Conseils pour éviter les applications dangereuses sur Android

Pour éviter d'installer des applications douteuses sur Android, vous devez savoir comment déterminer si une application est sûre. Ces conseils cruciaux vous aideront.

Ali Arslan ⁝

Principaux points à retenir

- Google Play Protect analyse les applications du Play Store et des sources inconnues pour s'assurer qu'elles sont sûres. Activez-le dans les paramètres du Play Store pour une protection supplémentaire.
- Évitez de télécharger des applications à partir de magasins tiers ou de sources inconnues afin de minimiser le risque de téléchargement d'applications malveillantes ou de logiciels malveillants.
- Vérifiez les autorisations de l'application avant l'installation pour déterminer les données ou les fonctionnalités auxquelles l'application peut accéder.
  Utilisez le Gestionnaire d'autorisations intégré ou AppBrain pour une analyse complète.

Le Google Play Store n'est pas le seul moyen de télécharger des applications Android. Les magasins d'applications tiers vous donnent accès à des applications qui ne sont pas disponibles sur le Play Store, certains prétendant même offrir des applications payantes gratuitement.
En chargeant ces applications, vous risquez potentiellement vos données personnelles.

Parfois, les applications sur le Play Store ne sont pas sûres non plus.
Ils peuvent demander une foule d'autorisations pour accéder à des données dont ils n'ont pas strictement besoin et diffuser des annonces pour vous suivre.
Bien que Google s'efforce de garder les applications nuisibles hors de Google Play, vous devez également prendre des précautions de votre côté.

Voyons donc comment détecter et éviter les applications potentiellement dangereuses sur Android.

