

Malafide apps zijn voor smartphones wat virussen zijn voor een Windows-pc. Ze hebben het vaak gemunt op persoonlijke, inlog- of bankgegevens. Ook proberen ze je soms ergens voor te laten betalen. Verder is er sms-malware die mensen ongemerkt abonneert op een betaald sms-abonnement. De apps duiken af en toe op in de appstores. Malafide apps zijn soms vermomd als onschuldig ogende apps, bijvoorbeeld een fotobewerker of game. Ook zijn er nep-bankapps.

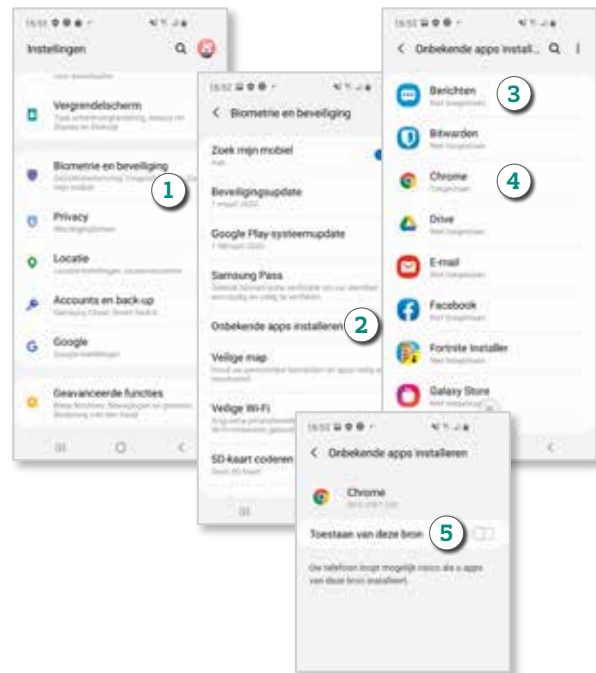
4.1 VEILIG DOWNLOADEN

Om het risico op malafide apps te beperken, is het belangrijk om alleen te downloaden via de officiële appstores. Bij Apple is het risico op schadelijke apps niet zo groot. Zonder de iPhone te kraken ("jailbreaken"), is het niet mogelijk om buiten de App Store apps te installeren. Android staat het standaard niet toe om buiten de Google Play Store om te gaan, maar dat kun je wel wijzigen. Controleer voor de zekerheid bij de instellingen dat apps uit "onbekende bronnen" niet geïnstalleerd mogen worden.



Android

1. Ga naar **Instellingen**, tik op **Biometrie en beveiliging**.
2. Tik op **Onbekende apps installeren**.
3. Controleer of overall **Niet toegestaan** staat.
4. Selecteer een app waar **Toegestaan** staat.
5. Zet het schuifje uit bij **Toestaan van deze bron**.



Gevaarlijk sms'je

Kwaadwillenden proberen soms apps geïnstalleerd te krijgen op smartphones door malafide sms'jes, WhatsApp- of Facebook Messenger-berichten te versturen. Ze beloven bijvoorbeeld een beveiligingsupdate voor een bankapp, noodzakelijk om via de app te kunnen blijven bankieren. Door via het voorgaande stappenplan het installeren uit onbekende bronnen uit te schakelen, voorkom je dat per ongeluk malware wordt geïnstalleerd na ontvangst van een malafide bericht.

4.2 PRIVACYSCHENDE APPS

De kans dat je echt kwaadaardige apps op je iPhone of Android-toestel krijgt, is niet zo heel groot als je de maatregelen uit paragraaf 4.1 hebt genomen. Zowel Google als Apple houdt zijn appstore in de gaten, al is er geen garantie. Er is een grotere kans op privacyschendingen. Voordat je een app installeert, is het belangrijk om de privacyvoorwaarden door te nemen, al zijn die vaak slecht leesbaar. Het lezen van recensies over een app is ook nuttig. Kijk extra uit bij gratis apps van buiten Europa, waar de privacywetgeving minder streng is.

