Programmabeleid voor ontwikkelaars (ingangsdatum: 1 oktober 2020)

Samen bouwen aan 's werelds meest betrouwbare bron voor apps en games

Uw innovatie is de drijvende kracht achter ons gedeelde succes, maar daar hoort wel een verantwoordelijkheid bij. Dit programmabeleid voor ontwikkelaars, samen met de distributieovereenkomst voor ontwikkelaars, garandeert dat we via Google Play de meest innovatieve en vertrouwde apps ter wereld blijven leveren aan meer dan een miljard mensen. U kunt ons beleid hieronder bekijken.

Beperkte content

Elke dag gebruiken mensen over de hele wereld Google Play om toegang tot apps en games te krijgen. Voordat u een app indient, moet u zich afvragen of uw app geschikt is voor Google Play en voldoet aan de lokale wetgeving.

In gevaar brengen van kinderen

Apps met content die minderjarigen seksualiseert, worden onmiddellijk verwijderd uit de Store, met inbegrip van, maar niet beperkt tot, apps die pedofilie of ongepaste interactie met een minderjarige (zoals betasten of liefkozen) promoten.

Daarnaast zijn apps die aantrekkelijk zijn voor kinderen maar thema's voor volwassenen bevatten niet toegestaan, met inbegrip van, maar niet beperkt tot, apps met overmatig geweld, bloed en bloedvergieten, en apps die schadelijke en gevaarlijke activiteiten weergeven of aanmoedigen. We staan ook geen apps toe die een negatief lichaams- of zelfbeeld promoten, waaronder apps die voor amusementsdoeleinden plastische chirurgie, afvallen en andere cosmetische aanpassingen van de fysieke verschijning van een persoon weergeven.

Als we ons bewust worden van content met beelden van kindermisbruik, melden we dit aan de betreffende autoriteiten en beëindigen we de Google-accounts van gebruikers die betrokken zijn bij de distributie van deze content.

Ongepaste content

We hebben normen opgesteld die content definiëren en verbieden die schadelijk of ongepast is voor onze gebruikers om ervoor te zorgen dat Google Play een veilig en respectvol platform blijft.

Seksuele content en grof taalgebruik

We staan geen apps toe die seksuele content of grof taalgebruik bevatten, waaronder pornografie, of content of services die zijn bedoeld voor seksuele bevrediging. Content met naaktheid kan worden toegestaan als deze primair bedoeld is voor educatieve, wetenschappelijke of artistieke doeleinden of voor documentaires en als het gebruik van deze beelden niet ongegrond is.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Afbeeldingen van seksuele naaktheid of seksueel suggestieve poses waarin een persoon naakt is, vervaagd is of minimale kleding aan heeft en/of als deze kleding in een passende openbare context niet acceptabel zou zijn.
- Afbeeldingen, animaties of illustraties van seksuele handelingen of seksueel suggestieve poses of de seksuele weergave van lichaamsdelen.
- Content waarin seksuele hulpmiddelen, seksgidsen, illegale seksuele thema's en fetisjen worden afgebeeld of content die functioneel als zodanig kan worden aangemerkt.
- Obscene of grove content, waaronder, maar niet beperkt tot, content die grof taalgebruik, scheldwoorden, expliciete teksten, seksuele zoekwoorden of zoekwoorden voor volwassenen bevat in de winkelvermelding of in de app.
- Content die bestialiteit afbeeldt, beschrijft of aanmoedigt.
- Apps die seksgerelateerd entertainment, escortservices of andere services promoten die kunnen worden opgevat als het aanbieden van seksuele handelingen tegen een vergoeding.
- Apps die mensen denigreren of objectiveren.

Aanzetten tot haat

We staan geen apps toe die geweld of haat promoten tegen personen of groepen op basis van ras, etnische afkomst, religie, handicap, leeftijd, nationaliteit, veteranenstatus, seksuele geaardheid, geslacht, genderidentiteit of elk ander kenmerk dat wordt gekoppeld aan systemische discriminatie of marginalisatie.

Apps die content voor educatieve, wetenschappelijke, artistieke of documentairedoeleinden bevatten die betrekking heeft op nazi's, kunnen in bepaalde landen worden geblokkeerd in overeenstemming met de lokale wet- en regelgeving.

Hieronder vindt u voorbeelden van veelvoorkomende schendingen:

- Content of taalgebruik waarin wordt beweerd dat een beschermde groep onmenselijk of minderwaardig is of het verdient om te worden gehaat.
- Apps met haatdragende uitdrukkingen, stereotypen of theorieën dat een beschermde groep negatieve kenmerken heeft (zoals kwaadaardig, corrupt, enzovoort) of die impliciet of expliciet stellen dat de groep een bedreiging vormt.
- Content of uitspraken om anderen te doen geloven dat mensen moeten worden gehaat of gediscrimineerd omdat ze lid zijn van een beschermde groep.
- Content die haatsymbolen, zoals vlaggen, symbolen, insignes, attributen of gedrag in verband met haatgroepen promoot.

Geweld

We staan geen apps toe die zinloos geweld of andere gevaarlijke activiteiten afbeelden of mogelijk maken. Apps die fictief geweld in de context van een game weergeven, zoals tekenfilms, jagen of vissen, zijn over het algemeen toegestaan.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Grafische afbeeldingen of beschrijvingen van realistisch geweld of gewelddadige bedreigingen tegen een persoon of dier.
- Apps die zelfbeschadiging, zelfmoord, kwetsen, intimidatie, eetstoornissen, wurgspellen of andere handelingen promoten waarbij ernstig letsel of de dood kan optreden.

Terroristische content

Het is terroristische organisaties niet toegestaan apps te publiceren op Google Play voor welk doel dan ook, inclusief werving.

We staan ook geen apps toe met content met betrekking tot terrorisme, zoals content waarin tot terroristische acties of geweld wordt aangezet of waarin terroristische aanslagen worden gevierd. Als u aan terrorisme gerelateerde content post voor educatieve, wetenschappelijke of artistieke doeleinden, of in de context van een documentaire, moet u voldoende informatie bieden, zodat gebruikers de context begrijpen.

Gevoelige gebeurtenissen

We staan geen apps toe die ongevoeligheid tonen ten opzichte van een natuurramp, gruweldaad, conflict, overlijden of een andere tragische gebeurtenis. Apps met content die gerelateerd is aan een gevoelige gebeurtenis, zijn over het algemeen toegestaan als die content een educatieve, wetenschappelijke, artistieke of documentaire waarde heeft of gebruikers wil wijzen op of bewust wil maken van de gevoelige gebeurtenis.

Hieronder vindt u voorbeelden van veelvoorkomende schendingen:

- Gebrek aan gevoeligheid met betrekking tot de dood van een echt persoon of groep mensen als gevolg van zelfmoord, overdosis, natuurlijke oorzaken, enzovoort.
- Ontkennen van een grote tragische gebeurtenis.
- Profiteren van een tragische gebeurtenis zonder waarneembare voordelen voor de slachtoffers.

Pesten en intimidatie

We staan geen apps toe die bedreigingen, intimidatie of pesten bevatten of mogelijk maken.

Hieronder vindt u voorbeelden van veelvoorkomende schendingen:

- Slachtoffers van internationale of religieuze conflicten kwetsen.
- Content die anderen probeert te exploiteren, zoals afpersing, chantage, enzovoort.
- Content posten om iemand publiekelijk te vernederen.
- De slachtoffers van een tragische gebeurtenis, of hun vrienden en familie, lastigvallen.

Gevaarlijke producten

We staan geen apps toe die de verkoop van explosieven, vuurwapens, munitie of bepaalde accessoires voor vuurwapens mogelijk maken.

- Beperkte accessoires zijn onder meer die welke ervoor zorgen dat een vuurwapen gaat lijken op een automatisch vuurwapen of waarmee van een vuurwapen een automatisch vuurwapen kan worden gemaakt (zoals bump stocks, trekkers voor mitrailleurs, pallen voor aanvalsgeweren, ombouwkits) en magazijnen of riemen met meer dan 30 patronen.

We staan geen apps toe die instructies geven voor het vervaardigen van explosieven, vuurwapens, munitie, beperkte vuurwapenaccessoires of andere wapens. Dit omvat tevens instructies voor het ombouwen van een vuurwapen zodat het automatisch kan vuren of lijkt alsof het automatisch kan vuren.

Marihuana

We staan geen apps toe die de verkoop van marihuana of marihuanaproducten mogelijk maken, ongeacht of marihuana legaal is of niet.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Gebruikers in staat stellen marihuana te bestellen met behulp van een winkelwagenfunctie in de app.
- Gebruikers helpen de levering of het ophalen van marihuana te regelen.
- De verkoop van producten met THC (tetrahydrocannabinol) mogelijk maken, waaronder producten als CBD-olie met THC.

Tabak en alcohol

We staan geen apps toe die de verkoop van tabak (waaronder e-sigaretten en vape-pennen) mogelijk maken of het illegale of ongepaste gebruik van alcohol of tabak aanmoedigen.