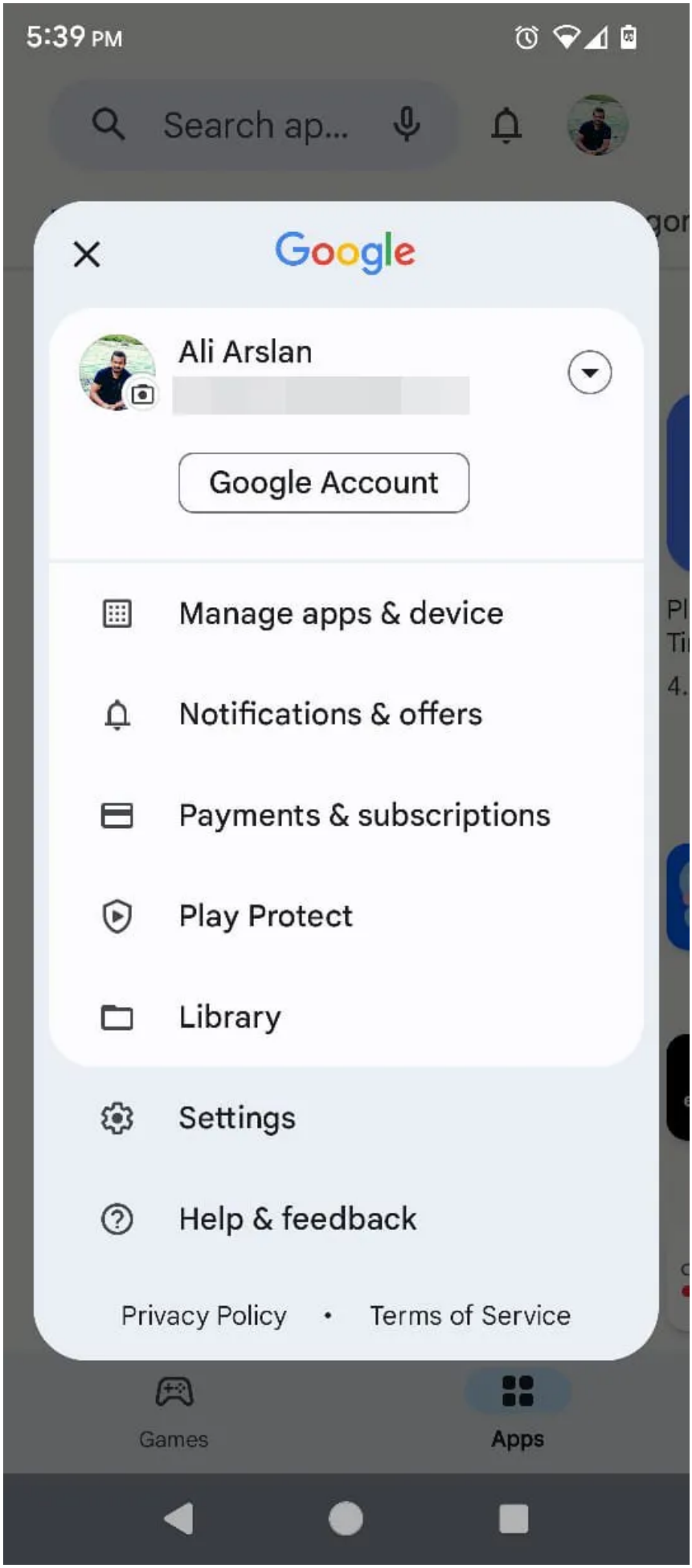
1. Utilisez Google Play Protect

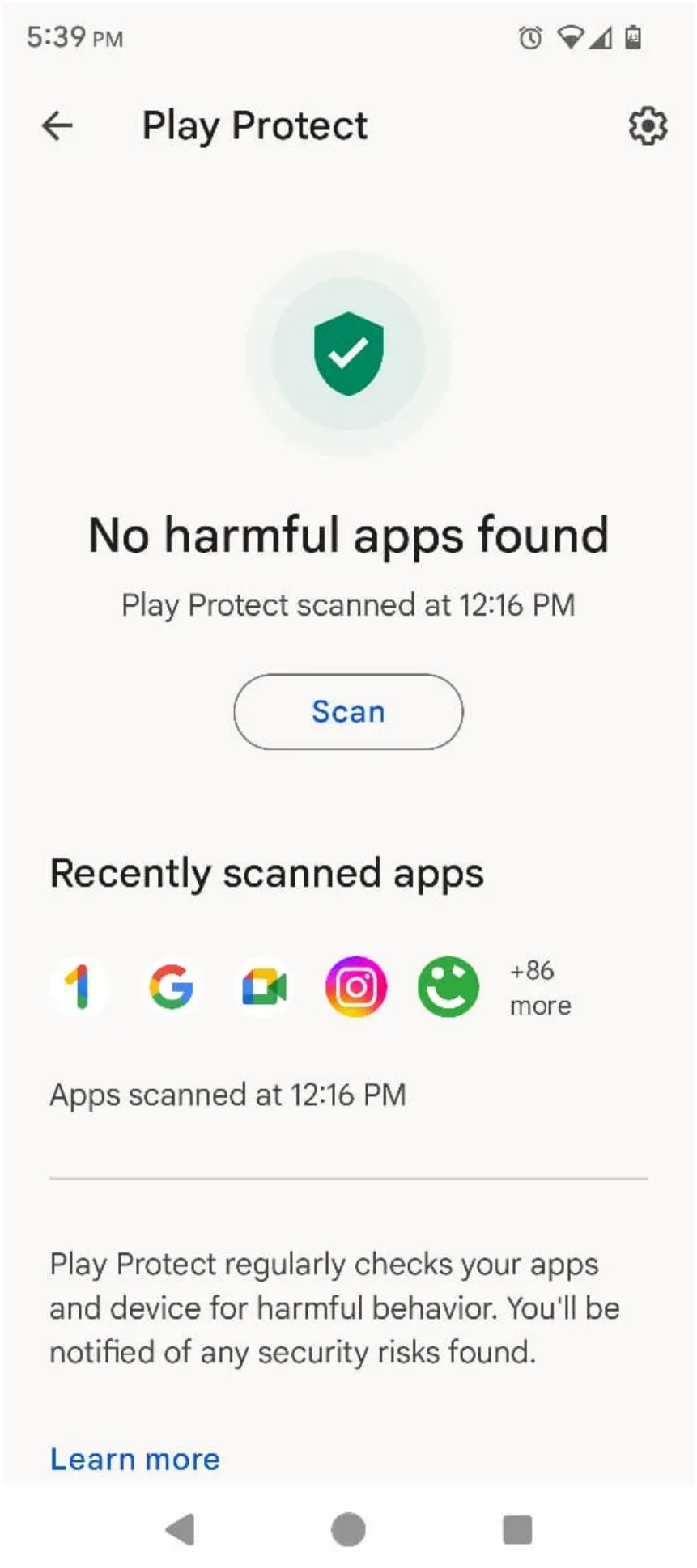
Le Play Store est l'endroit le plus sûr pour parcourir et installer des applications Android. Google utilise une variété de mécanismes de sécurité et s'assure que les applications que vous téléchargez sont sûres.

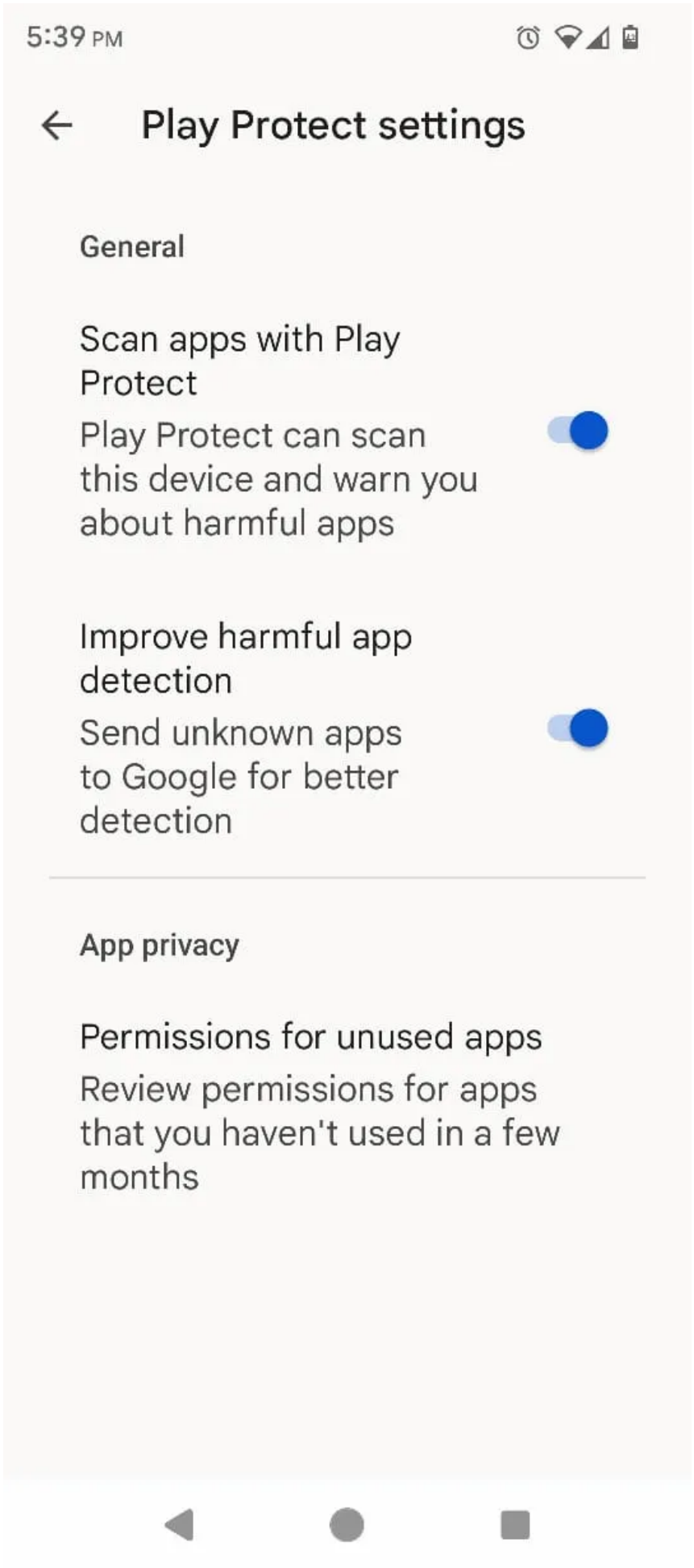
L’un de ces mécanismes est Google Play Protect, qui fonctionne en arrière-plan pour analyser les applications du Play Store ainsi que toutes celles que vous installez à partir de sources inconnues.