4.2a Controleer de toegangsrechten

Veel apps nemen het niet zo nauw met de privacy van gebruikers. Ze kopiëren bijvoorbeeld het adresboek, zonder dat die gegevens nodig zijn voor de functionaliteiten van de app. Om te voorkomen dat apps met allerlei gegevens aan de haal gaan, is het belangrijk niet zomaar toegang te geven tot persoonlijke gegevens. Daarbij volstaat meestal logisch nadenken: het spreekt voor zich dat een navigatieapp toegang nodig heeft tot de locatie. Als een zaklamp-app toegang wil tot het adresboek, is er iets niet in de haak. Aarzel niet om toegang te weigeren. Apps moeten vooraf toegang vragen voor ze bij bepaalde gegevens kunnen. Tik niet gedachteloos op OK, maar beoordeel eerst of toegang tot de gevraagde gegevens logisch is. Bij twijfel, niet doen.

- Beste Argenta-klant, uw bankkaart is verouderd. Vraag dringend vóór 9 juli uw nieuwe kaart aan op x.co/bankkaart
- Beste Julien, proficiat, u hebt € 1000 gewonnen. Ga naar <https://wx.com/789> om u te registreren.
- Uw ING-internetbankieren werd geblokkeerd vanwege een ongeautoriseerde inlogpoging. Verifieer uw "Mijn ING" hier: x.co/ing

Via een zoekopdracht op internet kom je er soms achter of je de gevraagde toegang kunt accepteren. Er staat bijvoorbeeld waarom toegang tot onderdelen al dan niet logisch is. Ook wordt gewaarschuwd voor apps die te veel toegangsrechten vragen.

Android

Sinds Android 6.0 moeten apps toestemming vragen om toegang te krijgen tot de volgende onderdelen van de telefoon:

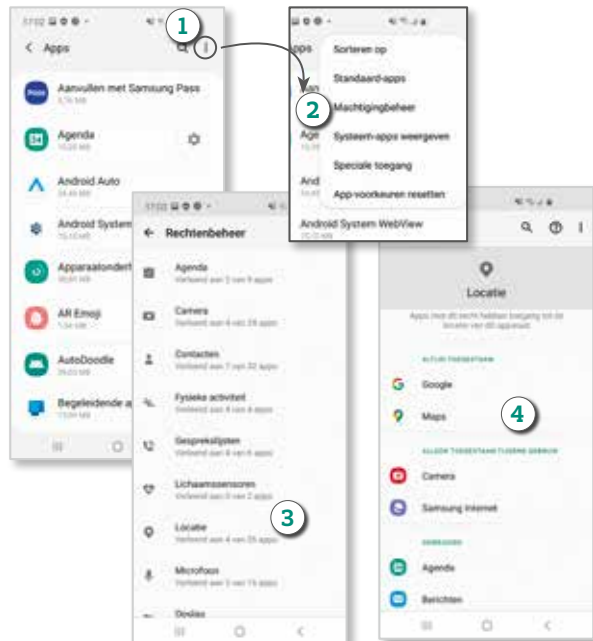
- ▶ Agenda's;
- ▶ Camera;
- ▶ Contacten;
- ▶ Gesprekkenlijst;
- ▶ Lichaamssensoren;
- ▶ Locatie;
- ▶ Microfoon;
- ▶ Opslagruimte;
- ▶ Sms;
- ▶ Telefoon.

Je kunt eenvoudig nagaan welke apps toegang hebben gekregen tot de verschillende onderdelen.