Hieronder vindt u voorbeelden van veelvoorkomende schendingen:

- Het gebruik of de verkoop van alcohol of tabak aan minderjarigen afbeelden of aanmoedigen.
- Impliceren dat de consumptie van tabak iemands sociale, seksuele, professionele, intellectuele of atletische status kan verbeteren.
- Overmatig drankgebruik op positieve wijze afbeelden, waaronder een positief beeld van overmatig alcoholgebruik, comazuipen of drankwedstrijden.

Financiële dienstverlening

We staan geen apps toe waarmee gebruikers worden blootgesteld aan misleidende of schadelijke financiële producten en diensten.

Ten behoeve van dit beleid definiëren we financiële producten en diensten als producten en diensten die betrekking hebben op het beheren en het investeren van geld en cryptocurrency's, met inbegrip van persoonlijk advies.

Als uw app financiële producten en diensten bevat of promoot, moet u voldoen aan de nationale en lokale voorschriften voor alle regio's en landen die uw app target (u moet bijvoorbeeld specifieke kennisgevingen opnemen zoals vereist door de lokale wetgeving).

Binaire opties

We staan geen apps toe die gebruikers de mogelijkheid bieden te handelen in binaire opties.

Cryptocurrency's

We staan geen apps toe die cryptocurrency minen op een apparaat. We staan wel apps toe die het minen van cryptocurrency op afstand beheren.

Persoonlijke leningen

We definiëren een persoonlijke lening als het eenmalig verstrekken van een geldelijke lening door een persoon, organisatie of entiteit aan een individuele consument, die niet is bedoeld voor het financieren van de aankoop van vaste activa of onderwijs. Consumenten van persoonlijke leningen hebben informatie nodig over de kwaliteit, kenmerken, tarieven, aflossingsschema's, risico's en voordelen van leningen om weloverwogen beslissingen te kunnen nemen over het afsluiten van een lening.

- Voorbeelden: persoonlijke leningen, salarisvoorschotten, peer-to-peer-leningen, leningen op onderpand

- Niet inbegrepen: hypotheken, autoleningen, studieleningen, doorlopend krediet (zoals creditcards, persoonlijke kredietlijnen)

Apps die persoonlijke leningen verstrekken, waaronder, maar niet beperkt tot, apps die rechtstreeks leningen aanbieden, apps waarmee leads kunnen worden gegenereerd en apps die consumenten in contact brengen met externe verstrekkers van leningen, moeten de volgende informatie publiceren in de metadata van de app:

- De minimum en maximum periode voor terugbetaling
- De maximum jaarlijkse rentevoet (APR), die over het algemeen de rentevoet plus vergoedingen en andere kosten voor een jaar omvat, of een vergelijkbare andere rentevoet die overeenkomstig de lokale wetgeving is berekend
- Een representatief voorbeeld van de totale kosten van de lening, inclusief alle toepasselijke kosten
- Een privacybeleid waarin het openen, verzamelen, gebruiken en delen van persoonlijke en gevoelige gebruikersgegevens volledig bekend wordt gemaakt.

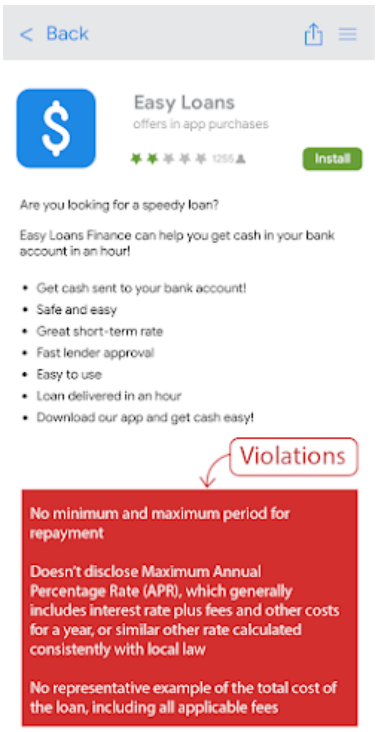
We staan geen apps toe die persoonlijke leningen promoten die binnen zestig dagen of eerder na de uitgiftedatum van de lening volledig moeten worden terugbetaald (we verwijzen hiernaar met de term 'kortlopende persoonlijke leningen').

Persoonlijke leningen met een hoge jaarlijkse rentevoet

In de Verenigde Staten staan we geen apps toe voor persoonlijke leningen waarvoor de jaarlijkse rentevoet 36% of hoger is. Apps voor persoonlijke leningen in de Verenigde Staten moeten de maximum jaarlijkse rentevoet weergeven, berekend in overeenstemming met de Truth in Lending Act (TILA).

Dit beleid is van toepassing op apps die rechtstreeks leningen aanbieden, apps waarmee leads kunnen worden gegenereerd en apps die consumenten in contact brengen met externe verstrekkers van leningen.

Hieronder vindt u een voorbeeld van veelvoorkomende schendingen:



Kansspelen, games en wedstrijden waarbij wordt gespeeld om echt geld

Apps waarmee kan worden gespeeld om echt geld, advertenties die verband houden met kansspelen waarbij wordt gespeeld om echt geld en daily fantasy sport-apps zijn toegestaan, als deze aan bepaalde vereisten voldoen.

Apps voor kansspelen

(Momenteel alleen toegestaan in Frankrijk, Ierland en het Verenigd Koninkrijk.)
Op andere locaties staan we geen apps toe die content of services bevatten die online kansspelen mogelijk maken.

Content en services die online kansspelen mogelijk maken, zijn toegestaan, op voorwaarde dat ze voldoen aan de volgende vereisten:

- De ontwikkelaar moet de aanvraagprocedure doorlopen om de app te distribueren op Play.
- De app moet voldoen aan alle toepasselijke wetten en branchenormen voor elk land waarin de app wordt gedistribueerd.
- De ontwikkelaar moet een geldige kansspellicentie hebben voor elk land waarin de app wordt gedistribueerd.
- De app moet voorkomen dat minderjarige gebruikers aan kansspelen doen in de app.
- De app moet gebruik voorkomen vanuit landen die niet vallen onder de door de ontwikkelaar geleverde kansspellicentie.
- De app mag NIET kunnen worden gekocht als een betaalde app op Google Play. Ook mag de app niet gebruikmaken van in-app-facturering via Google Play.
- De app moet gratis kunnen worden gedownload en geïnstalleerd vanuit de Google Play Store.
- De app moet zijn geclassificeerd als alleen voor volwassenen (of het IARC-equivalent daarvan).
- De app en bijbehorende app-vermelding moeten duidelijke informatie bevatten over een verantwoordelijke benadering van kansspelen.

Andere apps voor games, wedstrijden en toernooien om echt geld

We staan geen content of services toe waarmee gebruikers kunnen inzetten, wedden of deelnemen met echt geld (waaronder in-app-items die zijn gekocht met geld) om een prijs in geldwaarde te ontvangen. Dit omvat, maar is niet beperkt tot, online casino's, sportweddenschappen, loterijen die niet voldoen aan de vereisten voor kansspel-apps hierboven en games die prijzen in contant geld of andere echte waarde bieden.

Hieronder vindt u enkele voorbeelden van schendingen:

- Games die geld accepteren in ruil voor een kans om een fysieke of geldprijs te winnen.
- Games met 'loyaliteitspunten' (bijvoorbeeld betrokkenheid of activiteit) die (1) worden verdiend of versneld door aankopen met echt geld, die (2) kunnen worden ingewisseld voor items of prijzen met een echte geldwaarde.
- Apps die de inzet van kansspelen, in-app-valuta's die vereist zijn voor deelname, winst of stortingen accepteren of beheren om in aanmerking te komen voor een fysieke of geldprijs.
- Apps die een call-to-action bieden om met echt geld in te zetten op, te wedden op of deel te nemen aan games, wedstrijden of toernooien, zoals apps met navigatie-elementen (menu-items, tabbladen, knoppen, enzovoort) die gebruikers uitnodigen zich te registreren (REGISTREER NU) of deel te nemen (DOE NU MEE) aan een toernooi om kans te maken op een geldprijs.

Advertenties voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld in op Play gedistribueerde apps

We staan apps toe die reclame maken voor kansspelen of wedstrijden, competities of toernooien waarbij om echt geld wordt gespeeld als ze voldoen aan de volgende vereisten:

- De app en advertentie (waaronder adverteerders) moeten voldoen aan alle toepasselijke wetten en branchenormen voor elke locatie waar de advertentie wordt weergegeven.
- De advertentie moet voldoen aan lokale licentievereisten voor alle kansspelgerelateerde producten en services die worden gepromoot.
- De app mag geen kansspeladvertenties weergeven aan gebruikers waarvan bekend is dat ze jonger dan achttien jaar zijn.
- De app mag niet zijn aangemeld voor het programma 'Gemaakt voor gezinnen'.
- De app mag geen gebruikers targeten die jonger dan achttien jaar zijn.
- Als er reclame wordt gemaakt voor een app voor kansspelen (zoals hierboven gedefinieerd), moet de advertentie op de bestemmingspagina, in de vermelding van de geadverteerde app of in de app zelf duidelijke informatie weergeven over een verantwoordelijke benadering van kansspelen.-
- De app mag geen gesimuleerde content met betrekking tot kansspelen aanbieden (zoals sociale casino-apps, apps met virtuele gokautomaten).
- De app mag geen ondersteuningsfunctionaliteit voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld bieden (zoals functionaliteit voor hulp bij gokken, uitbetalingen, het bijhouden van sportscores/kansberekening of het beheren van deelnamegeld).
- U mag geen eigendomsbelang hebben in de kansspelservices of services voor games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld waarvoor in de app wordt geadverteerd.
- App-content mag geen kansspelservices of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld, promoten of gebruikers naar deze services leiden.

