

Les applis malveillantes sont au smartphone ce que les virus sont à un PC Windows. Elles prennent souvent pour cible les données personnelles ou bancaires. Parfois, elles cherchent à vous extorquer de l'argent. Par ailleurs, il existe des malwares par SMS qui vous abonnent, ni vu ni connu, à des SMS payants. Ces applis malveillantes font parfois leur apparition dans les boutiques d'applis. Elles se présentent parfois sous une forme innocente (logiciel photo, jeu...). Il existe aussi de fausses applis bancaires.

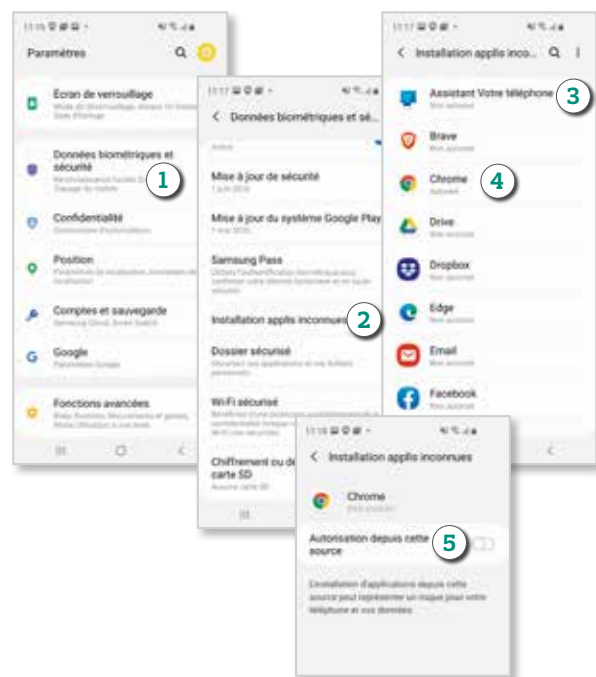
4.1 TÉLÉCHARGEMENTS SÉCURISÉS

Pour limiter le risque d'applis malveillantes, mieux vaut télécharger uniquement sur les boutiques officielles. Chez Apple, le risque est faible. Si l'iPhone n'a pas été débridé (jailbreak), il est impossible d'y installer d'autres applis que celles de l'App Store. Par défaut, Android empêche de s'aventurer en dehors du Play Store mais cette restriction peut être levée. Vérifiez donc dans les paramètres que les applis de «sources inconnues» ne peuvent pas être installées.



Android

1. Allez dans **Paramètres** et appuyez sur **Données biométriques et sécurité**.
2. Appuyez sur **Installation applis inconnues**.
3. Vérifiez que **Non autorisé** figure partout.
4. Sélectionnez une appli où **Autorisé** s'affiche.
5. Désactivez le curseur dans **Autorisation depuis cette source**.



SMS dangereux

Des personnes mal intentionnées tentent parfois de vous faire installer des applis sur votre smartphone en vous envoyant des SMS ou des messages véreux par WhatsApp ou Messenger. Elles vous font croire, par exemple, à une mise à jour de sécurité pour une appli bancaire, nécessaire pour pouvoir continuer à l'utiliser. En empêchant, conformément aux étapes décrites ci-dessus, l'installation à partir de sources inconnues, vous éviterez d'installer par mégarde un malware après avoir reçu un message malveillant.

4.2 APPLIS INTRUSIVES

La probabilité que des applis nuisibles se retrouvent sur votre iPhone ou Android est faible si vous prenez les mesures décrites au point 4.1. Google et Apple surveillent leurs boutiques, mais sans garantie. En revanche, la probabilité d'une atteinte à votre vie privée est plus élevée. Avant d'installer une appli, mieux vaut prendre connaissance de ses conditions de respect de la vie privée, même si elles sont peu intelligibles. Il est aussi utile de lire des avis sur l'appli concernée. Méfiez-vous des applis gratuites provenant de pays non européens où la législation est moins stricte.

