Android veiliger

Smart, maar ook safe!

Android mag dan niet bekendstaan als het veiligste besturingssysteem, het blijkt wel erg populair: zo'n 75 procent van alle smartphones in Nederland draait op Googles systeem, en wereldwijd is dat zelfs meer dan 85 procent. In dit artikel geven we u een aantal tips waarmee u met Android toch ook veilig aan de slag kunt.

Tekst Toon van Daele

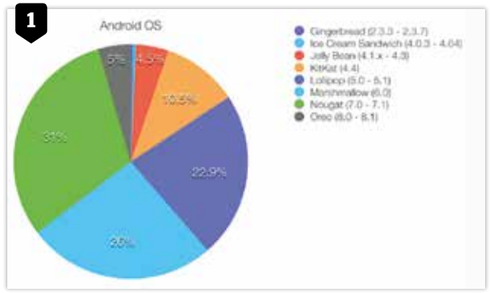
Een gerust gevoel met Android

In vergelijking met Apples iOS is Googles Android de overduidelijke winnaar – althans, op het gebied van marktpenetratie. Wat betreft veiligheid moet Android echter nog steeds het onderspit delven, zoals bijvoorbeeld blijkt uit www.tiny.cc/andvsios. Dat is onder meer te wijten aan de hoge fragmentatiegraad van Android. Er zijn namelijk talloze verschillende toestellen met vaak uiteenlopende Android-versies op de markt **(afbeelding 1)** en elk toestel heeft zijn eigen onvolkomenheden en zwakheden. Bovendien is het updatemechanisme minder dwingend dan bij Apple. Gebruikers kunnen op een niet-geroot apparaat tevens probleemloos apps uit andere stores dan de officiële Play Store installeren.

Google zelf maakt zich echter sterk dat Android inmiddels net zo veilig is als iOS (zie ook www.tiny.cc/andsec). Mechanismen als Google Play Protect, zes (in plaats van twee) jaar ondersteuning van de Linux-kernel en een snellere uitrol van beveiligingsupdates ('project Treble') wijzen inderdaad op een grotere bewustwording van de veiligheidsproblematiek.

In de praktijk blijkt het echter vooral de gebruiker zelf die bepaalt hoe veilig zijn of haar Android-apparaat is, en als u de tips uit dit artikel ter harte neemt, dan hoeft u zich weinig zorgen te maken. We baseren ons hierbij op Android Oreo, maar de meeste tips gelden eveneens voor iets oudere varianten.

1



Vergrendeling

Met het oog op meer veiligheid hoort u er als gebruiker in elk geval voor te zorgen dat uw toestel niet zomaar kan worden gebruikt wanneer iemand het inschakelt. Dat regelt u via *Instellingen*, waar u *Beveiliging en locatie*, *Schermbeveiliging* kiest. Doorgaans kunt u, in oplopende volgorde van veiligheid, kiezen uit *Gezichtsontgrendeling*, *Patroon*, *Pincode* of *Wachtwoord* **(afbeelding 2)**. Tik zeker ook op het tandwielpictogram naast de optie *Schermbeveiliging* en kies *Automatisch vergrendelen*. U kunt hier dan instellen na hoeveel tijd nadat de slaapstand is ingegaan uw toestel automatisch wordt vergrendeld. Houd deze tijd zo kort mogelijk en stel ook de slaapstand zelf kort genoeg in. Dat laatste regelt u via *Instellingen*, *Weergave*, *Slaapstand*. Bij *Automatisch vergrendelen* treft u tevens een optie om het scherm onmiddellijk te vergrendelen wanneer u de aan-uitknop gebruikt.

Afhankelijk van uw toestel kunt u uw scherm ook ontgrendelen met een vingerafdruk; deze optie vindt u eveneens terug bij *Instellingen*, *Beveiliging en locatie*.

Android kent een hoge fragmentatiegraad (bron: PLUS QA, 2018).