Pour vérifier l’état de Play Protect sur votre appareil, ouvrez le **Play Store**, appuyez sur votre photo d’affichage, puis sélectionnez **Play Protect**.
Vérifiez ensuite l’état des applications **récemment analysées** et activez l’option **Améliorer la détection des applications nuisibles** dans ses paramètres pour envoyer des applications inconnues à Google pour un examen plus approfondi, si vous le souhaitez.

De cette façon, il vous protège mieux contre les applications que vous chargez sur votre appareil Android.


5:39 PM
Search ap...
Google
Ali Arslan
Google Account
Manage apps & device
Notifications & offers
Payments & subscriptions
Play Protect
Library
Settings
Help & feedback
Privacy Policy • Terms of Service
Games
Apps


5:39 PM
Play Protect
No harmful apps found
Play Protect scanned at 12:16 PM
Scan
Recently scanned apps
+86 more
Apps scanned at 12:16 PM
Play Protect regularly checks your apps and device for harmful behavior. You'll be notified of any security risks found.
Learn more


5:39 PM
Play Protect settings
General
Scan apps with Play Protect
Play Protect can scan this device and warn you about harmful apps
Improve harmful app detection
Send unknown apps to Google for better detection
App privacy
Permissions for unused apps
Review permissions for apps that you haven't used in a few months

2. Évitez les applications provenant de magasins tiers et de sources inconnues

Il peut y avoir certaines situations où vous devrez prendre la route du chargement latéral ou de la boutique d'applications tierce.
Par exemple, vous pouvez vouloir une application qui n'est pas disponible sur le Play Store dans votre région ou installer une ancienne version d'une application particulière si la nouvelle commence à planter ou supprime les fonctionnalités dont vous avez besoin.

En règle générale, nous vous recommandons de ne pas installer autant que possible d'applications en dehors du Play Store, bien que si vous en avez besoin, vous devriez utiliser les sites les plus réputés et les plus sûrs pour télécharger des fichiers APK.

Il existe de nombreux autres magasins d'applications et beaucoup d'entre eux ne nécessitent même pas d'enregistrement de développeur pour soumettre des applications. Ils manquent souvent de contrôles de sécurité, de politiques strictes et de contrôle de la qualité, il est donc plus facile de télécharger des applications malveillantes.

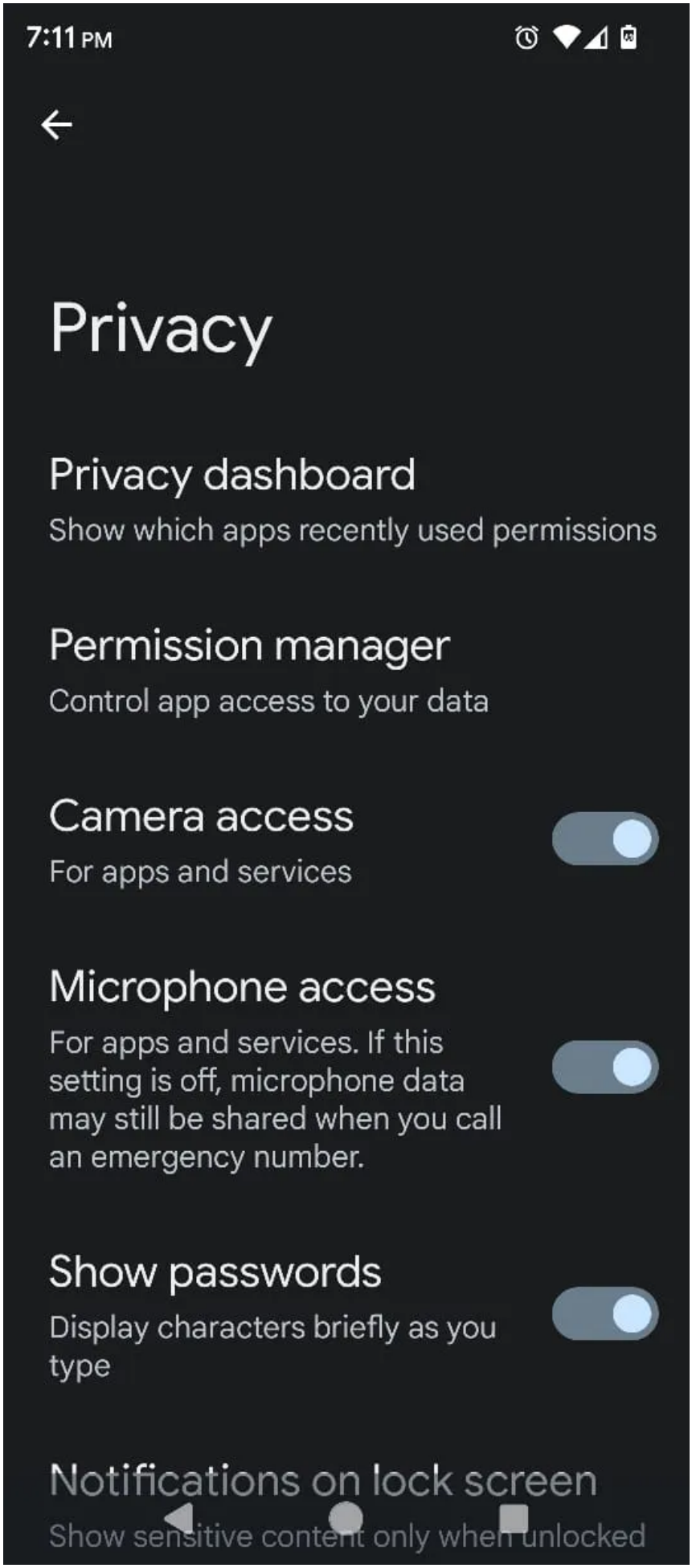
Enfin, si vous essayez d'obtenir une version fissurée ou modifiée d'une application, vous ne les trouverez que sur des sites Web et des magasins douteux, et vous ne serez jamais sûr de télécharger un logiciel malveillant au lieu d'un APK légitime.
Donc, une règle de base: si cela semble trop beau pour être vrai, il est préférable de l'éviter.