Alleen apps voor kansspelen (zoals hierboven gedefinieerd) of apps die aan al deze vereisten voor kansspeladvertenties voldoen, mogen advertenties bevatten voor kansspelen of games, wedstrijden of toernooien waarbij om echt geld wordt gespeeld.

Hieronder vindt u enkele voorbeelden van schendingen:

- Een app die is ontworpen voor minderjarige gebruikers en waarin een advertentie wordt weergegeven waarin kansspelservices worden gepromoot
- Een gesimuleerde casinogame die casino's waar wordt gespeeld om echt geld promoot of die gebruikers naar dergelijke casino's leidt
- Een speciale app voor het bijhouden van kansberekening in sport met geïntegreerde kansspeladvertenties die een link bevatten naar een site voor sportweddenschappen
- Een nieuws-app die advertenties weergeeft voor een kansspelservice die eigendom is van of wordt beheerd door de ontwikkelaar van de app
- Apps met kansspeladvertenties die ons beleid voor misleidende advertenties schenden, zoals advertenties die aan gebruikers worden weergegeven als knoppen, iconen of andere interactieve in-app-elementen

Apps met Daily fantasy sports (DFS)

We staan apps met Daily fantasy sports (DSF), zoals gedefinieerd in de toepasselijke lokale wetgeving, alleen toe als ze voldoen aan de volgende vereisten:

- De app wordt 1) alleen gedistribueerd in de Verenigde Staten of 2) komt in aanmerking volgens de hierboven genoemde vereisten aan kansspel-apps.
- De ontwikkelaar moet de aanvraagprocedure voor DFS doorlopen en worden geaccepteerd om de app op Google Play te kunnen distribueren.
- De app moet voldoen aan alle toepasselijke wetgeving en branchenormen voor de landen waar de app wordt gedistribueerd.
- De app moet voorkomen dat minderjarige gebruikers wedden of geldtransacties uitvoeren in de app.
- De app mag NIET kunnen worden gekocht als een betaalde app op Google Play. Ook mag de app niet gebruikmaken van in-app-facturering via Google Play.
- De app moet gratis kunnen worden gedownload en geïnstalleerd vanuit de Google Play Store.
- De app moet zijn geclassificeerd als alleen voor volwassenen (of het IARC-equivalent daarvan).
- De app en bijbehorende app-vermelding moeten duidelijke informatie bevatten over een verantwoordelijke benadering van kansspelen.

Indien de app wordt gedistribueerd in de VS, zijn de volgende aanvullende vereisten van toepassing:

- De app moet voldoen aan alle toepasselijke wetten en branchenormen voor elke staat in en elk grondgebied van de Verenigde Staten waar de app wordt gedistribueerd.
- De ontwikkelaar moet beschikken over een geldige licentie voor elke staat in en elk grondgebied van de Verenigde Staten waar een licentie vereist is voor apps met Daily fantasy sports.
- De app moet voorkomen dat deze kan worden gebruikt in staten in of grondgebieden van de Verenigde Staten waar de ontwikkelaar niet beschikt over een licentie die is vereist voor apps met Daily fantasy sports.
- De app moet voorkomen dat deze kan worden gebruikt in staten in of grondgebieden van de Verenigde Staten waar apps met Daily fantasy sports niet legaal zijn.

Illegale activiteiten

We staan geen apps toe die illegale activiteiten ondersteunen of promoten.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Het faciliteren van de verkoop of aankoop van illegale drugs of geneesmiddelen op recept waarvoor geen recept is uitgeschreven.
- Het afbeelden of aanmoedigen van het gebruik of de verkoop van drugs, alcohol of tabak door minderjarigen.
- Instructies voor het kweken of vervaardigen van illegale drugs.

Door gebruikers gegenereerde content

Door gebruikers gegenereerde content (UGC) is content die gebruikers bijdragen aan een app en die zichtbaar of toegankelijk is voor ten minste een groep gebruikers van de app.

Apps met UGC moeten:

- vereisen dat gebruikers de gebruiksvoorwaarden en/of het gebruikersbeleid van de app accepteren voordat gebruikers UGC kunnen maken of uploaden,

- aanstootgevende content en gedrag definiëren (op een manier die voldoet aan het programmabeleid voor ontwikkelaars van Google Play) en deze verbieden in de gebruiksvoorwaarden of het gebruikersbeleid van de app,
- robuuste, doeltreffende en voortdurende moderatie van UGC implementeren, voor zover redelijk en consistent met het soort UGC dat wordt gehost door de app.
  - In het geval van apps met live streaming moet aanstootgevende UGC zo snel mogelijk in realtime worden verwijderd.
  - In het geval van AR-apps (augmented reality) moet UGC-moderatie (inclusief het rapportagesysteem in apps) rekening houden met zowel aanstootgevende AR-UGC (bijvoorbeeld een seksueel expliciete AR-afbeelding) als gevoelige AR-ankerlocatie (bijvoorbeeld AR-content die is verankerd aan een gebied dat niet toegankelijk is, zoals een militaire basis of een privéterrein waar AR-verankering problemen kan veroorzaken voor de eigenaar van de locatie).
- een gebruiksvriendelijk in-app-systeem bieden voor het melden van aanstootgevende UGC en waar nodig actie ondernemen tegen die UGC,
- gebruikers van de apps die de gebruiksvoorwaarden en/of het gebruikersbeleid van de app schenden, verwijderen of blokkeren,
- verstrekken van waarborgen om te voorkomen dat in de app inkomsten worden gegenereerd door de stimulering van aanstootgevend gedrag van gebruikers.

Apps waarvan de weergave van bezwaarlijke UGC het hoofddoel is, worden verwijderd uit Google Play. Ook apps die uiteindelijk hoofdzakelijk worden gebruikt voor het hosten van bezwaarlijke UGC of die onder gebruikers de reputatie ontwikkelen dat het een geschikte plek is voor dat soort content, worden verwijderd uit Google Play.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Seksueel expliciete content die is gemaakt door gebruikers promoten, waaronder de implementatie of het toestaan van betaalde functies die voornamelijk tot doel hebben het delen van aanstootgevende content te stimuleren.
- Apps met door gebruikers gegenereerde content die onvoldoende beschermingsmaatregelen bevatten tegen bedreigingen, intimidatie of pesten, in het bijzonder tegen minderjarigen.
- Posts, reacties of foto's plaatsen met een app die primair bedoeld zijn om een andere persoon te intimideren of aan te merken voor misbruik, kwaadwillende aanvallen of bespotting.
- Apps die klachten van gebruikers over bezwaarlijke content voortdurend negeren.

Niet-goedgekeurde stoffen

Google Play staat geen apps toe die niet-goedgekeurde stoffen promoten of verkopen, ongeacht claims met betrekking tot de legaliteit. Voorbeelden:

- Alle items op deze niet-volledige lijst met verboden farmaceutische producten en supplementen.
- Producten die efedra bevatten.
- Producten die hCG (humaan choriongonadotrofine) bevatten in verband met gewichtsverlies of gewichtsbeheersing of indien gepromoot in combinatie met anabole steroïden.
- Kruiden- en dieetsupplementen met actieve farmaceutische of gevaarlijke ingrediënten.
- Onjuiste of misleidende gezondheidsclaims, waaronder claims die impliceren dat een product even effectief is als geneesmiddelen op recept of gereguleerde stoffen.
- Niet door de overheid goedgekeurde producten die worden gepromoot alsof ze veilig of effectief zijn ter voorkoming, behandeling of genezing van een bepaalde ziekte of aandoening.
- Producten die zijn onderworpen aan acties of waarschuwingen van overheden of regulerende instanties.
- Producten met namen die een verwarrende gelijkenis vertonen met een niet-goedgekeurd farmaceutisch product of supplement of gereguleerde stof.

Ga naar www.legitscript.com voor meer informatie over de niet-goedgekeurde of misleidende farmaceutische producten en supplementen die we controleren.

Intellectueel eigendom

Als ontwikkelaars het werk van iemand anders kopiëren of gebruiken zonder de vereiste toestemming, is dit schadelijk voor de eigenaar van dat werk. Maak niet op oneerlijke wijze gebruik van het werk van anderen.

Intellectueel eigendom

We staan geen apps of ontwikkelaarsaccounts toe die inbreuk maken op de intellectuele-eigendomsrechten van anderen (waaronder handelsmerken, auteursrechten, patenten, handelsgeheimen en andere eigendomsrechten). We staan ook geen apps toe die inbreuk op intellectuele-eigendomsrechten stimuleren of veroorzaken.