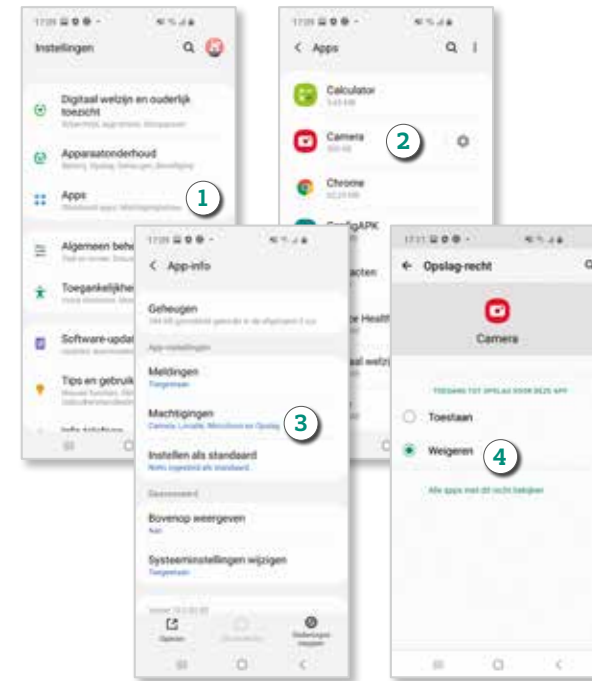


Android

1. Ga naar **Instellingen**, tik op **Apps** en dan op de drie stippen.
2. Selecteer **Machtigingbeheer**.
3. Per onderdeel staat vermeld hoeveel apps toegang hebben. Tik op een onderdeel (bijvoorbeeld Locatie).
4. Nu is het mogelijk de toegangsrechten per app aan of uit te zetten.



Android geeft ook per app een overzicht van verleende machtigingen. Zo is voor individuele apps te beoordelen of ze niet te veel rechten hebben.





Android

1. Ga naar **Instellingen**, tik op **Apps**.
2. Kies een app.
3. Tik op **Machtigingen**.
4. Tik op een onderdeel en kies **Toestaan** of **Weigeren**.

iOS

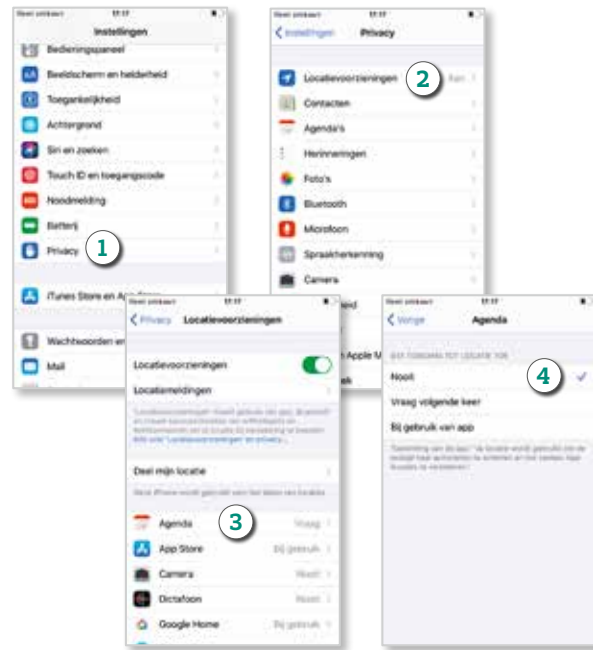
Apps kunnen in iOS toegang vragen tot de volgende onderdelen:

- ▶ Locatie;
- ▶ Contacten;
- ▶ Agenda's;
- ▶ Herinneringen;
- ▶ Foto's;
- ▶ Bluetooth;
- ▶ Microfoon;
- ▶ Spraakherkenning;
- ▶ Camera;
- ▶ Gezondheid;
- ▶ Woning;
- ▶ Mediabibliotheek;
- ▶ Beweging en conditie.



iOS

1. Ga naar **Instellingen** en tik op **Privacy**.
2. Tik op een onderdeel (bv. Locatievoorzieningen).
3. Hier staat welke apps toegang hebben.
4. Selecteer de app en beperk indien gewenst de toegang.



Je kunt ook per app bekijken welke machtigingen er zijn. Zo kun je snel een individuele app tot de orde roepen als je het idee hebt dat die te veel rechten heeft.



iOS

1. Ga naar **Instellingen** en scrol naar de app, bijvoorbeeld Dictafon.
2. Tik op een onderdeel, bijvoorbeeld Locatie.
3. Verander toegang tot locatie van "Bij gebruik van app" naar "Nooit".

4.2b Geen reclametracking

Apps willen net als websites graag weten wie hun gebruikers zijn. Websites plaatsen daartoe cookies op de pc. Op smartphones werkt dit anders. Ze beschikken over een speciaal advertentie-ID: een unieke code die niet te herleiden is tot het toestel. Van een gedetailleerd profiel is het echter alsnog mogelijk te achterhalen wie daarachter schuilgaat. Je kunt toegang tot dat ID daarom beter afschermen.