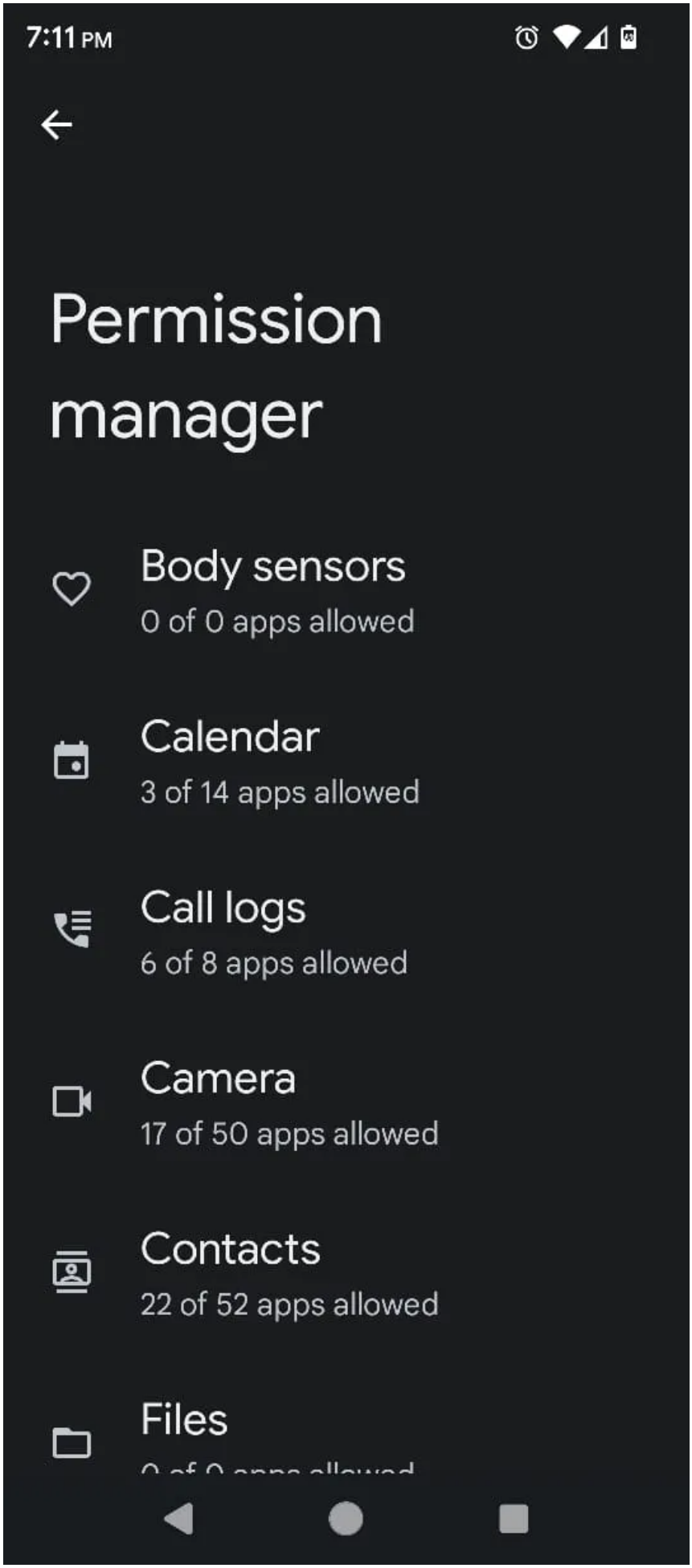
3. Recoupez les autorisations de l'application