We reageren op duidelijke meldingen van vermeende inbreuk op auteursrecht. Raadpleeg onze auteursrechtprocedures voor meer informatie of voor het indienen van een DMCA-verzoek.

Als u een klacht wilt indienen over de verkoop en promotie van namaakartikelen in een app, kunt u een melding van namaakartikelen indienen.

Als u de eigenaar bent van een handelsmerk en van mening bent dat er op Google Play een app beschikbaar is die inbreuk maakt op uw handelsmerkrechten, raden we u aan rechtstreeks contact op te nemen met de ontwikkelaar om uw zorgen kenbaar te maken. Als u niet tot een oplossing kunt komen met de ontwikkelaar, kunt u via dit formulier een handelsmerkklacht indienen.

Als u schriftelijke documentatie heeft die aantoont dat u over de rechten beschikt om de intellectuele eigendom van derden te gebruiken in uw app of winkelvermelding (zoals merknamen en logo's en grafische items), neemt u contact op met het Google Play-team voordat u uw klacht indient, om er zeker van te zijn dat uw app niet wordt geweigerd op grond van een schending van intellectuele eigendom.

Onbevoegd gebruik van auteursrechtelijk beschermd materiaal

We staan geen apps toe die inbreuk maken op een auteursrecht. Ook na het aanpassen van auteursrechtelijk beschermd materiaal kan er nog steeds sprake zijn van schending. Ontwikkelaars kan worden gevraagd bewijs te leveren van hun rechten voor het gebruik van auteursrechtelijk beschermd materiaal.

Wees voorzichtig bij het gebruik van auteursrechtelijk beschermde content om de functionaliteit van uw app aan te tonen. Over het algemeen is het veiliger om originele content te maken.

Hierna volgen enkele voorbeelden van auteursrechtelijk beschermd materiaal dat vaak wordt gebruikt zonder toestemming of andere juridisch geldige reden:

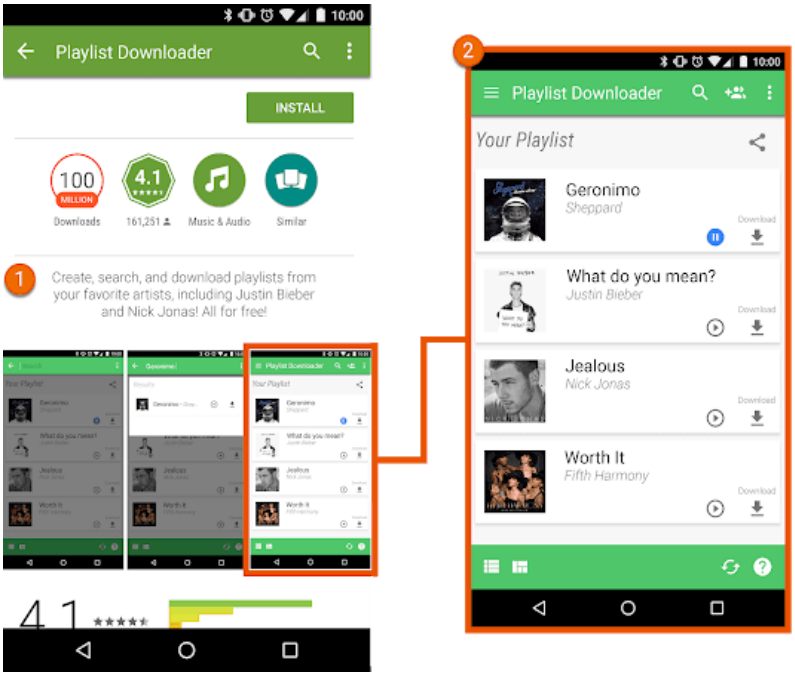
- omslagen/hoezen voor muziekalbums, videogames en boeken,
- marketingafbeeldingen uit films, televisieprogramma's of videogames,
- afbeeldingen uit stripboeken, tekenfilms, films, muziekvideo's of televisieprogramma's,
- logo's van amateur- of professionele sportteams,
- foto's die afkomstig zijn van het social media-account van een bekende persoon,
- professionele afbeeldingen van bekende personen,
- reproducties of 'fan art' die niet te onderscheiden zijn van het oorspronkelijke auteursrechtelijk beschermde werk,
- apps met soundboards die audiofragmenten afspelen uit auteursrechtelijk beschermd materiaal,
- volledige reproducties of vertalingen van boeken die zich niet in het publieke domein bevinden.

Stimuleren van inbreuk op auteursrecht

We staan geen apps toe die auteursrechtschending veroorzaken of stimuleren. Voordat u uw app publiceert, moet u onderzoeken of er manieren zijn waarop uw app auteursrechtschending stimuleert. Vraag indien nodig om juridisch advies.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Streaming-apps waarmee gebruikers een lokale kopie van auteursrechtelijk beschermd materiaal kunnen downloaden zonder toestemming.
- Apps die het streamen en downloaden van auteursrechtelijk beschermd materiaal stimuleren, met inbegrip van muziek en video, in strijd met de toepasselijke auteursrechtwetgeving:



① De beschrijving in deze app-vermelding stimuleert gebruikers om auteursrechtelijk beschermd materiaal te downloaden zonder toestemming.
② Het screenshot in de app-vermelding stimuleert gebruikers om auteursrechtelijk beschermd materiaal te downloaden zonder toestemming.

Inbreuk op handelsmerk

We staan geen apps toe die inbreuk maken op de handelsmerken van anderen. Een handelsmerk is een woord, symbool of een combinatie hiervan waarmee de bron van een goed of service wordt geïdentificeerd. Zodra een handelsmerk is verkregen, geeft dit de eigenaar het exclusieve recht op het gebruik van het handelsmerk met betrekking tot bepaalde goederen of services.

Inbreuk op een handelsmerk vindt plaats wanneer er sprake is van onjuist of onbevoegd gebruik van een identiek of soortgelijk handelsmerk op zo'n manier dat het waarschijnlijk is dat er verwarring ontstaat over de bron van dat product. Als uw app handelsmerken van andere partijen gebruikt en dit tot verwarring kan leiden, kan uw app worden opgeschort.

Namaak

We staan geen apps toe die namaakartikelen verkopen of de verkoop ervan promoten. Namaakartikelen zijn voorzien van een handelsmerk of logo dat niet of nauwelijks te onderscheiden is van het handelsmerk van iemand anders. Deze artikelen bevatten geïmiteerde merkkenmerken van het product met het doel ze te promoten als officiële producten van de merkeigenaar.

Privacy, misleiding en apparaatmisbruik

We streven ernaar de privacy van gebruikers te beschermen en een veilige omgeving te bieden aan onze gebruikers. Apps die misleidend of kwaadwillend zijn of die een netwerk, apparaat of persoonlijke gegevens misbruiken, zijn ten strengste verboden.

Gebruikersgegevens

U moet transparant zijn over hoe u omgaat met gebruikersgegevens (zoals gegevens die worden verzameld van of over een gebruiker, waaronder apparaatgegevens). Dit houdt in dat u bekend moet maken dat uw app toegang heeft tot de gegevens en deze verzamelt, gebruikt en deelt en dat u het gebruik van de gegevens moet beperken tot de bekendgemaakte doeleinden. Als uw app persoonlijke of gevoelige gegevens verwerkt, moet daarnaast rekening worden gehouden met de aanvullende eisen die worden vermeld in het gedeelte 'Persoonlijke en gevoelige gegevens' hieronder. Deze vereisten voor Google Play gelden in aanvulling op eventuele vereisten die worden voorgeschreven in de toepasselijke wetgeving op het gebied van privacy en gegevensbescherming.

Persoonlijke en gevoelige informatie

Persoonlijke en gevoelige gebruikersgegevens omvatten onder meer persoonlijk identificeerbare informatie, financiële en betalingsgegevens, verificatiegegevens, het telefoonboek, contacten, apparaatlocatie, gegevens over sms-berichten en gesprekken, microfoon- en camerагegevens en andere gevoelige apparaat- of gebruiksgegevens. Als uw app gevoelige gebruikersgegevens verwerkt, moet u het volgende doen:

- De toegang tot persoonlijke of gevoelige gegevens die worden verkregen via de app en de verzameling, het gebruik en het delen ervan beperken tot doeleinden die direct verband houden met de verstrekking en verbetering van de functies van de app (zoals door de gebruiker verwachte functies die worden beschreven en gepromoot in de beschrijving van de app in de Play Store). Apps die het gebruik van deze gegevens uitbreiden tot de weergave van advertenties moeten voldoen aan ons advertentiebeleid.
- Een privacybeleid plaatsen dat wordt weergegeven in zowel het daarvoor bestemde veld in de Play Console als in de app zelf. Het privacybeleid moet, samen met kennisgevingen in de app, duidelijk bekendmaken hoe uw app toegang heeft tot gebruikersgegevens en deze verzamelt, gebruikt en deelt. In uw privacybeleid moet bekend worden gemaakt tot welke soorten persoonlijke en gevoelige gegevens uw app toegang heeft, welke soorten persoonlijke en gevoelige gegevens uw app verzamelt en gebruikt en met welke partijen deze gegevens worden gedeeld.
- Alle persoonlijke of gevoelige gebruikersgegevens beveiligd verwerken, waaronder de overdracht van de gegevens met behulp van moderne versleuteling (bijvoorbeeld via https).
- Waar mogelijk een verzoek om runtimerechten gebruiken voordat toegang wordt verkregen tot gegevens die worden afgeschermd door Android-rechten.
- Geen persoonlijke of gevoelige gebruikersgegevens verkopen.

