Android veilig?

Rein de Jong

Maak Android zo veilig mogelijk!

Veel gebruikers ‘leven’ op hun smartphone, met daarop al hun financiële informatie, afspraken, e-mail, familiekiekjes en nog veel meer. Juist daarom is het zo belangrijk dat deze data niet in verkeerde handen valt. Google kan daarbij helpen, maar de primaire verantwoordelijkheid ligt bij jou. Mobiele apparaten veilig maken en houden is niet eenvoudig.

Vooral de op Android gebaseerde apparaten vormen een dankbaar aanvalsdoel. In de eerste plaats vanwege de enorme aantallen Android-apparaten, maar ook omdat veel gebruikers de veiligheid niet voorop hebben staan. Daarenboven is het droevig gesteld met de bescherming van de al wat oudere en goedkopere Android-apparaten. Dat laatste is de toestelfabrikanten aan te rekenen, die hun verantwoordelijkheid niet nemen door veiligheidsupdates laat of helemaal niet uit te rollen.

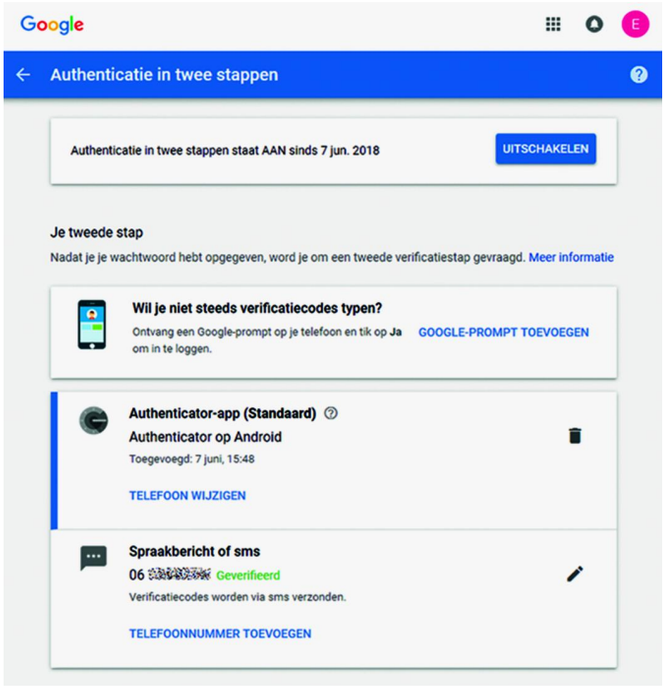
Google, de maker van Android, heeft ook de nodige steekjes laten vallen. Veel van de wat oudere Android-apparaten worden sowieso niet meer bijgewerkt; in het goedkopere segment mag je blij zijn wanneer je een veiligheidsupdate krijgt. Google heeft echter plannen om het update- en Play Store-beleid in positieve zin te veranderen. Apple daarentegen, heeft een veel strenger, soms zelfs rigide, toelatingsbeleid tot hun Store. Of we dat ook bij Android moeten wensen is de vraag, want het is niet alleen veiligheid waarop Apple hun apps test. De moraal van Apple is vaak hoger dan die van de gebruiker…

1 Hoe dan?

Hoe maak je jouw Android-apparaat zo veilig mogelijk? Wat kun je doen om het werken met Android niet al te zeer te beperken en toch zo veilig mogelijk te zijn?

1.1 Stel tweefactor-authenticatie in voor je Google-account
Basisvoorwaarde om een Androidapparaat te beveiligen is een veilig Google-account. Is je Google-account niet goed beveiligd, dan is je data op je telefoon, die je immers naar Google synchroniseert, ook niet veilig. Bovendien zijn alle door jou gebruikte Google-diensten dan ook onveilig.

Stel dus Tweefactor-authenticatie (2FA) in voor je Google-account. Er zijn diverse mogelijkheden om de tweede factor in te stellen. Van een eenvoudige sms tot het gebruik van een fysieke security key (USB/Bluetooth).
Zelf gebruik ik een Authenticator-app (Microsoft, LastPass of Google).