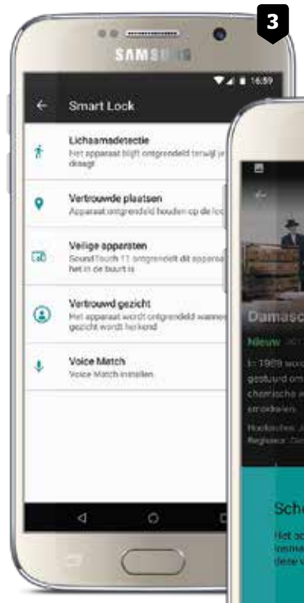
Smart Lock

Natuurlijk, beveiliging werkt alleen als u die daadwerkelijk gebruikt – en het voortdurend moeten intikken van een pincode of wachtwoord leidt er vaak toe dat gebruikers deze beveiliging weer uitschakelen. De Smart Lock-functie van Android zorgt ervoor dat uw toestel automatisch wordt ontgrendeld onder veilige voorwaarden, bijvoorbeeld wanneer het is verbonden met een specifiek bluetooth- of nfc-apparaat, zoals een smartwatch of het audiosysteem van uw auto, wanneer u zich thuis bevindt of zolang u het op uw lichaam draagt.

2

U stelt het in als volgt: ga naar *Instellingen*, *Beveiliging en locatie* en selecteer *Smart Lock*. Kies een of meer van de aangeboden opties, zoals *Lichaamsdetectie*, *Vertrouwde plaatsen*, *Veilige apparaten*, *Vertrouwd gezicht* of *Voice Match* **(afbeelding 3)**. Kiest u bijvoorbeeld voor *Vertrouwde plaatsen*, klik dan op *Vertrouwde plaats toevoegen*, zoom voldoende in op Google Maps en duid de gewenste locatie aan, zoals uw woning.

3



Smart Lock: veiligheid met meer comfort.

Scherm vastzetten

Met Android 5.0 werd tevens de functie 'scherm vastzetten' (screen pinning) geïntroduceerd. Hiermee kunt u het gebruik van het toestel tot één specifieke app beperken, wat veiliger is als u het toestel even door iemand anders laat gebruiken. Ook deze functie schakelt u in vanuit *Instellingen*, *Beveiliging en locatie*. Tik hier *Scherm vastzetten* aan en zet de schakelaar op *Aan*. Zorg dat hier ook *Vraag pin voor losmaken* is ingeschakeld.

4

Even die app vastpinnen, zodat uw kennis niet 'per ongeluk' iets anders doet …

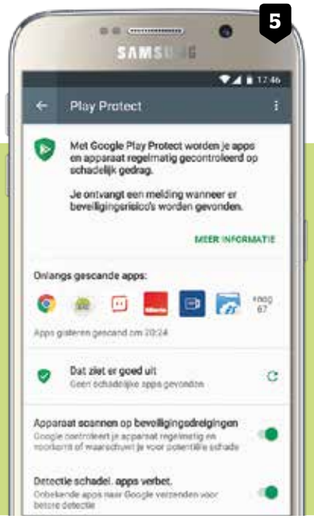
Vervolgens keert u terug naar het startscherm door op de Home-knop te drukken, waarna u de app opent die u wilt vastzetten. Terwijl die is geopend, drukt u opnieuw op de Home-knop, gevolgd door de Overzicht-knop (knopje met vierkantje, rechtsonder). Sleep het beeld naar boven: de zojuist geopende app staat nu vooraan in de lijst met actieve apps. Tik het pictogram met de punaise aan, rechtsonder in het scherm: de functie is nu actief **(afbeelding 4)**. Om die weer los te koppelen, drukt u tegelijkertijd op de toetsen Terug en Overzicht en houdt u die even ingedrukt, waarna u desgevraagd uw pincode invoert.

Apparaat vinden

Als u uw apparaat ergens verloren bent, het ergens in huis laat rondslingeren of het is gestolen, heeft Android een ingebouwd mechanisme waarmee u het niet alleen snel kunt lokaliseren, maar het ook kunt laten rinkelen en zelfs vergrendelen en wissen. Daartoe dient u wel de functie *Vind mijn apparaat* in te schakelen in de rubriek *Beveiliging en locatie*.