Vereisten ten aanzien van prominente kennisgeving en toestemming

In gevallen waarin gebruikers mogelijk niet redelijkerwijs kunnen verwachten dat hun persoonlijke of gevoelige gebruikersgegevens nodig zijn om de beleidsconforme functies of functionaliteit van uw app te verstrekken of te verbeteren (zoals gegevensverzameling op de achtergrond van uw app), moet u voldoen aan de volgende eisen:

U moet een in-app-kennisgeving verstrekken over de verzameling, het gebruik en het delen van gegevens. De kennisgeving in de app:

- moet in de app zelf worden weergegeven, niet alleen in de beschrijving van de app of op een website,
- moet worden weergegeven tijdens normaal gebruik van de app en mag niet vereisen dat de gebruiker naar een menu of instellingen navigeert,
- moet beschrijven tot welke gegevens toegang wordt verkregen of welke gegevens worden verzameld,
- moet duidelijk maken hoe de gegevens worden gebruikt en/of gedeeld,
- **mag niet** alleen in een privacybeleid of servicevoorwaarden worden geplaatst,
- **mag niet** worden opgenomen in combinatie met andere kennisgevingen die niet gerelateerd zijn aan de verzameling van persoonlijke of gevoelige gegevens.

De in-app-kennisgeving moet worden weergegeven bij en onmiddellijk voorafgaan aan een verzoek om toestemming van de gebruiker en, waar beschikbaar, gekoppelde runtimerechten. U mag geen toegang krijgen tot persoonlijke of gevoelige gegevens of deze verzamelen voordat de gebruiker toestemming verleent. Het verzoek om toestemming in de app:

- moet in het toestemmingsdialoogvenster duidelijk en ondubbelzinnig worden weergegeven,
- moet een bevestigende actie van de gebruiker vereisen (bijvoorbeeld tikken om te accepteren of een selectievakje aanvinken),
- mag het feit dat de gebruiker de kennisgeving verlaat (bijvoorbeeld door ergens anders te tikken of op de terug- of startknop te drukken) **niet** interpreteren als toestemming, en
- **mag niet** gebruikmaken van berichten die automatisch worden gesloten of verlopen om zo toestemming te verkrijgen van de gebruiker.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Een app die toegang heeft tot de voorraad geïnstalleerde apps van een gebruiker en deze gegevens niet behandelt als persoonlijke of gevoelige gegevens waarop de bovenstaande vereisten betreffende het privacybeleid, de prominente kennisgeving en toestemming van toepassing zijn.
- Een app die toegang heeft tot de telefoonboek- of contactgegevens van een gebruiker en die deze gegevens niet behandelt als persoonlijke of gevoelige gegevens waarop de bovenstaande vereisten betreffende het privacybeleid, de prominente kennisgeving en toestemming van toepassing zijn.
- Een app die het scherm van een gebruiker opneemt en deze gegevens niet als persoonlijke of gevoelige gegevens behandelt op grond van dit beleid.
- Een app die de apparaatlocatie verzamelt en het gebruik niet duidelijk bekend maakt en toestemming verkrijgt in overeenstemming met de vereisten hiervoor .
- Een app die op de achtergrond van de app beperkte rechten verzamelt, bijvoorbeeld voor tracking-, onderzoeks- of marketingdoeleinden, en het gebruik ervan niet volledig openbaar maakt en geen toestemming krijgt in

overeenstemming met de bovenstaande vereisten.

Specifieke beperkingen voor toegang tot gevoelige gegevens

In aanvulling op de voorgaande vereisten worden in de tabel hierna de vereisten voor specifieke activiteiten beschreven.

Activiteit	Vereiste
Uw app verwerkt financiële of betalingsgegevens of nummers van door de overheid uitgegeven identiteitsbewijzen	De app mag persoonlijke of gevoelige gebruikersgegevens met betrekking tot financiële of betalingsactiviteiten of nummers van door de overheid uitgegeven identiteitsbewijzen nooit openbaar maken.
Uw app verwerkt niet-openbare telefoonboek- of contactgegevens	We staan geen ongeautoriseerde publicatie of openbaarmaking van niet-openbare contactgegevens van mensen toe.
Uw app bevat een antivirus- of beveiligingsfunctie, zoals antivirus, antimalware of beveiligingsgerelateerde functies	Uw app moet een privacybeleid plaatsen dat, samen met openbaarmakingen in de app, toelicht welke gebruikersgegevens door uw app worden verzameld en overgedragen, hoe deze gegevens worden gebruikt en met wie de gegevens worden gedeeld.

EU-U.S. Privacy Shield (EU-VS privacyschild)

Privacy Shield

Als u door Google beschikbaar gestelde persoonlijke gegevens opent, gebruikt of verwerkt waarin een persoon direct of indirect wordt geïdentificeerd en die afkomstig zijn uit de Europese Unie of Zwitserland ('Persoonlijke gegevens uit de EU'), is het volgende van toepassing:

- U moet voldoen aan alle toepasselijke wetgeving, richtlijnen, voorschriften en regels met betrekking tot privacy, gegevensbeveiliging en gegevensbescherming.
- U mag Persoonlijke gegevens uit de EU alleen openen, gebruiken of verwerken voor doeleinden die overeenkomen met de toestemming die is verkregen van de persoon waarop de Persoonlijke gegevens uit de EU betrekking hebben.
- U moet passende organisatorische en technische maatregelen implementeren om de Persoonlijke gegevens uit de EU te beschermen tegen verlies, misbruik en ongeautoriseerde of onwettige toegang, openbaarmaking, aanpassing en vernietiging.
- U moet hetzelfde beveiligingsniveau leveren als is vereist door de Privacy Shield-principes.

U moet regelmatig nagaan of u deze voorwaarden naleeft. Als u op enig moment niet aan deze voorwaarden kunt voldoen (of als er een aanzienlijk risico bestaat dat u er niet aan kunt voldoen), moet u ons onmiddellijk per e-mail informeren via data-protection-office@google.com en onmiddellijk stoppen met de verwerking van Persoonlijke informatie uit de EU of redelijke en passende maatregelen nemen om een toereikend beschermingsniveau te herstellen.

Rechten

Gebruikers moeten verzoeken om rechten kunnen begrijpen. U mag alleen om rechten verzoeken die noodzakelijk zijn om bestaande functies of services in uw app uit te voeren die worden gepromoot in uw Play-winkelvermelding. U mag rechten die toegang geven tot gebruikers- of apparaatgegevens niet gebruiken voor niet-bekendgemaakte, niet-uitgevoerde of niet-toegestane functies of doeleinden. Persoonlijke of gevoelige gegevens waar toegang tot is verkregen door middel van rechten, mogen nooit worden verkocht.

Verzoek in context om rechten voor toegang tot gegevens (via incrementele autorisatie), zodat gebruikers begrijpen waarom uw app verzoekt om die rechten. Gebruik de gegevens uitsluitend voor de doeleinden waarmee de gebruiker heeft ingestemd. Als u de gegevens later voor andere doeleinden wilt gebruiken, moet u dat aan gebruikers vragen en ervoor zorgen dat zij instemmen met het aanvullende gebruik.

Beperkte rechten

In aanvulling op het bovenstaande, worden beperkte rechten omschreven als rechten die zijn geclassificeerd als Gevaarlijk, Speciaal of Handtekening, en hierop zijn de volgende aanvullende vereisten en beperkingen van toepassing:

- Gevoelige gebruikers- of apparaatgegevens waar toegang tot wordt verkregen via beperkte rechten, mogen alleen worden overgedragen aan derden als dat noodzakelijk is om bestaande functies of services in de app waarin de gegevens worden verzameld aan te bieden of te verbeteren. U mag ook gegevens overdragen als dat noodzakelijk is

om te voldoen aan de toepasselijke wetgeving of als onderdeel van een overname, fusie of verkoop van activa met een juridisch toereikende kennisgeving aan de gebruikers. Alle andere soorten overdracht of verkoop van de gebruikersgegevens zijn verboden.

- Respecteer het besluit van een gebruiker als deze een verzoek om beperkte rechten afwijst. Gebruikers mogen ook niet worden gemanipuleerd of gedwongen om toestemming te geven voor niet-cruciale rechten. U moet zich redelijk inspannen om tegemoet te komen aan gebruikers die geen toegang verlenen tot gevoelige rechten (bijvoorbeeld de gebruiker toestaan handmatig een telefoonnummer in te toetsen als ze de toegang tot de gesprekslijsten hebben beperkt).