Android

1. Ga naar **Instellingen** en tik op **Google**.
2. Kies voor **Advertenties**.
3. Zet het schuifje bij **Afmelden voor personalisatie van advertenties** aan.



iOS

1. Ga naar **Instellingen** en kies voor **Privacy**.
2. Scrol naar beneden en tik op **Reclame**.
3. Zet het schuifje achter **Beperk reclametracking** aan.



4.3 APPS EN SITES AFSCHERMEN

Zowel iPhones als Android-toestellen hebben mogelijkheden om apps af te schermen in een gezinssituatie. Zo is te voorkomen dat kinderen inhoud te zien krijgen die niet geschikt voor ze is. De mogelijkheden in iOS zijn wel veel uitgebreider dan die in Android.

Android

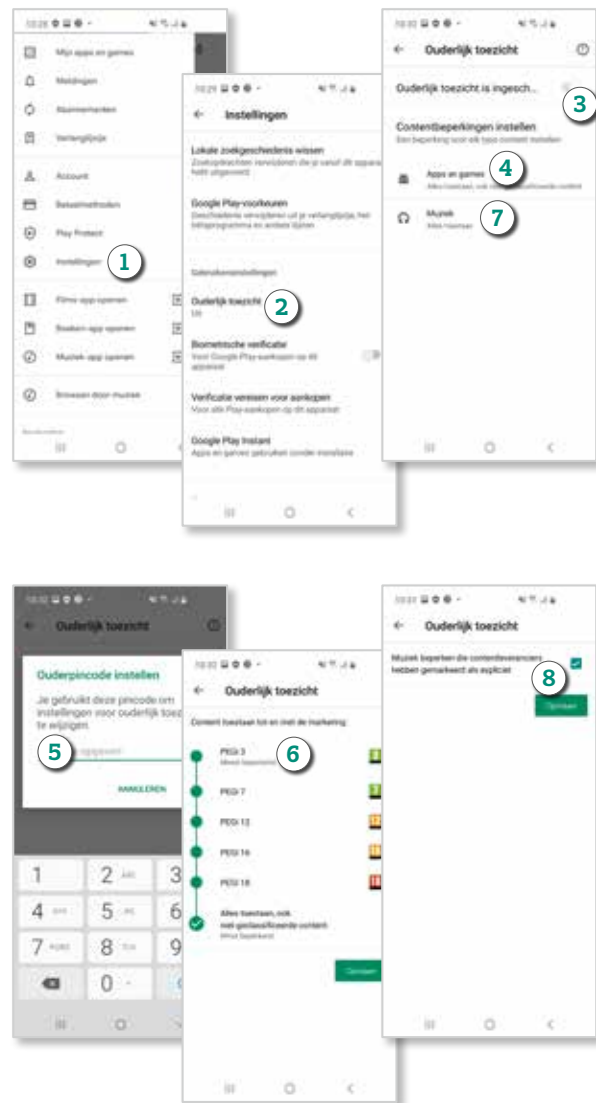
In Android zijn alleen de instellingen in de Google Play Store aan te passen.