4.2a Contrôlez les droits d'accès

De nombreuses applis prennent des libertés avec la vie privée des utilisateurs. Elles copient par exemple le carnet d'adresses sans que ces données soient nécessaires à leur fonctionnement. Ne leur donnez pas trop facilement accès à vos données à caractère personnel. Le sens logique suffit la plupart du temps : il va de soi qu'une appli de navigation doit avoir accès à votre localisation. En revanche, il y a quelque chose qui cloche si une appli lampe de poche a besoin de votre carnet d'adresses. N'hésitez pas à lui en refuser l'accès. Les applis doivent solliciter votre consentement préalable avant d'accéder à certaines données. N'appuyez pas sur OK sans réfléchir, demandez-vous plutôt si l'accès aux données requises semble logique. Dans le doute, abstenez-vous.

Cher client d'Argenta, votre carte bancaire est périmée. Demandez d'urgence votre nouvelle carte sur x.co/bankkaart

Cher Julien, félicitations, vous avez gagné 1000 €. Allez sur <https://wx.com/789> pour vous enregistrer.

Votre PC banking ING a été bloqué suite à une tentative de connexion non autorisée. Consultez "Mon ING" sur x.co/ing

Par une simple recherche sur le web, vous arriverez peut-être à savoir s'il faut accepter l'accès demandé, ou la raison pour laquelle il est logique d'accorder l'accès. Vous serez aussi mis en garde contre les applis qui exigent trop de droits d'accès.

Android

Depuis Android 6.0, les applis doivent demander l'autorisation d'accéder aux éléments suivants du téléphone :

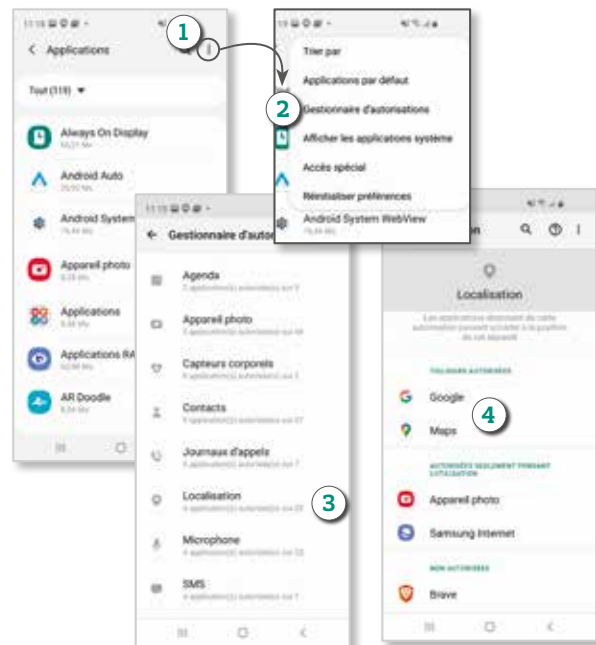
- ▶ agenda ;
- ▶ appareil photo ;
- ▶ contacts ;
- ▶ liste des conversations ;
- ▶ capteurs corporels ;
- ▶ localisation ;
- ▶ microphone ;
- ▶ espace de sauvegarde ;
- ▶ SMS ;
- ▶ téléphone.

Vous pouvez vérifier facilement quelles applis ont accès aux différents éléments.