Op bepaalde beperkte rechten kunnen de hieronder beschreven extra vereisten van toepassing zijn. Het doel van deze beperkingen is de waarborging van de privacy van de gebruiker. We kunnen beperkte uitzonderingen toestaan op de onderstaande vereisten in zeldzame gevallen waarin apps een zeer aantrekkelijke of noodzakelijke functie bieden waarbij momenteel geen alternatieve methode is om de functie aan te bieden. We beoordelen voorgestelde uitzonderingen op potentiële privacy- of beveiligingsgevolgen voor gebruikers.

Rechten voor sms en gesprekslijsten

Sms en gesprekslijsten worden beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige informatie en de volgende beperkingen van toepassing zijn:

Beperkte rechten	Vereiste
Uw app-manifest verzoekt om de rechtengroep Gesprekkenlijst (zoals READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	De app moet actief worden geregistreerd als de standaard telefoon- of Assistent-handler op het apparaat.
Uw app-manifest verzoekt om de rechtengroep Sms (zoals READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	De app moet actief worden geregistreerd als de standaard sms- of Assistent-handler op het apparaat.

Apps zonder standaard sms-, telefoon- of Assistent-handlermogelijkheden mogen het gebruik van de bovenstaande rechten niet definiëren in het manifest. Dit omvat tevens tekst in tijdelijke aanduidingen in het manifest. Daarnaast moeten apps actief worden geregistreerd als standaard sms-, telefoon- of Assistent-handler voordat gebruikers wordt gevraagd om een van de bovenstaande rechten te accepteren. De apps moeten onmiddellijk stoppen met het gebruik van de rechten als ze niet langer de standaardhandler zijn. De toegestane gebruiksmogelijkheden en uitzonderingen zijn beschikbaar op deze pagina van het Helpcentrum.

Apps mogen alleen de rechten (en eventuele gegevens die afkomstig zijn van deze rechten) gebruiken om goedgekeurde kernfunctionaliteit van de app te leveren. Kernfunctionaliteit wordt gedefinieerd als het belangrijkste doel van de app. Dit kan bestaan uit een reeks kernfuncties die alle duidelijk moeten worden beschreven en gepromoot in de beschrijving van de app. Zonder de kernfunctie is de app 'defect' of wordt deze onbruikbaar. De overdracht, het delen of het gelicentieerde gebruik van deze gegevens mag uitsluitend plaatsvinden voor het verstrekken van kernfuncties of -services binnen de app en het gebruik ervan mag nooit worden uitgebreid tot eventuele andere doeleinden (zoals de verbetering van andere apps of services, reclame- of marketingdoeleinden). U mag geen alternatieve methoden (waaronder andere rechten, API's of externe bronnen) gebruiken om gegevens te verkrijgen die zijn toegewezen aan rechten voor sms- en gesprekslijsten.

Locatierechten

De apparaatlocatie wordt beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige gegevens en de volgende vereisten van toepassing zijn:

- Apps mogen geen toegang krijgen tot gegevens die zijn beschermd door locatierechten (zoals ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) nadat dit niet langer noodzakelijk is om de betreffende functies of services in uw app te leveren.
- U mag nooit om locatierechten van gebruikers verzoeken met als enige doel advertenties of analyses. Apps die het toegestane gebruik van deze gegevens uitbreiden tot de weergave van advertenties, moeten voldoen aan ons advertentiebeleid.
- Apps moeten verzoeken om het laagst mogelijke bereik (bijvoorbeeld geschat in plaats van gedetailleerd en voorgrond in plaats van achtergrond) om de betreffende functie of service te verstrekken waarvoor de locatie vereist is. Gebruikers mogen redelijkerwijs verwachten dat de functie of service het locatieniveau nodig heeft waarom wordt verzocht. We kunnen bijvoorbeeld apps afwijzen die zonder overtuigende motivering verzoeken om achtergrondlocatie.
- De locatie op de achtergrond mag alleen worden gebruikt om functies te bieden die nuttig zijn voor de gebruiker en relevant zijn voor de kernfunctionaliteit van de app.

Apps mogen toegang tot de locatie hebben via de service op de voorgrond (als de app alleen toegang op de voorgrond heeft, bijvoorbeeld 'tijdens gebruik') als het gebruik:

- is gestart als een voortzetting van een door de gebruiker gestarte actie in de app, en
- meteen wordt beëindigd nadat de beoogde toepassing van de door de gebruiker gestarte actie is voltooid door de app.

Apps die specifiek zijn ontworpen voor kinderen, moeten voldoen aan het beleid voor Gemaakt voor gezinnen.

Rechten voor toegang tot alle bestanden

Bestanden en directorykenmerken op het apparaat van een gebruiker worden beschouwd als persoonlijke en gevoelige gebruikersgegevens waarop het beleid voor persoonlijke en gevoelige gegevens en de volgende vereisten van toepassing zijn:

- Apps mogen alleen toegang vragen tot apparaatopslag die essentieel is voor de werking van de app en mogen geen toegang vragen tot apparaatopslag namens derden voor doeleinden die geen verband houden met kritieke, op de gebruiker gerichte app-functionaliteit.
- Android-apparaten met R (Android 11, API-niveau 30) of hoger hebben het recht MANAGE_EXTERNAL_STORAGE nodig om toegang in gedeelde opslag te beheren. Alle apps die R targeten en brede toegang tot gedeelde opslag vragen ('Toegang tot alle bestanden'), moeten een juiste toegangscontrole doorlopen voordat ze kunnen worden gepubliceerd. Apps die dit recht mogen gebruiken, moeten gebruikers duidelijk vragen 'Toegang tot alle bestanden' in te schakelen voor hun app onder de instellingen voor 'Speciale app-toegang'. Raadpleeg dit Help-artikel voor meer informatie over de R-vereisten.

Apparaat- en netwerkmisbruik

We staan geen apps toe die het apparaat van de gebruiker, andere apparaten of computers, servers, netwerken, Application Programming Interfaces (API's) of services, met inbegrip van, maar niet beperkt tot andere apps op het apparaat, een Google-service of het netwerk van een erkende provider, verstoren, onderbreken, beschadigen of daartoe op onbevoegde wijze toegang verkrijgen.

Apps op Google Play moeten voldoen aan de standaardvereisten voor systeemoptimalisatie van Android die zijn vastgelegd in de richtlijnen voor core app-kwaliteit (Core App Quality Guidelines) voor Google Play.

Een app die wordt gedistribueerd via Google Play, mag zichzelf niet aanpassen, vervangen of updaten via een andere methode dan het updatemechanisme van Google Play. Ook mag een app geen uitvoerbare code (zoals dex-, jar- of so-bestanden) downloaden via een andere bron dan Google Play. Deze beperking is niet van toepassing op code die wordt uitgevoerd op een virtuele machine en beperkte toegang heeft tot Android-API's (zoals JavaScript in een WebView of browser).

We staan geen code toe die kwetsbaarheden in de beveiliging introduceert of misbruikt. Raadpleeg het programma voor de verbetering van de beveiliging van apps voor meer informatie over de meest recente beveiligingsproblemen die zijn gemarkeerd voor ontwikkelaars.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- apps die een andere app verstoren of blokkeren door de weergave van advertenties,
- apps met informatie over valsspelen die van invloed zijn op de spelbeleving van andere apps,
- apps die instructies bevatten over het hacken van services, software of hardware of dit mogelijk maken, of die beveiligingsmaatregelen omzeilen,
- apps die toegang krijgen tot een service of API of deze gebruiken op een manier die de servicevoorwaarden ervan schendt,
- apps die niet in aanmerking komen voor opname op de witte lijst en die proberen het energiebeheer van het systeem te omzeilen,
- apps die proxyservices naar derden mogelijk maken, mogen dat alleen doen in apps waar dat het primaire, op gebruikers gerichte doel van de app is,
- apps of code van derden (bijvoorbeeld SDK's die uitvoerbare code (zoals DEX-bestanden of native code) downloaden via een andere bron dan Google Play,
- apps die andere apps installeren op een apparaat zonder voorafgaande toestemming van de gebruiker,
- apps die een link bevatten naar kwaadwillende software of de distributie of installatie daarvan mogelijk maken.