Bent u ooit op zoek naar uw apparaat, dan volstaat het naar www.android.com/find te surfen. Of u googelt gewoon naar *find my device*: als het goed is verschijnt de locatie dan zomaar bovenaan in de zoekresultaten. Of u zet hiervoor de app Find My Device in, als u vanaf een ander Android-toestel wilt zoeken.

5

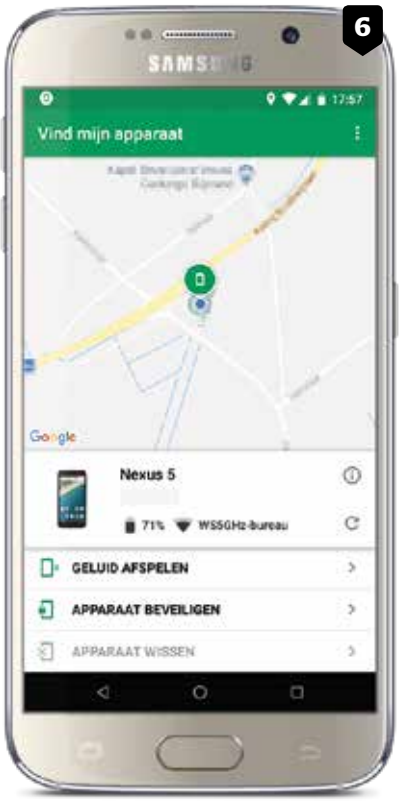


Play Protect

Sinds juli 2017 heeft Google de functie Play Protect gelanceerd, een soort beveiligingssuite die uit verschillende onderdelen bestaat, waaronder *Vind mijn apparaat* (zie verderop). Minder bekend is dat Play Protect uw smartphone ook van realtime monitoring voorziet. Deze functie controleert de geïnstalleerde apps continu en bij verdacht gedrag krijgt u een melding te zien. Play Protect is standaard ingeschakeld, maar het kan nooit kwaad het nog eens te checken: ga naar *Instellingen, Beveiliging en locatie* en kies *Google Play Protect*. We raden u aan hier beide opties in te schakelen: *Apparaat scannen op beveiligingsdreigingen* en *Detectie schadelijke apps verbeteren* **(afbeelding 5)**. Deze laatste optie zorgt ervoor dat informatie over apps die u buiten de Google Play Store om installeert (slecht idee: zie eveneens verderop) naar Google wordt gestuurd.

Volgens het onafhankelijke testbureau AV-Test hoort Play Protect wat malwaredetectie betreft niet meteen bij de beste van de klas, maar het is zeker raadzaam deze bescherming geactiveerd te laten.

APlay Protect: niet feilloos, maar absoluut zinvol.



Apparaat uit het oog verloren? Google vindt het snel terug!

U treft hier opties als *Geluid afspelen*, *Apparaat wissen en Apparaat beveiligen* (lees: vergrendelen en uitloggen van uw Google-account en desgewenst een bericht op het vergrendelingsscherm laten verschijnen) **(afbeelding 6)**.

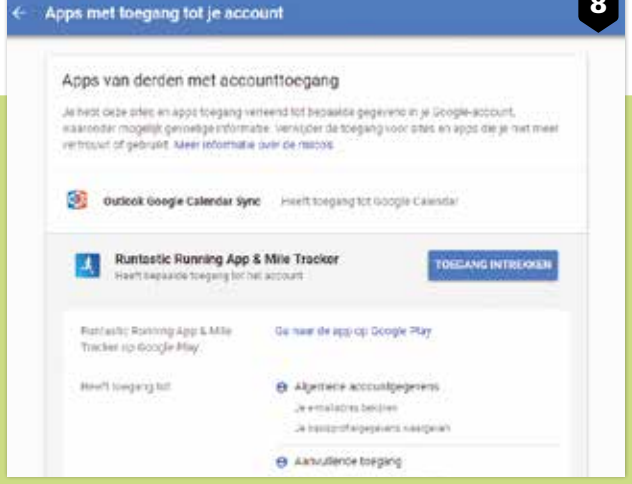
App-permissies

Al kunt u uw apparaat zo instellen dat ook het downloaden van apps buiten de officiële Play Store om mogelijk wordt, uit veiligheidsoverwegingen kunt u dat maar beter niet doen. Het is trouwens geen slecht idee om in de Play Store enkele *Beoordelingen & recensies* te lezen (inclusief het aantal downloads) en de *Contactgegevens van ontwikkelaar* even door te nemen.