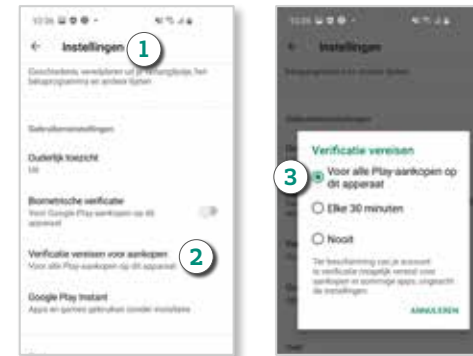
Android

Google Play Store

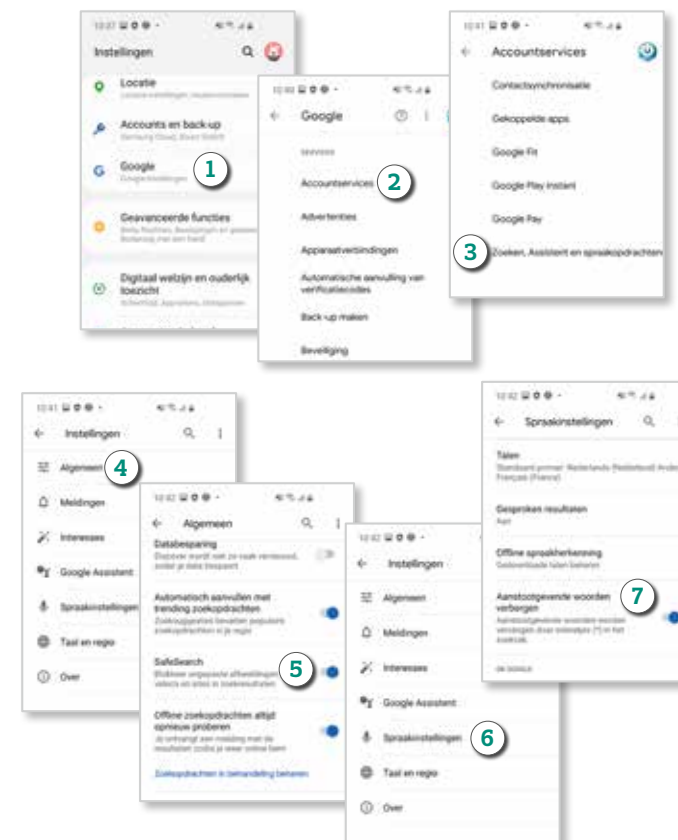
1. Open de Play Store, open het menu en tik op **Instellingen**.
2. Selecteer **Ouderlijk toezicht**.
3. Zorg dat het schuifje aan staat.
4. Tik op **Apps en Games**.
5. Kies een ouderpincode, om te voorkomen dat een kind de instelling kan wijzigen.
6. Bepaal hier welke restrictie er moet gelden.
7. Ga een stap terug en tik op **Muziek**.
8. Vink hier eventueel de optie aan om expliciete muziekteksten te filteren. Dit geldt alleen voor muziek die via Google Play Muziek wordt gekocht.



Verder kun je instellen dat er altijd een verificatie vereist is bij het doen van aankopen via de Google Play Store.



Android heeft verder de functie Google SafeSearch, die ongepaste sites en afbeeldingen weert uit zoekresultaten in Chrome.



Android



Google Play Store

1. Open de Play Store en ga naar **Instellingen**.
2. Tik op **Verificatie vereisen voor aankopen**.
3. Kies **Voor alle Play-aankopen op dit apparaat**.



Android



Google Play Store

1. Ga naar **Instellingen**, tik op **Google**.
2. Tik op **Accounts en services**.
3. Kies **Zoeken, Assistent en spraakopdrachten**.
4. Kies voor **Algemeen**.
5. Scrol naar beneden en zet het schuifje bij **SafeSearch** aan.
6. Ga een stapje terug en kies **Spraakinstellingen**.
7. Zet het schuifje bij **Aanstootgevende woorden verbergen** aan, om ze te verbergen.