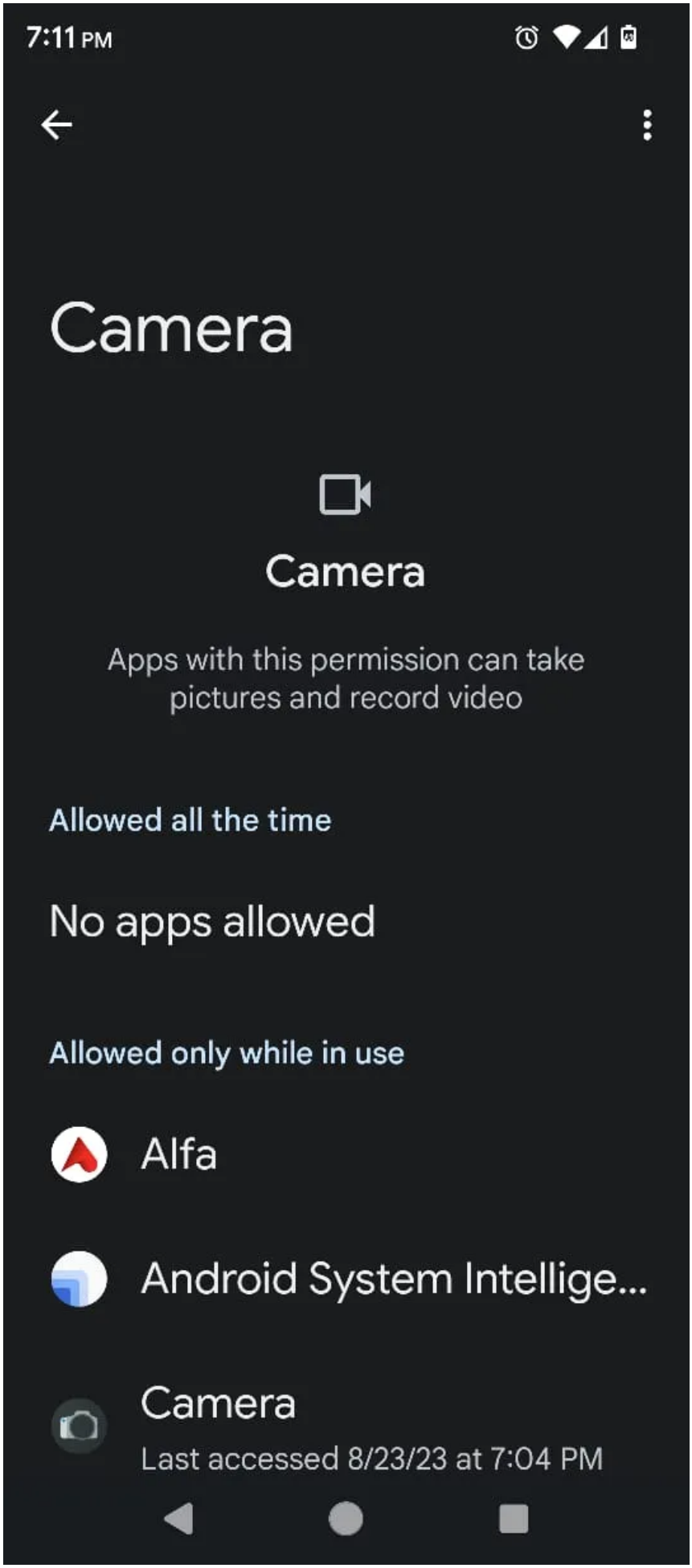
Depuis Android Marshmallow, vous accordez aux applications une autorisation individuelle d'accéder à certaines données ou fonctionnalités selon vos besoins.
Avant d'installer une application, vous devez examiner complètement les autorisations souhaitées par l'application.

Au bas de la page d'informations de chaque application, vous verrez une section intitulée Détails de **l'autorisation**.
Mais ce n'est qu'un résumé de base.
Il vous indique les autorisations demandées par les applications, mais pas l'utilisation réelle des autorisations.

C'est là que le **gestionnaire d'autorisations** intégré est utile.
Cette section des paramètres de votre téléphone Android contient tous les composants auxquels les applications peuvent demander l'autorisation d'accès.
Vous pouvez appuyer sur chaque composant pour obtenir une liste des applications qui y ont accès.
Par exemple, appuyez sur **Appareil** photo pour trouver les applications accédant à l'appareil photo, et vous pouvez modifier l'autorisation pour chaque application à partir d'ici.


7:11 PM
Privacy
Privacy dashboard
Show which apps recently used permissions
Permission manager
Control app access to your data
Camera access
For apps and services
Microphone access
For apps and services. If this setting is off, microphone data may still be shared when you call an emergency number.
Show passwords
Display characters briefly as you type
Notifications on lock screen
Show sensitive content only when unlocked


7:11 PM
Permission manager
Body sensors
0 of 0 apps allowed
Calendar
3 of 14 apps allowed
Call logs
6 of 8 apps allowed
Camera
17 of 50 apps allowed
Contacts
22 of 52 apps allowed
Files


7:11 PM
Camera
Camera
Apps with this permission can take pictures and record video
Allowed all the time
No apps allowed
Allowed only while in use
Alfa
Android System Intellige...
Camera
Last accessed 8/23/23 at 7:04 PM

