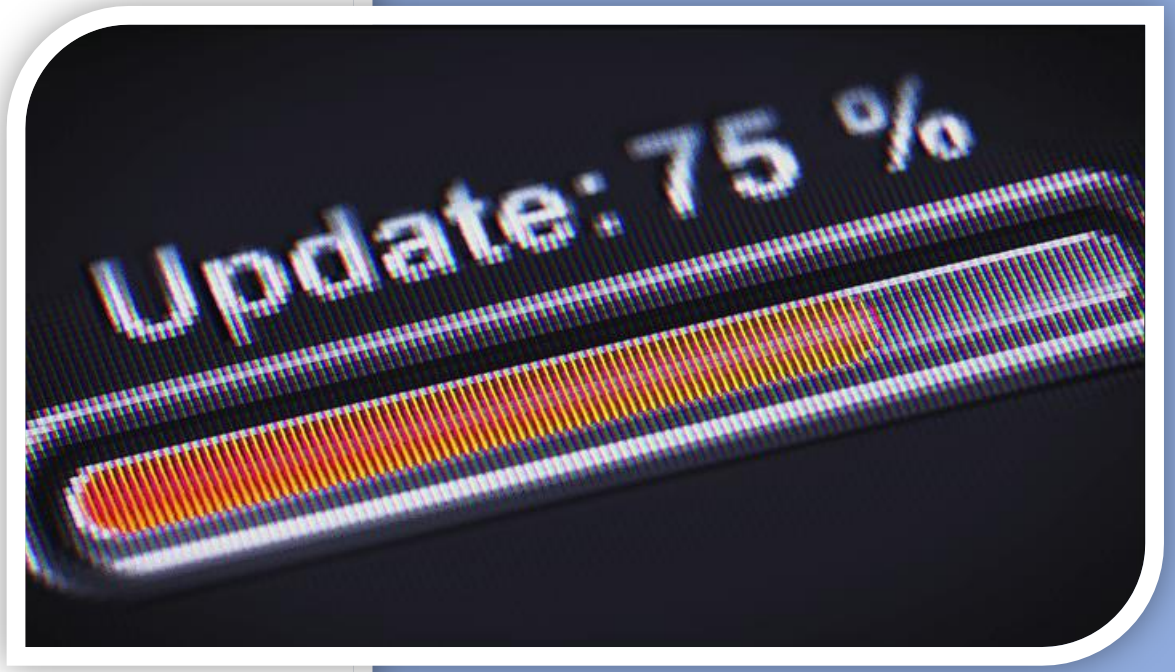


1) Faites Paramètres.
2) puis A propos du téléphone.
3) puis Toutes les spécifications.


Paramètres
Rechercher dans les paramètres
À propos de l'appareil
MIUI Global 12.5.4
Mise à jour d'applications système
État de sécurité
Cartes SIM & réseaux mobiles
Wi-Fi
Freebox-5F71B9
Bluetooth
Activé
Point d'accès Wi-Fi mobile
Désactivé
Connexion & partage
Toujours afficher & Écran de verrouillage


21:54
Toutes les spécifications
Modèle de l'appareil
Redmi Note 7
RAM
4,00 Go
CPU
Octa-core Max 2.20GHz
Version Android
10 QKQ1.190910.002
à jour du correcti
2021-10-01
Version MIUI
MIUI Global
12.5.3Stable
12.5.3.0(QFGMIXM)
Modèle

Profitez pour mettre a jour le firmwares.




Secure Your
Android
10

Si vous avez la configuration requise,
alors allez sur Playstore
Saisissez antivirus et validez.
Choisissez
Avast

Qui est très efficace pour

- Analyser
- Augmenter la vitesse de la ram
- Nettoyer
- Analyser le wifi
- Optimise le chargement
- Verrouille des applications

En plus d'une application antivol
et une protection de votre vie privée en ligne
avec Secure line mais qui est malheureusement payant.