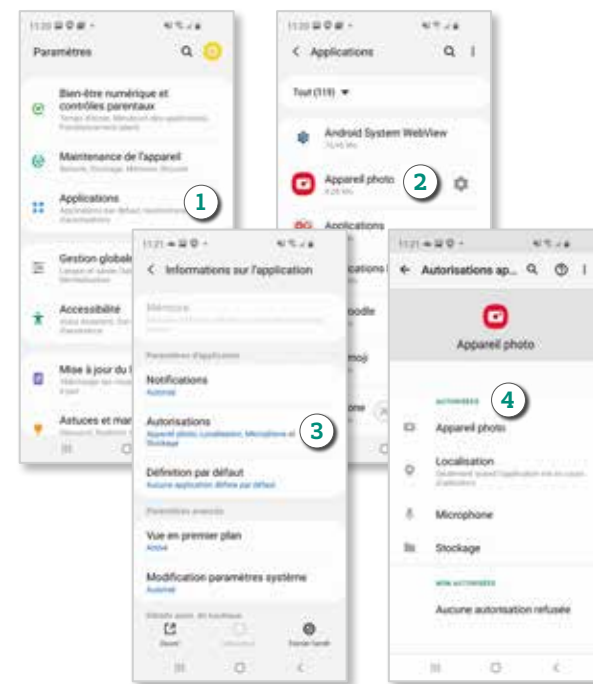


Android

1. Allez dans **Paramètres** et appuyez sur **Applications**, puis sur les trois points.
2. Sélectionnez **Gestionnaire d'autorisations**.
3. Pour chaque élément, le nombre d'applis qui y ont accès est indiqué. Appuyez sur un élément (par exemple Localisation).
4. Vous pouvez à présent autoriser ou refuser les droits d'accès pour chaque appli.



Android donne aussi, pour chaque appli, un aperçu des autorisations accordées. Vous pouvez ainsi évaluer si elles n'ont pas trop de droits.





Android

1. Allez dans **Paramètres** et appuyez sur **Applications**.
2. Choisissez une application.
3. Appuyez sur **Autorisations**.
4. Appuyez sur un élément et choisissez **Autoriser** ou **Refuser**.

iOS

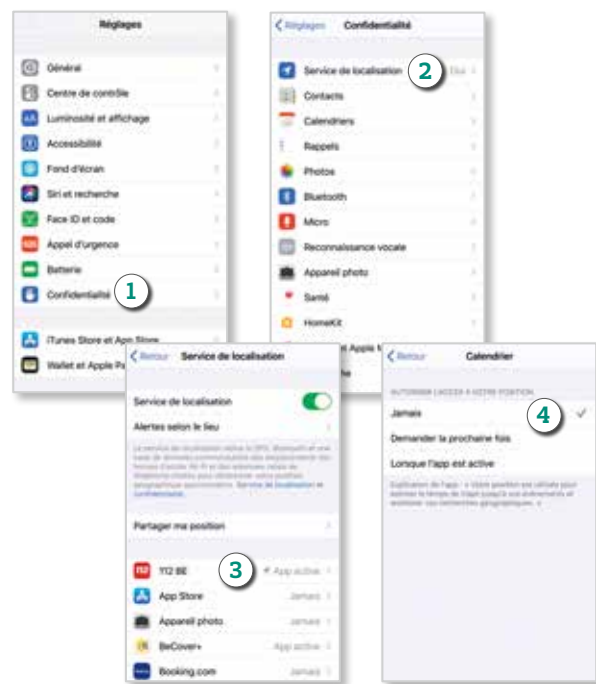
Dans iOS, les applis peuvent demander l'accès aux éléments suivants :

- ▶ localisation ;
- ▶ contacts ;
- ▶ agenda ;
- ▶ souvenirs ;
- ▶ photos ;
- ▶ Bluetooth ;
- ▶ microphone ;
- ▶ reconnaissance vocale ;
- ▶ appareil photo ;
- ▶ santé ;
- ▶ logement ;
- ▶ bibliothèque de médias ;
- ▶ exercice et condition.



iOS

1. Allez dans **Réglages** et appuyez sur **Confidentialité**.
2. Appuyez sur un élément.
3. Les applis qui y ont accès s'affichent.
4. Sélectionnez l'appli et, si vous le souhaitez, limitez l'accès.



Vous pouvez aussi vérifier les autorisations pour chaque appli et la recadrer si vous avez l'impression que vous lui avez octroyé trop de droits.



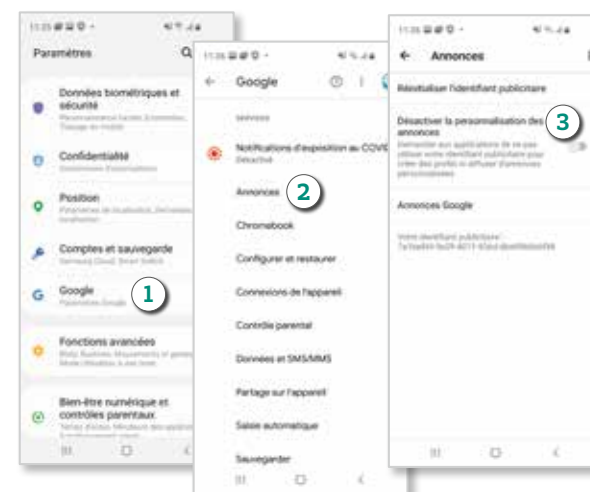
iOS

1. Allez dans **Réglages** et faites défiler le menu jusqu'à l'appli, par exemple «Dictaphone».
2. Appuyez sur un élément, par exemple «Position».
3. Faites passer l'accès à la position de «Lorsque l'app est active» à «Jamais».