Misleidend gedrag

We staan geen apps toe die gebruikers proberen te misleiden of oneerlijk gedrag mogelijk maken, waaronder, maar niet beperkt tot, apps waarvan is bepaald dat ze functioneel onmogelijk zijn. Apps moeten een nauwkeurige kennisgeving,

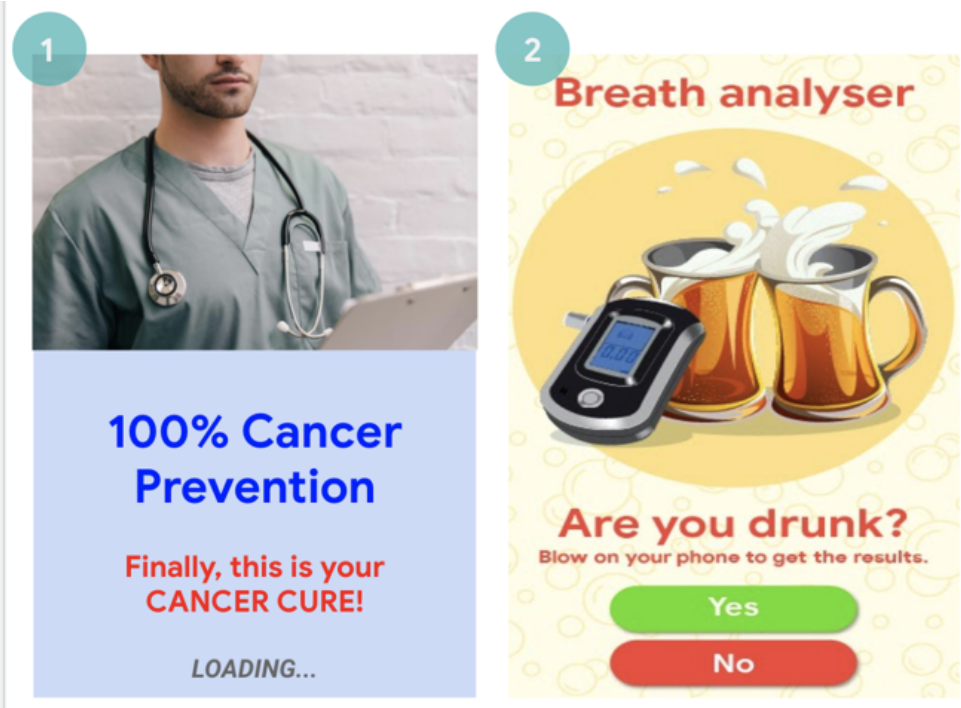
beschrijving en afbeeldingen/video van hun functionaliteit verstrekken in alle onderdelen van de metadata. Apps mogen geen functies of waarschuwingen nabootsen van het besturingssysteem of van andere apps. Wijzigingen in de apparaatinstellingen moeten worden doorgevoerd met medeweten en toestemming van de gebruiker en door de gebruiker ongedaan kunnen worden gemaakt.

Misleidende claims

We staan geen apps toe die onjuiste of misleidende informatie bevatten, waaronder in de beschrijving, de titel, het icoon en screenshots.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Onduidelijke of onjuiste beschrijving van de functionaliteit van apps:
  - Een app die stelt een racegame te zijn in de beschrijving en screenshots, maar in feite een puzzelgame is waar een afbeelding van een auto wordt gebruikt.
  - Een app die stelt een antivirus-app te zijn, maar slechts een gids bevat met informatie over het verwijderen van virussen.
- Namen van ontwikkelaars of apps die misleidend zijn voor hun huidige status of prestaties op Play (bijv. 'Keuze van de redactie', 'Nummer 1-app', 'Populairste betaalde app').
- Apps met medische of gezondheidsgerelateerde content of functies die misleidend of mogelijk schadelijk zijn.
- Apps die stellen te beschikken over functies die niet uitgevoerd kunnen worden (zoals apps voor de bestrijding van insecten), zelfs niet als dit wordt weergegeven als grap, nep, enzovoort.
- Apps die onjuist zijn gecategoriseerd, waaronder, maar niet beperkt tot, de app-classificatie of app-categorie.
- Aantoonbaar misleidende content die processen bij verkiezingen kan verstoren.
- Apps die ten onrechte beweren gelieerd te zijn aan een overheidsinstantie of dat ze overheidsservices bieden of ondersteunen waarvoor ze niet geautoriseerd zijn.
- Apps die ten onrechte beweren de officiële app van een gevestigde entiteit te zijn. Een titel als 'Justin Bieber Official' is niet toegestaan zonder de noodzakelijke toestemming of rechten.



(1) Deze app bevat medische of gezondheidsgerelateerde beweringen (genezing van kanker) die misleidend zijn
(2) Deze apps stellen te beschikken over functies die niet kunnen worden uitgevoerd (bijvoorbeeld uw telefoon gebruiken als blaastest)

Misleidende wijzigingen in de apparaatinstellingen

We staan geen apps toe die zonder medeweten en toestemming van de gebruiker wijzigingen aanbrengen in de apparaatinstellingen van de gebruiker of in functies van andere apps. Apparaatinstellingen en functies omvatten tevens systeem- en browserinstellingen, bookmarks, sneltoetsen, iconen, widgets en de weergave van apps op het startscherm.

Daarnaast staan we ook het volgende niet toe:

- Apps die de apparaatinstellingen of functies wijzigen met toestemming van de gebruiker, maar dat zodanig doen dat de wijziging niet eenvoudig ongedaan gemaakt kan worden.
- Apps of advertenties die apparaatinstellingen of functies wijzigen als service aan derden of ten behoeve van advertenties.
- Apps die gebruikers misleiden om apps van derden te verwijderen of uit te schakelen of om apparaatinstellingen of functies te wijzigen.
- Apps die gebruikers aansporen of aanmoedigen om apps van derden te verwijderen of uit te schakelen of om apparaatinstellingen of functies te wijzigen, tenzij dit deel uitmaakt van een verifieerbare beveiligingsservice.

Oneerlijk gedrag mogelijk maken

We staan geen apps toe waarmee gebruikers anderen kunnen misleiden of die functioneel op welke manier dan ook misleidend zijn, met inbegrip van, maar niet beperkt tot, apps die identiteitsdocumenten, burgerservicenummers, paspoorten, diploma's, creditcards en rijbewijzen genereren of dit mogelijk maken. Apps moeten voorzien in nauwkeurige kennisgevingen, titels, beschrijvingen en afbeeldingen/video met betrekking tot de functies en/of content van de app. Ze moeten ook presteren zoals de gebruiker redelijkerwijs en terecht kan verwachten.

Aanvullende app-bronnen (zoals game-items) mogen alleen worden gedownload als ze noodzakelijk zijn voor het gebruik van de app door de gebruiker. Gedownloade resources moeten voldoen aan alle beleidsregels van Google Play en voordat de download wordt gestart, moet de app dit melden aan gebruikers en duidelijk de grootte van de download aangeven.

De mededeling dat een app een 'grapje' is of 'bestemd voor amusementsdoeleinden' (of soortgelijke bewoordingen) stelt een app niet vrij van de toepassing van onze beleidsregels.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps die andere apps of websites nabootsen zodat gebruikers worden misleid om hun persoonlijke en verificatiegegevens bekend te maken.
- Apps die niet-geverifieerde of echte telefoonnummers, contacten, adressen of persoonlijke identificeerbare informatie weergeven of afbeelden van individuen of entiteiten die hiervoor geen toestemming hebben verleend.
- Apps met verschillende kernfunctionaliteit op basis van de geografie, apparaatparameters of andere gebruikersafhankelijke gegevens van een gebruiker waarbij deze verschillen niet prominent aan de gebruiker worden getoond in de winkelvermelding.
- Apps die aanzienlijk wijzigingen aanbrengen tussen versies zonder de gebruiker te waarschuwen (bijvoorbeeld in het gedeelte 'Wat is er nieuw') en de winkelvermelding te updaten.
- Apps die proberen hun gedrag tijdens de beoordeling aan te passen of te obfusceren.
- Apps met door content delivery network (CDN) ondersteunde downloads die geen melding geven aan de gebruiker en de grootte van de download niet bekendmaken voorafgaand aan de download.

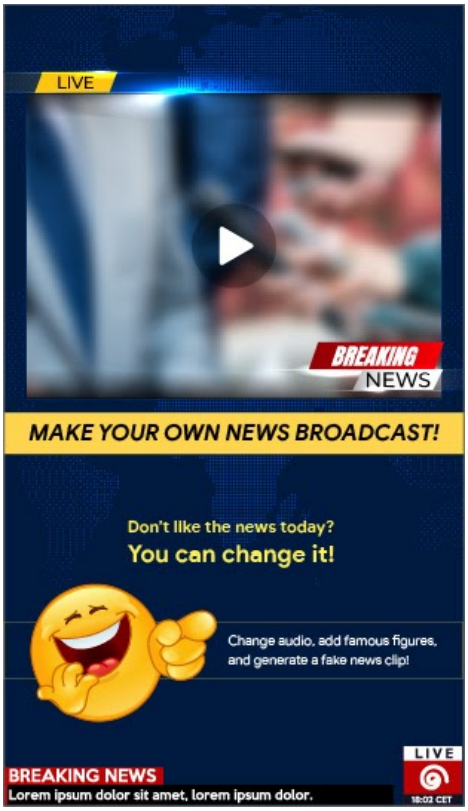
Gemanipuleerde media

We staan geen apps toe die onjuiste of misleidende informatie of claims promoten of helpen maken die worden overgebracht via afbeeldingen, video's en/of tekst. We staan geen apps toe waarvan is vastgesteld dat ze aantoonbaar misleidende of bedrieglijke afbeeldingen, video's en/of tekst bevatten of verspreiden en die schade kunnen toebrengen aan een gevoelig evenement, de politiek, sociale kwesties of andere zaken van publiek belang.