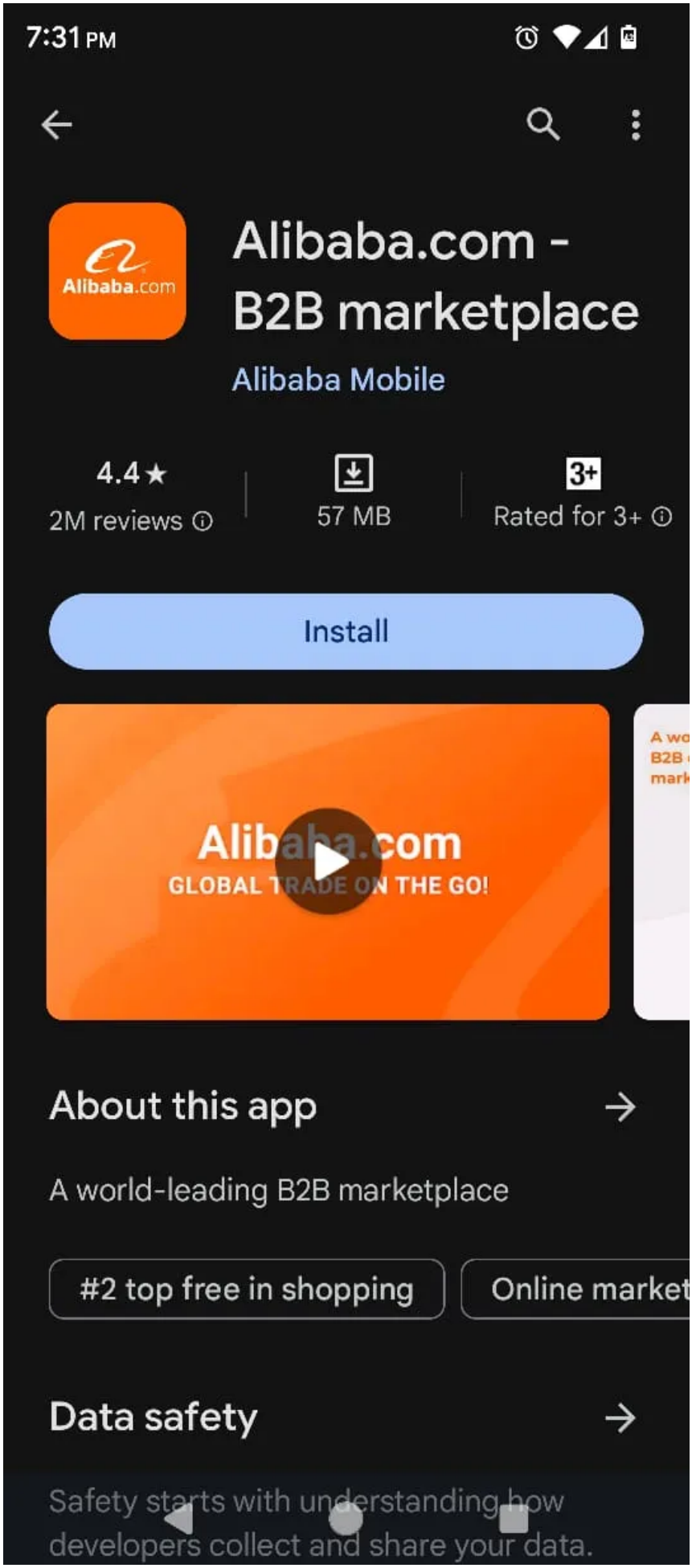
Vous pouvez également accéder à AppBrain et entrer un nom d'application dans la zone de recherche.
Cliquez ensuite sur la page de l'application pour voir une analyse approfondie.
Prenez note de l'âge et de la date de la dernière mise à jour de l'application, de la fréquence des mises à jour, des autorisations utilisées par l'application et des réseaux publicitaires utilisés par l'application.

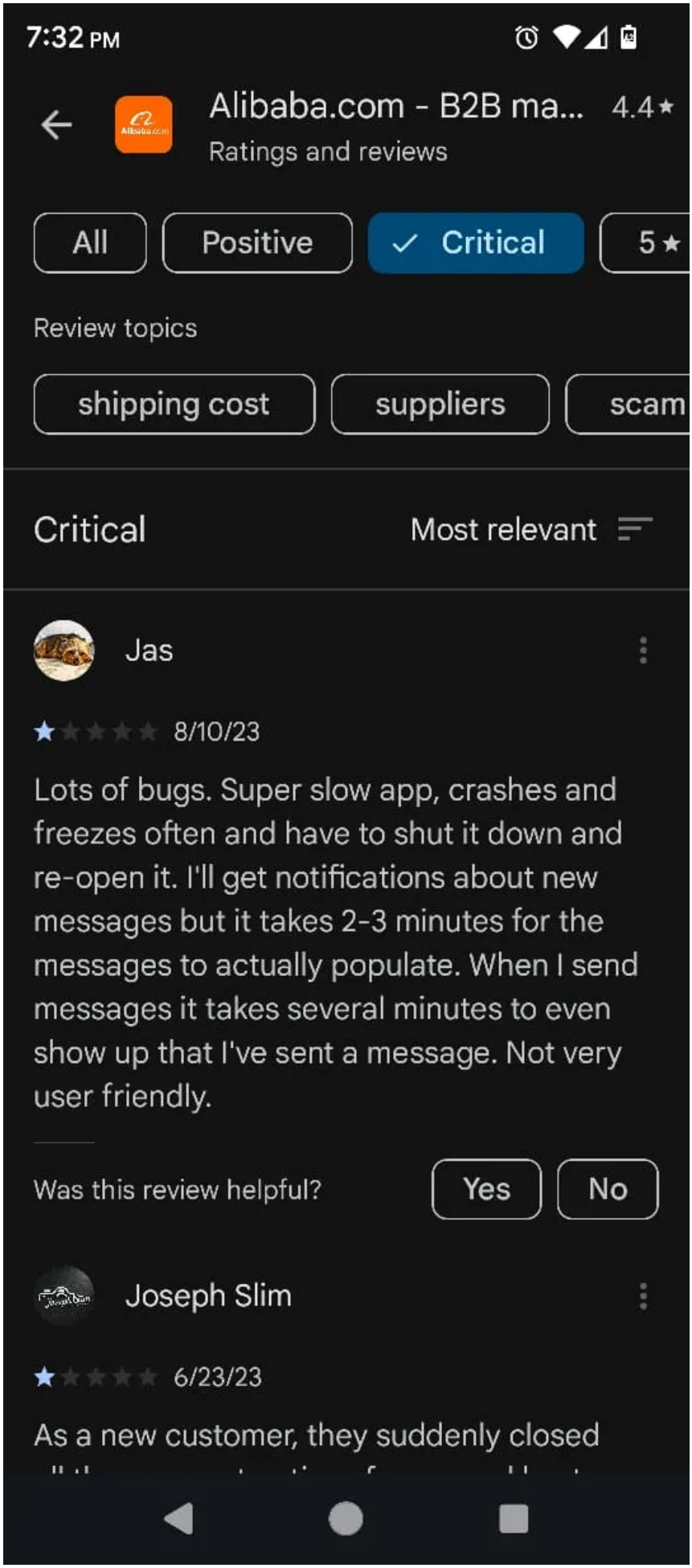
Sur la base de ces informations, vous pouvez décider d'installer ou d'ignorer l'application. AppBrain suggérera également des applications connexes afin que vous puissiez trouver une alternative qui a un bon score et moins d'autorisations.