4.2b Pas de suivi publicitaire

Tout comme les sites web, les applis aiment en savoir plus sur leurs utilisateurs. Les sites placent pour cela des cookies sur l'ordinateur. Il en va autrement sur les smartphones: ils disposent d'un identifiant publicitaire spécial, un code unique qui ne permet pas de remonter à l'appareil. Toutefois, il est encore possible de déterminer qui se cache derrière un profil détaillé. Mieux vaut dès lors limiter l'accès à cet identifiant.



Android

1. Allez dans **Paramètres** et appuyez sur **Google**.
2. Choisissez **Annonces**.
3. Activez le curseur dans **Désactiver la personnalisation des annonces**.



iOS

1. Allez dans **Réglages** et choisissez **Confidentialité**.
2. Faites défiler le menu jusqu'en bas et appuyez sur **Publicité**.
3. Activez le curseur dans **Suivi publicitaire limité**.



4.3 RESTREINDRE CERTAINES APPLIS ET SITES

Les iPhones et les appareils Android offrent la possibilité de restreindre certaines applis dans un cadre familial, de manière à éviter que les enfants soient exposés à des contenus inappropriés. Dans iOS, les possibilités sont bien plus larges que dans Android.

Android

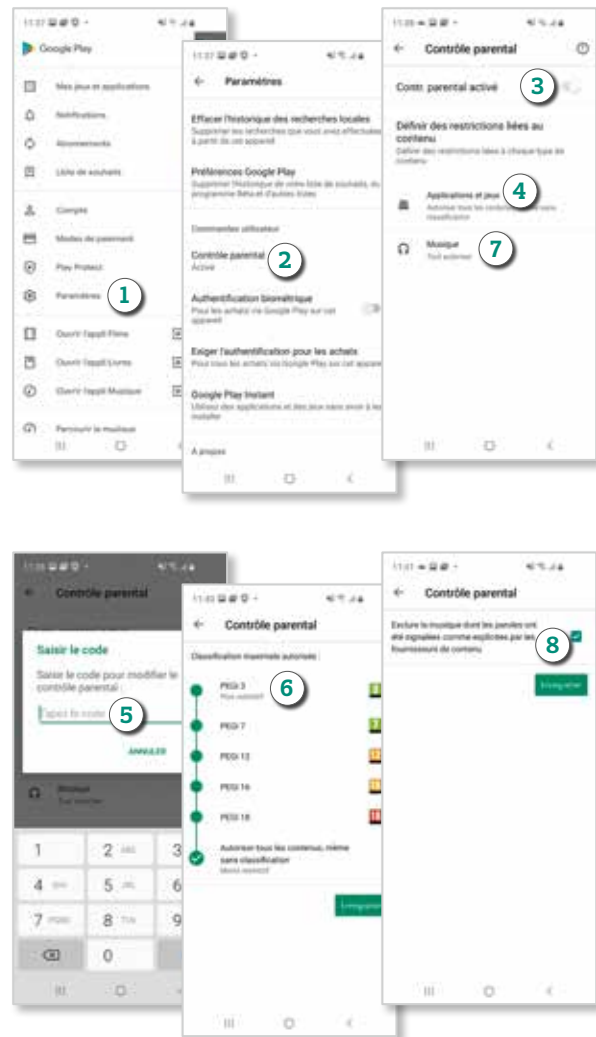
Dans Android, seuls les paramètres dans le Google Play Store peuvent être adaptés.