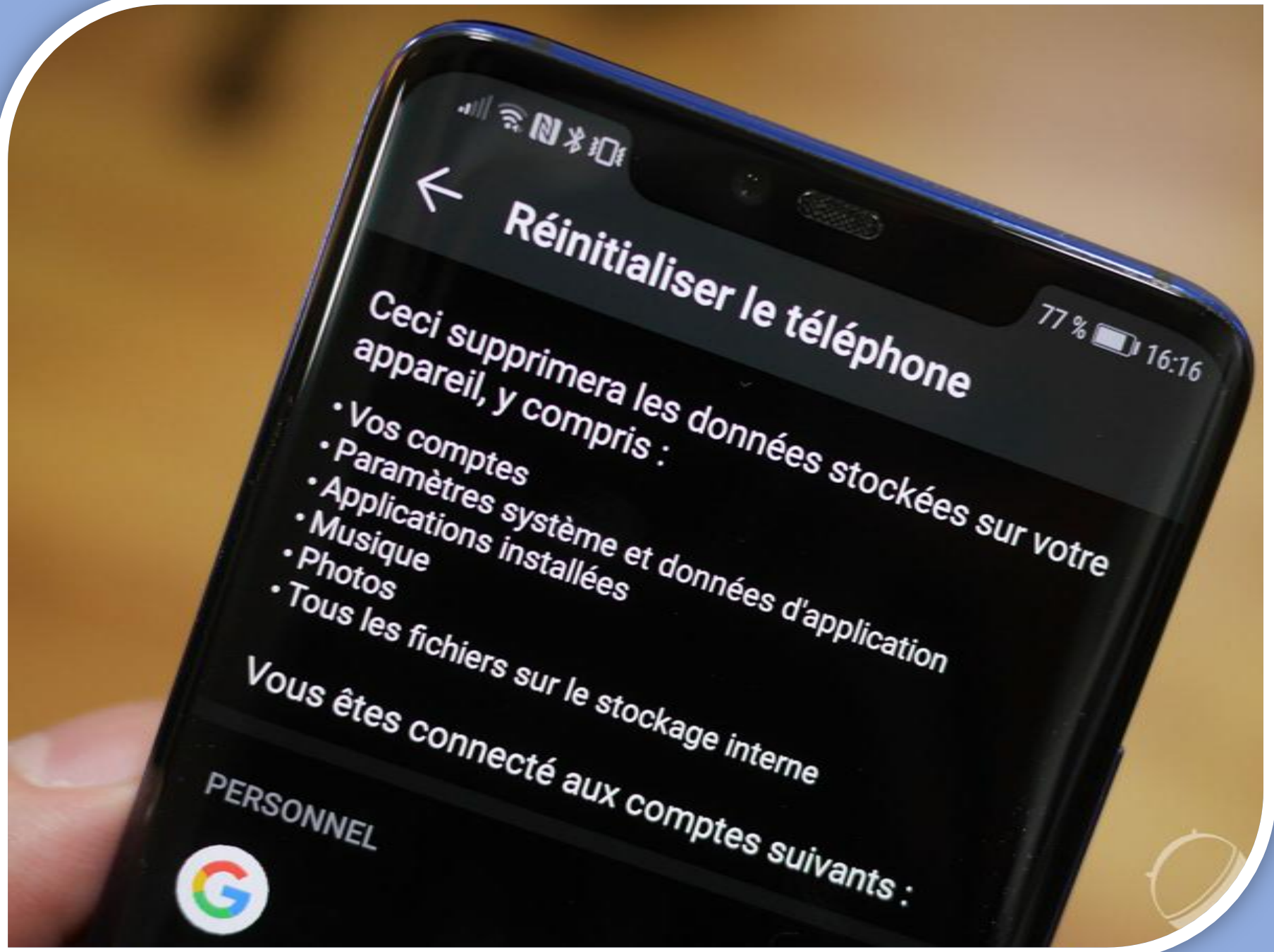
Pour une protection optimale, faire coupler obligatoirement l'antivirus avec une autre application qui s'appelle CLEAN MASTER

Qui est différend de CCLEANER, dont les fonctions ne sont plus a démontrer.