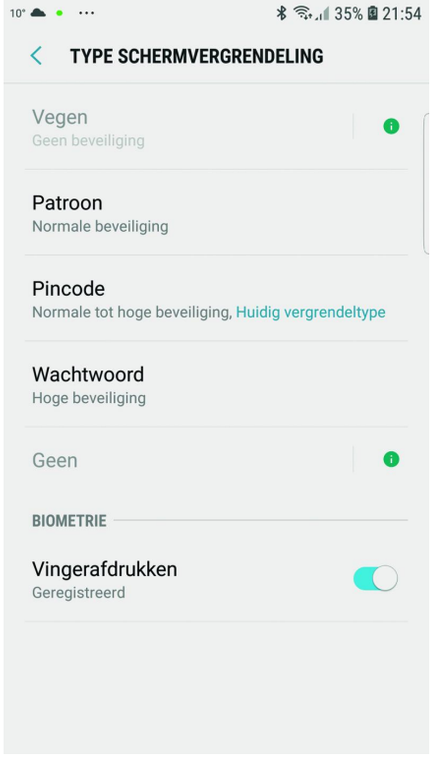


Het instellen van 2FA voor je Google-account?
1. Open de app *Instellingen* > *Google* > *Google-account* op je Android-telefoon of -tablet.
2. Tik bovenaan op *Beveiliging*.
3. Tik onder *Inloggen bij Google* op *Authenticatie in twee stappen*.
4. Tik op *Aan de slag*.

Als je 2FA nog niet hebt ingesteld, doe dat dan snel. En ben je toch bezig in de instellingen van je Google-account, doe dan ook tegelijk de Beveiligingscheck, die je ook op die pagina vindt.

1.2 Gebruik schermvergrendeling

Eigenlijk een dooddoener. Echter, ik zie nog veel Android-telefoons zonder toegangsbescherming! Het is de eerste verdediging tegen ongewenste toegang. Stel die dan ook in. De wijze waarop, varieert per Android-leverancier, maar meestal stel je het in via I*nstellingen* > *Beveiliging* > *Schermvergrendeling*.



Hoe? Ook dat varieert van apparaat tot apparaat, maar meestal kun je een Pincode, Patroon of Wachtwoord instellen. En vergeet niet een vingerafdruk, iris- of gezichtsscan (biometrie) in te stellen als je telefoon dat ondersteunt.

Je vraagt je nu af welke van de mogelijkheden het veiligst is? Elke optie heeft zijn voor- en nadelen. Patroon en Pin zijn vaak eenvoudig te herleiden wanneer je de invoer niet goed genoeg afschermt, of ze zijn op te maken uit de vegen op het scherm.
In theorie is een Pin robuuster dan een veegpatroon. Zorg dan wel dat je Pin uit meer dan vier cijfers bestaat. Liefst zes of meer. De beveiliging kan beter, want zelfs een biometrie is niet superveilig. Maar liever iets dan niets.
Ook kun je diverse informatie op het vergrendelscherm laten tonen zodat je de telefoon niet voor elk wissewasje hoeft te ontgrendelen. Bedenk daarbij echter wel wat je wel en wat je niet wenst te tonen. Een noodtelefoonnummer is wel zo handig en er is ook niet zoveel op tegen om het aantal nieuwe berichten te tonen.
De meeste gebruikers vinden het ontgrendelen van hun apparaat vervelend, het kost immers tijd en is gedoe. Gelukkig hebben de nieuwere versies van Android ‘Smart Lock’; dat maakt het vrijgeven van je telefoon eenvoudiger wanneer je thuis bent, je een smartwatch draagt, of elders bent waar het veilig is om je telefoon ontgrendeld te hebben.

1.3 Update je systeem

Naast de versie-upgrades brengt Google maandelijks veiligheidsupdates voor Android uit. Deze helpen je om je telefoon zo goed mogelijk te beveiligen tegen aanvallen. Hoewel niet elke toestelfabrikant even snel is met het uitbrengen van patches, installeer een patch zodra deze is uitgekomen.
Of je al dan niet een versieupgrade krijgt is sterk afhankelijk van de toestelfabrikant. Iedere fabrikant maakt het zijn ‘eigen’ Android. Daardoor worden upgrades moeilijker. Uiteraard moet je ook de apps updaten. Laat dat bij voorkeur automatisch gebeuren.