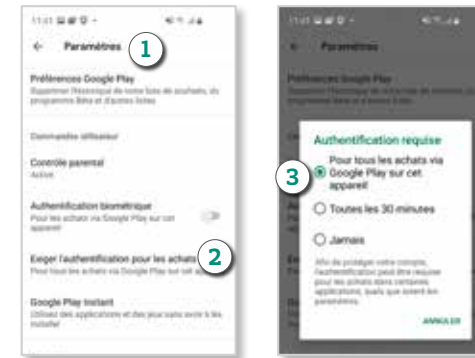
Android

Google Play Store

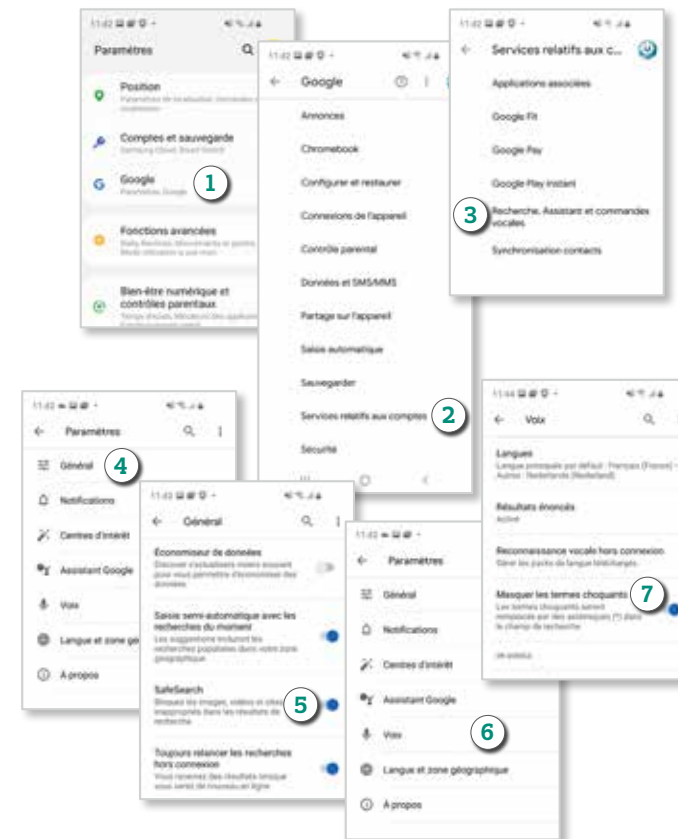
1. Ouvrez le Play Store, puis le menu, et appuyez sur **Paramètres**.
2. Sélectionnez **Contrôle parental**.
3. Veillez à ce que le curseur soit activé.
4. Appuyez sur **Applications et jeux**.
5. Choisissez un code PIN parental pour éviter qu'un enfant puisse modifier le paramètre.
6. Déterminez la restriction qui doit s'appliquer ici.
7. Cochez éventuellement l'option pour filtrer les paroles de chansons obscènes. Cela ne concerne que les morceaux de musique achetés via Google Play Musique.



Vous pouvez par ailleurs exiger qu'une authentification ait lieu avant tout achat dans le Google Play Store.



Android a aussi la fonction Google SafeSearch, qui supprime les sites et images inadéquats des résultats de recherche dans Chrome.



Android



Google Play Store

1. Ouvrez le Play Store et allez dans **Paramètres**.
2. Appuyez sur **Exiger l'authentification pour les achats**.
3. Choisissez **Pour tous les achats via Google Play sur cet appareil**.



Android



Google Play Store

1. Allez dans **Paramètres** et appuyez sur **Google**.
2. Appuyez sur **Services relatifs aux comptes**.
3. Choisissez **Recherche, Assistant et commandes vocales**.
4. Choisissez **Général**.
5. Faites défiler le menu vers le bas et activez le curseur de **SafeSearch**.
6. Revenez un pas en arrière et choisissez **Voix**.
7. Activez le curseur de **Masquer les termes choquants**.