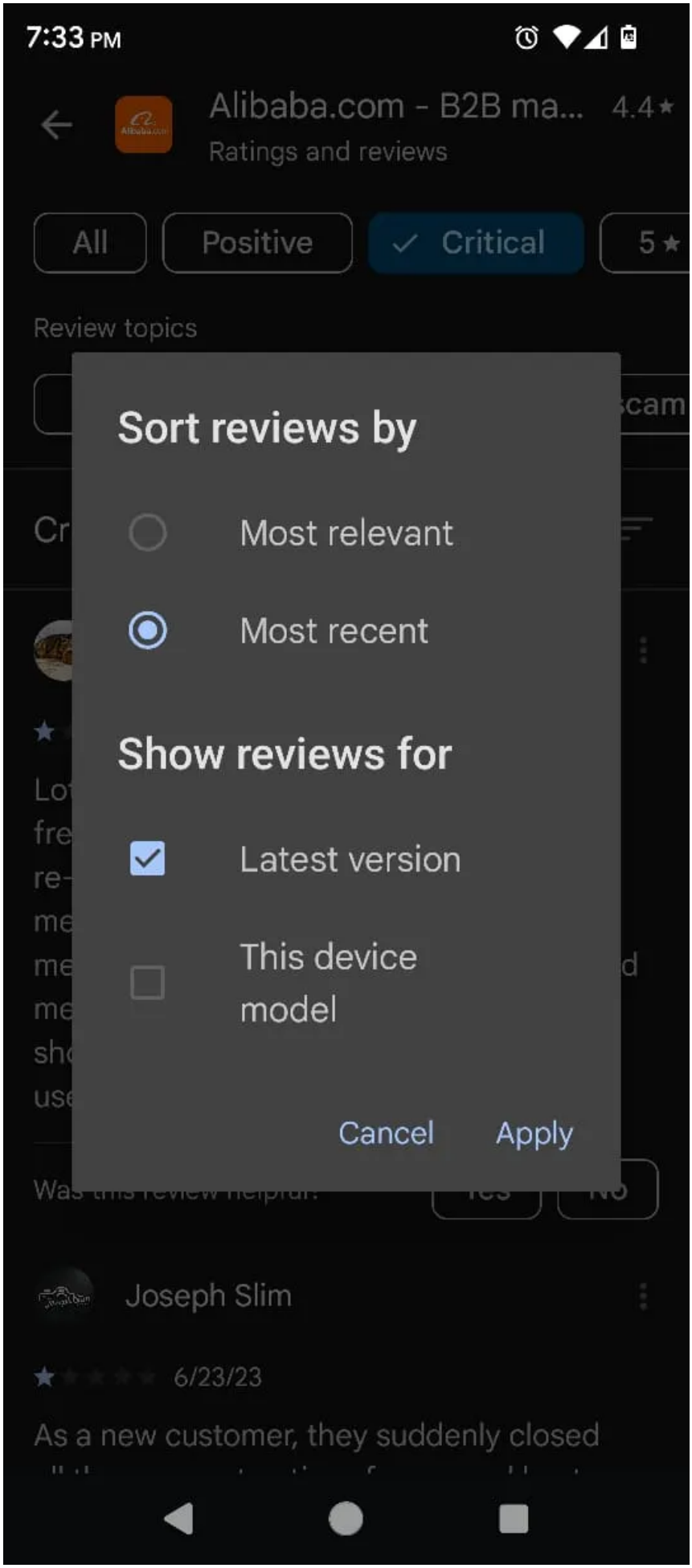
4. Consultez la page de description de l'application

Vérifier si une application fait ce qu'elle prétend faire est un bon moyen d'éliminer les applications problématiques.
Parfois, détecter un comportement anormal n'est pas facile. Un comportement considéré comme malveillant dans une application peut être une fonctionnalité d'une autre application.
Portez une attention particulière lorsque vous jetez un coup d'œil à la page de liste de l'application et utilisez ces conseils:

- Au lieu de regarder le nombre d'étoiles, lisez les critiques et faites attention à ce que les utilisateurs disent.
  Consultez les critiques et les **critiques les plus récentes** pour la **dernière version**. Certains développeurs achètent de fausses critiques, mais vous pouvez repérer ces éloges génériques.