1.4 Download alleen uit de PlayStore

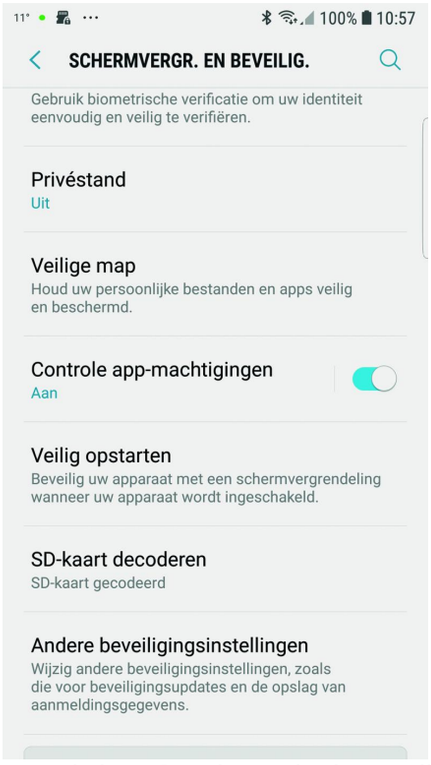
Wanneer je in het verleden wat ‘gesleuteld’ mocht hebben aan je telefoon, zou het zo maar kunnen zijn dat je apps kunt installeren uit een onbekende bron. Deze instelling maakt het mogelijk om niet-gecontroleerde apps buiten de Play Store om te installeren (‘sideloaden’ genaamd). Gelukkig wordt dit ‘sideloaden’ in de toekomst lastiger door wijzigingen in de Play Store. Deze wijzigingen maken het ontwikkelaars makkelijker om de app te splitsen in een kern en aanvullende pakketjes.
Om de veiligheid te verhogen, zou je ‘sideloaden’, moeten blokkeren (*Eigenschappen* > *Beveiliging* > *‘Onbekende apps installeren’*). Op nieuwere toestellen, vanaf Android 8.0, moet je dit per app controleren (*Eigenschappen* > *Apps* > > *Speciale toegang* > *Onbekende apps installeren*).
Mocht je ooit de ontwikkelaarsopties hebben aangezet en je gebruikt geen functies meer die daarop leunen? Schakel die dan uit!

1.5 Maak je toestel vindbaar

Je telefoon verliezen is voor velen een traumatische ervaring. Je wilt dus een mogelijkheid hebben om het toestel terug te kunnen vinden of, in het slechtste geval, de mogelijkheid te hebben het op afstand te wissen.
Google, en een aantal fabrikanten, bieden je de mogelijkheid het toestel te traceren. Het wordt *‘Zoek mijn mobiel’* genoemd en zou standaard ingeschakeld moeten staan op alle moderne Androids. Kijk even of het werkelijk zo is. Ook dit staat weer bij *Instellingen* > *Beveiliging* > *Zoek mijn mobiel*.

Mocht je onverhoopt je telefoon kwijt raken, start dan zo snel mogelijk ergens een browser, start **Google.nl** en tik in: *'zoek telefoon'*. Na ingelogd te zijn, zie je dan waar je telefoon voor het laatst verbinding heeft gemaakt met internet. Staat hij nog aan, dan kun je de telefoon, geluid laten maken, vergrendelen en zelfs wissen.

1.6 Versleutel en verberg je privégegevens



Sinds Android 3.0 heeft Google encryptie ingeschakeld staan voor de telefoongegevens.
Alleen niet standaard voor de SD-kaart. Dat moet je zelf instellen.

Verder vind je op het apparaat, afhankelijk van de Androidversie en fabrikant, een aantal mogelijkheden om je verder te beveiligen tegen nieuwsgierige ogen.

Al deze instellingen vind je bij: *Eigenschappen* > *Beveiliging*.

Privéstand
Daarmee beveilig je bestanden tegen pottenkijkers. Deze bestanden kun je alleen inzien nadat je een pincode hebt ingetoetst. Bestanden die je wilt beveiligingen kun je verplaatsen naar Privé.