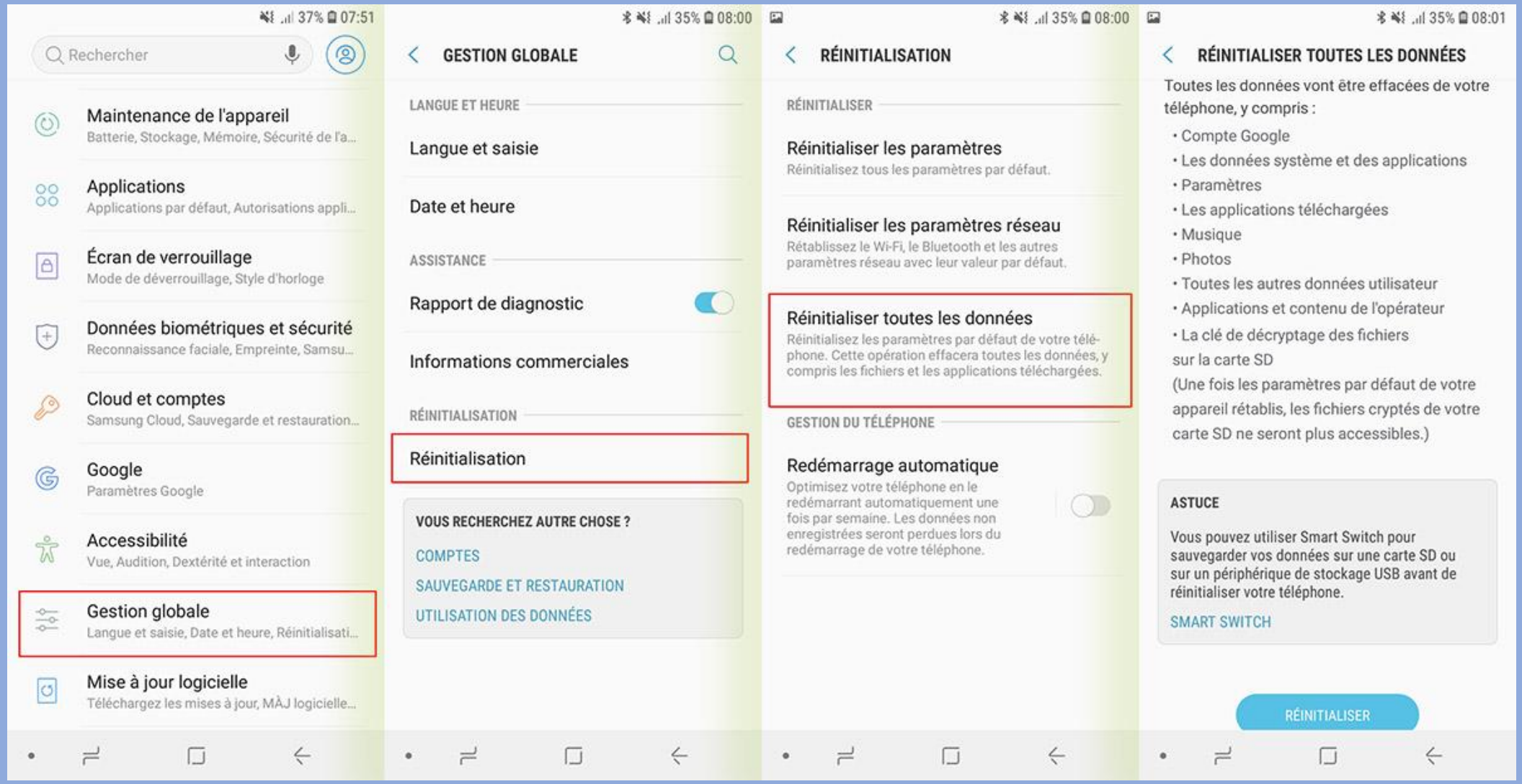
- Eradications des fichiers indésirables
- Boost du téléphone
- Refroidisseur du CPU
- Il englobe aussi un antivirus qui ne crée pas de conflit avec l'AVAST.
- Economiseur de batterie
- Nettoyeur de notification
- Sécurité WIFI
- Nettoie les vidéos et les conneries de Whatsapps,
- de Facebook et autres Twitter non protégées.

Si malgré toutes ces actions radicales, vous constatez encore des problèmes.
Vous devez réinitialiser votre téléphone, c’est-à-dire le remettre a l’état d’usine.


RÉGLAGES
D'USINE


Réinitialiser le téléphone
77 %
16:16
Ceci supprimera les données stockées sur votre appareil, y compris :
• Vos comptes
• Paramètres système et données d'application
• Applications installées
• Musique
• Photos
• Tous les fichiers sur le stockage interne
Vous êtes connecté aux comptes suivants :
PERSONNEL

Selon le modèle de Smartphone, c'est par les paramètres, puis a propos du téléphone




UPDATE...
N'OUBLIEZ PAS DE SAUVEGARDER VOS DONNÉES AVANT !


FlashDrive
USB OTG

Désactivez la synchronisation automatique avec le cloud


Tout est dit.