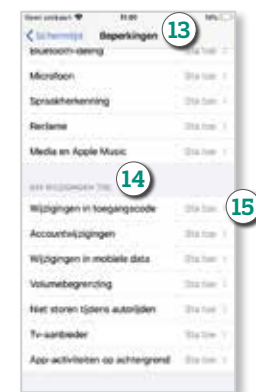
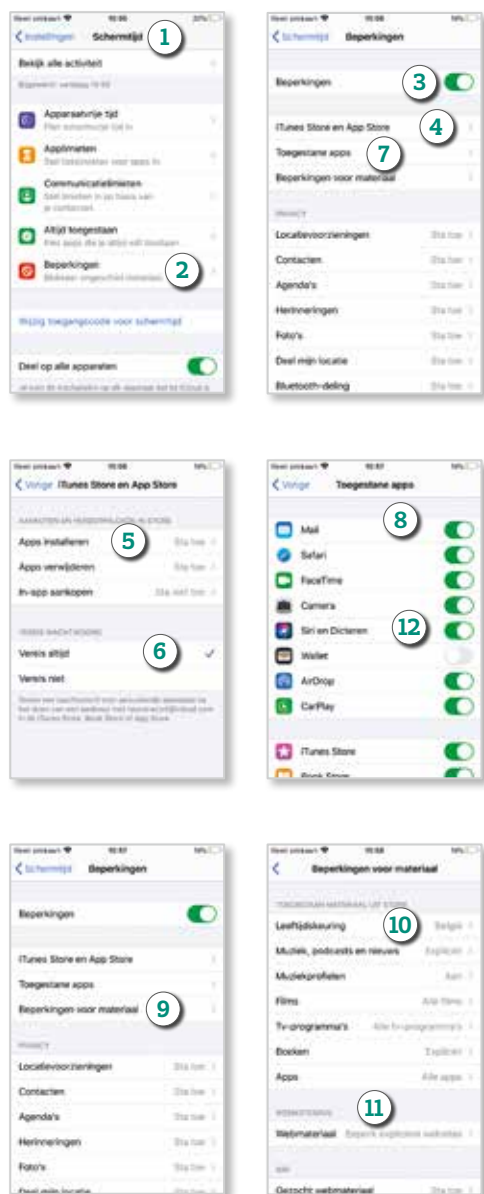
iOS

App Store

1. Ga naar **Instellingen**, tik op **Schermtijd**.
2. Kies voor **Beperkingen**.
3. Zet het schuifje aan.
4. Tik op **iTunes Store en App Store**.
5. Bepaal of het installeren en verwijderen van apps of in-app-aankopen zijn toegestaan.
6. Stel in of er een wachtwoord vereist is voor deze handelingen.
7. Ga een stap terug en tik op **Toegestane apps**.
8. Bepaal welke apps getoond mogen worden op de telefoon.
9. Ga een stap terug en tik op **Beperkingen voor materiaal**.
10. Stel in of er leeftijdsbeperkingen moeten gelden voor het aanschaffen van muziek, films, boeken enzovoort.
11. Door bij **Webmateriaal** te kiezen voor **Beperk expliciete websites**, wordt toegang tot bijvoorbeeld 18+-websites beperkt.

iOS

Apple biedt veel opties om instellingen, apps, muziek, podcasts enzovoort af te schermen. Zo kun je bijvoorbeeld voorkomen dat de toegangscode wordt gewijzigd, dat er aankopen worden gedaan via de App Store of dat er expliciete sites worden bekeken.



12. Je kunt ook aan spraakassistent Siri en Game Center beperkingen opleggen.

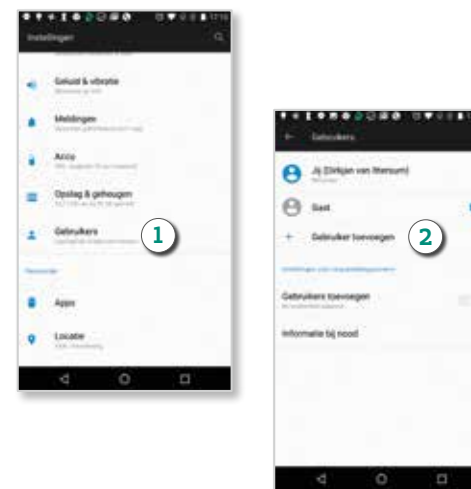
13. Ga terug naar **Beperkingen**.

14. Scrol naar beneden en kijk onder "Sta wijzigingen toe".

15. Hier is onder meer in te stellen of de toegangscode of wachtwoorden voor accounts gewijzigd mogen worden.

4.3a Tablet delen

In veel gezinnen wordt de tablet gedeeld. Op Android-tablets (en -smartphones) kun je meerdere personen op één apparaat elk een eigen account met eigen instellingen geven. Sommige fabrikanten van Android-toestellen hebben deze optie uitgeschakeld. Ook iOS heeft deze functie helaas niet.



Android

1. Ga naar **Instellingen**, tik op **(Accounts >) Gebruikers**.

2. Kies **Gebruiker toevoegen** om een nieuw account aan te maken.