7:31 PM
Alibaba.com - B2B marketplace
Alibaba Mobile
4.4★
2M reviews
57 MB
3+
Rated for 3+
Install
Alibaba.com
GLOBAL TRADE ON THE GO!
About this app
A world-leading B2B marketplace
#2 top free in shopping
Online market
Data safety
Safety starts with understanding how developers collect and share your data.


7:32 PM
Alibaba.com - B2B ma... 4.4★
Ratings and reviews
All
Positive
✓ Critical
5★
Review topics
shipping cost
suppliers
scam
Critical
Most relevant
Jas
8/10/23
Lots of bugs. Super slow app, crashes and freezes often and have to shut it down and re-open it. I'll get notifications about new messages but it takes 2-3 minutes for the messages to actually populate. When I send messages it takes several minutes to even show up that I've sent a message. Not very user friendly.
Was this review helpful?
Yes
No
Joseph Slim
6/23/23
As a new customer, they suddenly closed


7:33 PM
Alibaba.com - B2B ma... 4.4★
Ratings and reviews
All
Positive
Critical
5★
Review topics
Sort reviews by
Most relevant
Most recent
Show reviews for
Latest version
This device model
Cancel
Apply
Joseph Slim
6/23/23
As a new customer, they suddenly closed

- La description doit mettre en évidence et décrire les principales caractéristiques de l'application.
  Recherchez des signes de professionnalisme, y compris une structure de phrase appropriée, une grammaire propre et un manque de fautes d'orthographe.
  Un développeur réputé expliquera généralement les principales fonctionnalités au lieu de simplement les énumérer, et la plupart incluent également un lien de commentaires
- La politique du Play Store suggère que les captures d'écran doivent montrer les fonctionnalités les meilleures et les plus essentielles de votre application.
  Si la capture d'écran est volée dans la liste légitime, montrant des images plus généralisées de l'interface, c'est un signe d'avertissement.
- Jetez un coup d'œil rapide à la date de sortie de l'application et au nombre de personnes qui l'ont téléchargée.
  Une application récemment publiée par un petit développeur ne devrait pas avoir un grand nombre de téléchargements, et cela indique de faux téléchargements.
- Vérifiez le nom du développeur juste en dessous du nom de l'application.
  Vérifiez les autres applications qu'il a publiées, et si vous voyez une seule application (en particulier avec une incompatibilité dans le nombre de téléchargements et la date de publication), alors méfiez-vous.
- Pour voir si une application est une imitation, vérifiez l'orthographe.
  Par exemple, WhatsApp Messenger est développé par WhatsApp LLC.
  Si vous voyez « WhatsUp » ou « WhatzUp Messenger », fuyez!
- Si une application collecte et transmet des données personnelles ou sensibles de quelque manière que ce soit, elle doit le déclarer dans la politique de confidentialité. Au bas de chaque liste d'applications, il y a une section intitulée **Politique de confidentialité**.
  S'il n'y a pas une telle section ou un copier-coller générique, c'est un drapeau rouge.

5. Toujours installer les mises à jour du système

Google publie des mises à jour de sécurité mensuelles pour Android.
Idéalement, vous devriez installer les mises à jour dès leur arrivée, car elles protègent votre appareil contre les vulnérabilités spécifiques que les applications malveillantes tentent d'exploiter.

Cependant, tous les fabricants de mobiles ne publient pas de mises à jour en temps opportun.
Ainsi, votre décision d'achat avec votre prochain téléphone devrait tenir compte de la question de savoir si l'appareil bénéficiera d'un support pendant au moins deux ans de mises à niveau majeures, ainsi que de mises à jour de sécurité périodiques.

6. Évitez les applications et les liens clickbait

Ce point est une extension de tous les points énumérés ci-dessus, mais il est toujours assez important.
En tant que smartphone ou internaute, il est idéal de développer un sens de l'identification des pièges à clics.

Il existe des développeurs d'applications et de sites qui ont identifié certains besoins des utilisateurs, comme la conversion d'un PDF au format Excel, et ils utilisent ces mots-clés comme piège à clics parce qu'un grand nombre de personnes recherchent ces termes. Ainsi, avec leurs fausses applications et liens, ils sont généralement payés pour des clics ou des vues, ou ils peuvent essayer de vous pirater.

Vous pouvez détecter et éviter les pièges à clics sur votre téléphone Android en suivant les conseils que nous avons mentionnés, y compris le suivant.
Cependant, nous vous invitons à viser à faire de cette compétence une seconde nature pour rester en sécurité dans l'Internet sauvage et sauvage.

7. Utilisez un antivirus

Le dernier conseil est assez évident mais souvent ignoré.
Une application antivirus peut vous aider au cas où vous oublieriez de prendre vos mesures de précaution.
Il peut agir comme votre deuxième ligne de défense.
Vous avez beaucoup d'excellentes applications antivirus gratuites pour Android que vous pouvez installer.
La plupart de ces applications ne nécessitent qu'une configuration initiale, et elles fonctionnent en arrière-plan à partir de là.

Évitez les applications d'arnaque évidentes

Google fait de son mieux pour éloigner les applications malveillantes.
Il modifie fréquemment la politique du Store et interdit les applications qui enfreignent ces directives.
Si vous prenez les précautions décrites ici, vous êtes susceptible de rester en sécurité.

Ces conseils sont une combinaison d’étapes automatiques et manuelles afin que cela ne semble pas être une tâche fastidieuse.
Certains de ces conseils deviendront même un instinct pour vous, ne nécessitant aucun effort conscient avec le temps.

Recherche et mise en page:
Michel Cloutier
CIVBDL
20230904
"C'est ensemble qu'on avance"