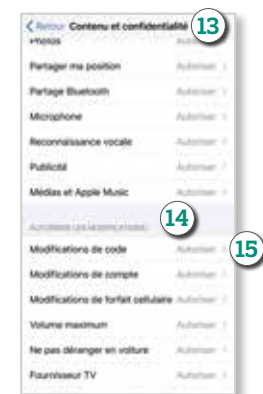
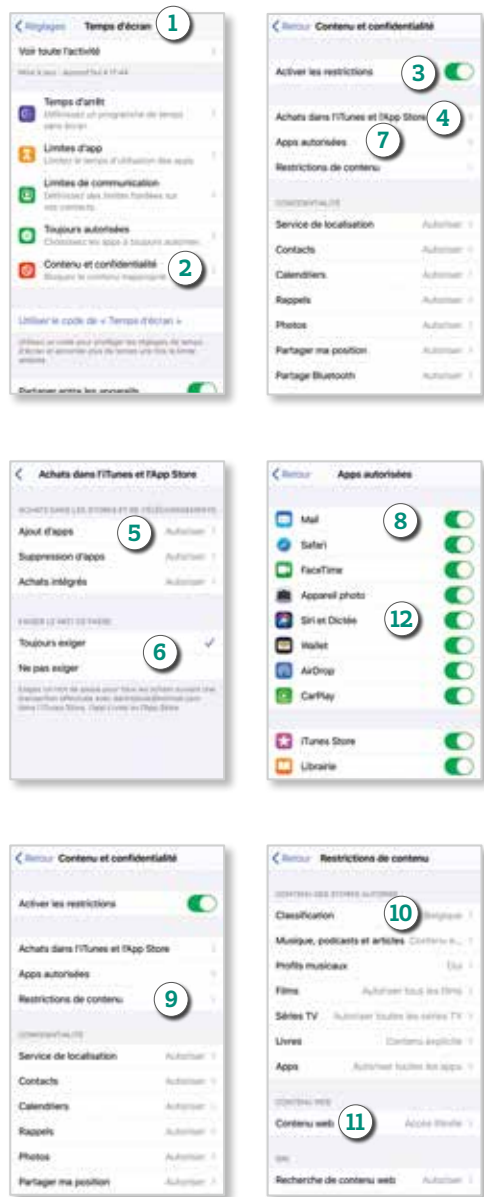
iOS

App Store

1. Allez dans **Réglages** et appuyez sur **Temps d'écran**.
2. Choisissez **Contenu et confidentialité**.
3. Activez le curseur.
4. Appuyez sur **Achats dans l'iTunes et l'App Store**.
5. Déterminez si l'installation et la suppression d'applis ou les achats dans une appli sont autorisés.
6. Instaurez au besoin un mot de passe pour ces opérations.
7. Revenez un pas en arrière et appuyez sur **Apps autorisées**.
8. Déterminez les applis pouvant être affichées sur le téléphone.
9. Revenez un pas en arrière et appuyez sur **Restrictions de contenu**.
10. Instaurez au besoin des restrictions d'âge pour l'achat de morceaux de musique, de films, de livres, etc.
11. En choisissant, dans **Contenu web**, l'option **Limiter les sites web pour adultes**, vous limiterez par exemple l'accès aux sites web réservés aux plus de 18 ans. ▶

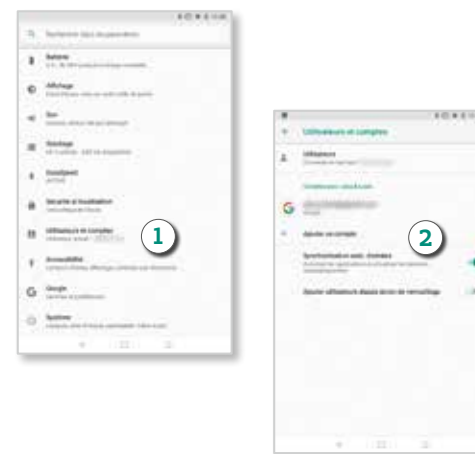
iOS

Apple offre de nombreuses options pour restreindre les réglages, les applis, la musique, les podcasts, etc. Vous pouvez par exemple éviter que le code d'accès soit modifié, que des achats soient effectués dans l'App Store ou que des sites pour adultes soient consultés.



4.3a Partage de tablette

De nombreuses familles se partagent la même tablette. Vous pouvez attribuer un compte personnel avec ses propres paramètres à plusieurs personnes partageant la même tablette (ou le même smartphone) Android. Certains fabricants ont désactivé cette option, qui n'existe pas sur iOS.



Android

1. Allez dans **Paramètres** et appuyez sur (Comptes >) Utilisateurs.
2. Choisissez **ajouter un compte** pour créer un nouveau compte.