Veilige map *(Samsung)*
Overlapt ten dele de privéstand. Naast bestanden, zoals foto's en andere bestanden, kun je ook apps naar de veilige map verplaatsen om ze te verbergen. Nadat je dit in de instellingen hebt aangezet vind je de veilige map terug in het apps-overzicht. Je zou kunnen overwegen om daar apps zoals DigiD, je Wachtwoordkluis en andere gevoelige apps te plaatsen.

1.7 Vermijd malware
Doordat Android het meest gebruikte OS is op telefoons en tablets, is het een dankbaar platform om aan te vallen. Ben je je bewust van veiligheid? Download je alleen uit de Play Store? Heb je minimaal Android 8.0 (Play Protect) en houd je je aan de hierboven gegeven aanbevelingen? In dat geval zou je zonder extra veiligheidspakket kunnen.
Voel je je veiliger met een beveiligingspakket, kijk dan of je internetprovider er een aanbiedt. Deze pakketten zijn vaak van F-secure en inbegrepen bij je abonnement of via je provider voordelig aan te schaffen.
Let wel! Een anti-malware-app maakt je telefoon minder snel. Het blijft altijd een afweging tussen veiligheid en snelheid.

1.8 Back-up je gegevens
Alleen een back-up beveiligt je tegen alle soorten van onheil. Telefoon defect of laten vallen, gestolen of verloren? Met een goede back-up kun je altijd weer bij je gegevens.
De meeste Android-toestellen voorzien in een back-up in de Cloud (*Instellingen* > (*Cloud en Accounts*) > *Back-up en herstel*).
Wanneer je de systeeminstellingen bij Google back-upt en de foto's en documenten laat synchroniseren naar een andere

cloudprovider, ben je redelijk safe.
Overigens is het ook een goede optie om je afbeeldingen met Google Foto's te synchroniseren. Daar heb je meer dan voldoende opslagruimte. WhatsApp moet je apart back-uppen in WhatsApp zelf.

2 In het algemeen

Naast Androidspecifieke maatregelen zijn er ook algemene maatregelen die de veiligheid verhogen. Voor alle internetapparaten, of het nu Windows, Linux of Apple betreft geldt:

Gebruik je gezonde verstand
Let op wat je doet! Je bent online, dat is per definitie een onveilige omgeving. Ook al ben je thuis, je beweegt je op de telefoon niet thuis, maar in de grote boze buitenwereld! Waan je dan ook niet veilig. Strooi op Social media niet met allerlei persoonlijke gegevens. Scherm je identiteit zoveel mogelijk af. Kijk goed wat je deelt en met wie!
Gebruik veilige wachtwoorden
Een wachtwoord dient uniek te zijn voor elke benutting. Voldoende lengte en bestaand uit meerdere tekensets. Overigens is lengte belangrijker dan tekenset. Wijzig altijd de wachtwoorden die door een leverancier zijn ingesteld. Gebruik een wachtwoordmanager of een opschrijfboekje om je wachtwoorden te onthouden. Wijzig de belangrijkste wachtwoorden (e-mail, bankieren) met regelmaat. Gebruik zo mogelijk tweefactor-authenticatie (2FA) en/of biometrie.

Mijd openbare netwerken
Wanneer je gebruik maakt van een open toegankelijke internetverbinding, moet je je ervan bewust zijn dat je wordt afgeluisterd. Doe daar geen gevoelige dingen met je telefoon. Wil je dat wel? Schakel dan Wifi uit en vertrouw op je 4G-verbinding of maak eerst een VPN-verbinding.

Herken dubieuze websites
Kijk goed of de naam van de website in de adresbalk overeenkomt met wat je verwacht. Ook is het een pre wanneer de website beveiligd is met **https://**. Ga niet op zoek naar illegale zaken en wees je ervan bewust dat veel gok- en

pornosites vaak malware trachten te verzenden. Word argwanend wanneer er veel taalfouten zijn. Zijn er contactgegevens, is er een KvK-nummer en zie je een keurmerk?