Controleer vooraf ook de machtigingen die de app zich wil toe-eigenen. Open de pagina van de app in de Play Store, tik op *Meer lezen* (net boven *Beoordelingen & recensies*), scrol helemaal naar beneden en kies *Meer weergeven* bij *App-machtigingen*. Kunt u zich hierin vinden, dan mag u de app installeren. Normaliter krijgt u dan bij de eerste keer dat u de app opstart de vraag om de machtigingen toe te staan.

Echter, ook na de installatie is het mogelijk de app specifieke machtigingen te ontnemen. Ga naar *Instellingen*, *Apps en meldingen*, *Alle <x> apps bekijken*. Tik de app aan en kies *Machtigingen*, waarna u individuele machtigingen kunt in- en uitschakelen **(afbeelding 7)**. Houd er wel rekening mee dat sommige app-functies hierdoor mogelijk niet meer goed zullen werken.

Af en toe de machtigingen van de app(-updates) controleren kan zeker geen kwaad!



Verdachte of niet langer gebruikte apps en diensten? Weg ermee!

Google-account

Uw Google-account is natuurlijk nauw verweven met uw Android-apparaat, dus is het verstandig een aantal zaken te controleren die impact kunnen hebben op de veiligheid van dat account. Zo doet u er goed aan af en toe de apps en diensten te controleren die aan uw account gekoppeld zijn. Dat kan via https://myaccount.google.com/permissions. Items die u niet langer gebruikt, klikt u aan en haalt u weg met de knop *Toegang intrekken* **(afbeelding 8)**. Hetzelfde geldt voor apparaten die u niet langer in uw bezit hebt: surf naar https://myaccount.google.com/device-activity en haal overtollige apparaten weg. Treft u hier een toestel aan dat u nooit zelf hebt gebruikt, dan kunt u het best meteen het wachtwoord van uw Google-account wijzigen.

Het is sowieso verstandig om 'authenticatie in twee stappen' voor uw Google-account in te stellen. Surf naar www.google.com/landing/2step, klik op *Aan de slag* en volg de verdere instructies. Tot slot is het aan te raden een algehele veiligheidscontrole van uw Google-account uit te voeren: https://myaccount.google.com/security-checkup is hiervoor het aangewezen vertrekpunt.

Ten slotte

Neemt u alle bovenstaande tips ter harte, dan hoeft u zich nog maar weinig zorgen te maken. We gaan er dan wel van uit dat u de aangeboden updates altijd snel installeert en dat u uw apparaat niet 'root'. Immers, een geroot apparaat valt ook voor malafide doeleinden makkelijker te manipuleren.

Verder raden we u aan data op uw apparaat te versleutelen. Dat gaat zeer eenvoudig: ga opnieuw naar *Instellingen* en kies *Beveiliging en locatie*, waar u – mogelijk in een submenu – een optie als *Encryptie* of *Versleutelen* terugvindt. Selecteer die en volg de verdere instructies. De hele versleutelingsprocedure neemt al snel een uur in beslag.

Tot slot kunt u overwegen een antivirus-app te installeren, zoals Avast Mobile Security & Antivirus (www.tiny.cc/avamob) **(afbeelding 9)**, Bitdefender Antivirus Free (www.tiny.cc/bitmob) of AVL (www.tiny.cc/avlav). Houd er wel rekening mee dat zulke apps ook stroom verbruiken en dat ze doorgaans advertenties bevatten.

Een extra antivirus-app is vooral nuttig voor mensen die het met de andere beveiligingsmaatregelen niet zo nauw nemen.