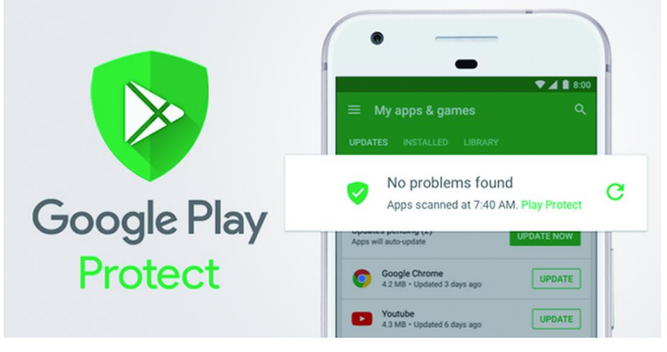
Lijkt een aanbieding te mooi om waar te zijn,
dan is het vaak ook zo.

Maak bij betalingen gebruik van een creditcard of PayPal en controleer steeds of je daarbij gegevens invoert via een beveiligde verbinding. Dan zijn je aankopen verzekerd.

3 Wat doet Google?

Naast je eigen verantwoordelijkheid om je gegevens te beschermen, mag je ook van Google verwachten dat zij al het mogelijke doen om de gebruikers van hun producten te beschermen.

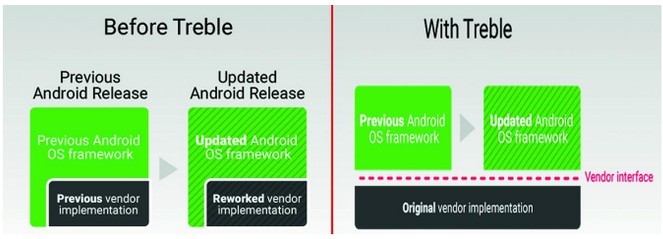
Google Play Protect
Google voorziet, vanaf Android 8.0, in een bescherming met de naam ‘Play Protect’. Play Protect is altijd ingeschakeld en het scant de apps op je telefoon en in de Play Store. Het heeft tot doel je tegen kwaadaardige apps te beschermen (ook nep-apps). Het scant zelfs ‘ge-sideloade’ apps.



Apparaatversleuteling
In eerdere versies van Android was helemaal geen versleuteling mogelijk. Later moest je het handmatig instellen en vandaag de dag is het standaard ingeschakeld en niet uitschakelbaar. Dus al je gevoelige gegevens zijn op je telefoon opgeslagen in een onleesbare vorm die je alleen kunt vrijgeven door je veiligheidscode in te geven. Nog wel even de SD-kaart, indien aanwezig handmatig versleutelen zoals aangegeven.

Android One
Google is bezig de veiligheid van Android te verbeteren door in de Android One de basis van Android los te koppelen van de fabrikant-specifieke software. De update van de basis, stock Android, wordt nu de verantwoordelijkheid van Google en niet meer die van de fabrikant. Dit geeft de mogelijkheid tot het sneller patchen van veiligheidsgaten en het langer uitrollen van nieuwe Android-versies voor de goedkopere telefoons.
Fabrikanten die nu al Android One telefoons bieden zijn o.a.: Nokia, Xiaomi, General Mobile, Motorola, HTC en natuurlijk die van Google zelf.

Project Treble
Sinds de release van Android 8 koppelt Google optioneel het hardware-afhankelijke deel van Android (Denk hierbij vooral aan de drivers) af van de rest van het basissysteem. Daardoor kan een update onafhankelijk van de aanpassingen van een chipfabrikant worden doorgevoerd. Dus sneller!



4 Tot slot

Het is niet moeilijk om je Android telefoon of tablet te beveiligen. Neem een paar minuten om de instellingen te controleren. Weten dat je alles hebt gedaan om zo veilig mogelijk met je Android-toestel om te gaan, verzekert je van een gerust gevoel wanneer je je telefoon gebruikt of wanneer die onverhoopt zoek raakt.

Mocht je een ander toestel overwegen, dan moge het duidelijk zijn dat Android One apparaat de voorkeur geniet.

*Mocht jij als lezer een tip hebben, aarzel dan niet om die mij te **melden**, dan neem ik hem op in de lijst.*

Links:

Dit artikel	http://reindejong.nl/v-android
Mijn eigen site	http://reindejong.nl
Computerveiligheid	http://bit.ly/r-veilig
Google 2FA	http://bit.ly/r-2fa