Apps die media manipuleren of wijzigen, als dat verder gaat dan gebruikelijke en redactioneel aanvaardbare aanpassingen voor duidelijkheid of kwaliteit, moeten gewijzigde media als zodanig bekendmaken of watermerken als het voor de doorsnee persoon mogelijk niet duidelijk is dat de media is gewijzigd. Er kunnen uitzonderingen worden gemaakt voor het publieke belang of voor een duidelijke satire of parodie.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- apps die een publiek figuur toevoegen aan een demonstratie tijdens een politiek gevoelig evenement;
- apps die publieke figuren of media van een gevoelig evenement gebruiken om de mogelijkheden om media te wijzigen te promoten in de winkelvermelding van een app;
- apps die mediaclips wijzigen om een nieuwsuitzending te imiteren.



(1) Deze app biedt functionaliteit om mediaclips te wijzigen om een nieuwsuitzending na te bootsen en zonder watermerk beroemde of openbare personen aan de clip toe te voegen.

Verkeerde voorstelling

We staan geen apps of ontwikkelaarsaccounts toe die zich voordoen als personen of organisaties of die een verkeerde voorstelling geven van hun eigenaar of primaire doel of deze informatie verbergen. We staan geen apps of ontwikkelaarsaccounts toe die betrokken zijn bij gecoördineerde activiteiten om gebruikers te misleiden. Dit omvat, maar is niet beperkt tot, apps of ontwikkelaarsaccounts die een verkeerde voorstelling geven van hun land van herkomst of dit verbergen en die content weergeven aan gebruikers in een ander land.

Malware

Malware is elke code die een gebruiker, de gegevens van een gebruiker of een apparaat in gevaar brengt. Malware omvat, maar is niet beperkt tot, potentieel schadelijke apps (Potentially Harmful Applications, PHA), binaire bestanden of frameworkaanpassingen, bestaande uit categorieën zoals Trojaanse paarden, phishing en spyware-apps. We updaten deze lijst voortdurend en voegen nieuwe categorieën toe.

Malware

Ons malwarebeleid is simpel: het Android-ecosysteem, inclusief de Google Play Store, en apparaten van gebruikers moeten vrij zijn van kwaadwillend gedrag (d.w.z. malware). Met behulp van dit fundamentele beginsel streven we ernaar om een beveiligd Android-ecosysteem te bieden voor onze gebruikers en hun Android-apparaten.

Hoewel er verschillende typen malware zijn met verschillende mogelijkheden, heeft malware meestal een van de volgende doelen:

- de integriteit van het apparaat van de gebruiker in gevaar brengen,
- de controle verkrijgen over het apparaat van een gebruiker,
- activiteiten op afstand mogelijk maken voor een aanvaller om toegang te krijgen tot een besmet apparaat, dit te gebruiken of op een andere manier te exploiteren,
- persoonsgegevens of andere gegevens van het apparaat halen zonder toereikende kennisgeving of toestemming,
- spam of opdrachten verspreiden vanaf het besmette apparaat naar andere apparaten of netwerken,
- de gebruiker oplichten.

Een app, binair bestand of frameworkaanpassing kan potentieel schadelijk zijn, en dus kwaadwillend gedrag genereren, zelfs als het niet de bedoeling was om schadelijk te zijn. Dit komt omdat apps, binaire bestanden of

frameworkaanpassingen anders kunnen functioneren, afhankelijk van veel verschillende variabelen. Oftewel: iets wat schadelijk is voor het ene Android-apparaat, hoeft mogelijk geen risico te vormen voor een ander Android-apparaat. Een apparaat waarop bijvoorbeeld de nieuwste versie van Android wordt uitgevoerd, heeft geen last van schadelijke apps die gebruikmaken van beëindigde API's om schadelijk gedrag uit te voeren. Een apparaat waarop nog een zeer vroege versie van Android wordt uitgevoerd, kan echter risico lopen. Apps, binaire bestanden of frameworkaanpassingen worden gemarkeerd als malware of PHA als ze duidelijk een risico vormen voor sommige of alle Android-apparaten en gebruikers.

De onderstaande malwarecategorieën weerspiegelen onze fundamentele overtuiging dat gebruikers moeten begrijpen hoe hun apparaat wordt gebruikt. Ze promoten ook een beveiligd ecosysteem dat robuuste innovatie en een vertrouwde gebruikerservaring mogelijk maakt.

Ga naar Google Play Protect voor meer informatie.

Backdoors

Code waarmee ongewenste, potentieel schadelijke bewerkingen op afstand kunnen worden uitgevoerd op een apparaat.

Deze bewerkingen kunnen onder meer bestaan uit gedrag waardoor de app, het binaire bestand of de frameworkaanpassing in een van de andere malwarecategorieën kan worden geplaatst als het automatisch wordt uitgevoerd. 'Backdoor' (achterdeur) is een algemene beschrijving van de manier waarop potentieel schadelijke bewerkingen kunnen worden uitgevoerd op een apparaat. Daarom komt dit niet volledig overeen met categorieën als factureringsfraude of commerciële spyware. Als gevolg daarvan kan een subset van dergelijke backdoors onder bepaalde omstandigheden door Google Play Protect worden behandeld als een kwetsbaarheid.

Factureringsfraude

Code waarmee op een opzettelijk misleidende manier automatisch kosten in rekening worden gebracht aan de gebruiker.

Telecomfraude wordt opgesplitst in sms-fraude, belfraude en telefoonrekeningfraude.

Sms-fraude

Code die kosten in rekening brengt aan gebruikers om zonder toestemming premium sms-berichten te sturen of die probeert de bijbehorende sms-activiteiten te verhullen door kennisgevingsovereenkomsten of sms-berichten van de mobiele provider te verbergen waarin de gebruiker op de hoogte wordt gesteld van kosten of waarin abonnementen worden bevestigd.

Bepaalde code (hoewel deze technisch gezien het gedrag met betrekking tot het sturen van sms-berichten bekend maakt) introduceert aanvullend gedrag dat sms-fraude mogelijk maakt. Voorbeelden omvatten het verbergen of onleesbaar maken van delen van een kennisgevingsovereenkomst voor de gebruiker of het voorwaardelijk onderdrukken van sms-berichten van de mobiele provider waarin de gebruiker op de hoogte wordt gesteld van kosten of waarin een abonnement wordt bevestigd.

Belfraude

Code waarmee kosten in rekening worden gebracht aan gebruikers door premium nummers te bellen zonder toestemming van de gebruiker.

Telefoonrekeningfraude

Code die gebruikers misleidt zodat ze zich abonneren of content kopen via hun mobiele telefoonrekening.

Telefoonrekeningfraude omvat elk type facturering, met uitzondering van premium sms-berichten en premium gesprekken. Voorbeelden hiervan omvatten rechtstreekse facturering via provider, draadloze toegangspunten (WAP) en overdracht van mobiele zendtijd. WAP-fraude is een van de meest voorkomende typen telefoonrekeningfraude. WAP-fraude kan gebruikers misleiden zodat ze op een knop klikken in een transparante WebView die onzichtbaar is geladen. Als de gebruiker de actie uitvoert, wordt een abonnement gestart dat steeds wordt verlengd. De sms of e-mail ter bevestiging wordt vaak onderschept om te voorkomen dat gebruikers de financiële transactie opmerken.

Stalkerware

Code die persoonlijke informatie vanaf het apparaat overdraagt zonder voldoende kennisgeving of toestemming en geen permanente melding weergeeft dat dit gebeurt.

Stalkerware-apps dragen meestal gegevens over aan een andere partij dan de PHA-provider.

Acceptabele varianten van deze apps kunnen door ouders worden gebruikt om hun kinderen in de gaten te houden. Deze apps mogen echter niet worden gebruikt om een persoon (bijvoorbeeld een echtgenoot/echtgenote) in de gaten te

houden zonder zijn of haar medeweten of toestemming, tenzij er een permanente melding wordt weergegeven als de gegevens worden overgedragen.

Alleen apps die zich houden aan het beleid en die exclusief zijn ontworpen en in de handel worden gebracht voor ouderlijk toezicht (waaronder in gezinsapps) of ondernemingsbeheer mogen in de Play Store worden verspreid met tracking- en rapportagefuncties, mits ze volledig voldoen aan de onderstaande vereisten.

Niet-stalkerware-apps die in de Play Store worden gedistribueerd en het gedrag van een gebruiker monitoren of bijhouden op een apparaat, moeten aan deze vereisten voldoen:

- Apps mogen zich niet presenteren als een spionage-oplossing of als oplossing voor geheim toezicht.
- Apps mogen geen trackinggedrag verbergen of verhullen of gebruikers proberen te misleiden over dergelijke functies.
- Apps moeten gebruikers een permanente melding en een uniek icoon aanbieden waarmee de app duidelijk kan worden geïdentificeerd.
- Apps en app-vermeldingen op Google Play mogen geen middelen bieden om functies te activeren of toegankelijk te maken die deze voorwaarden schenden, zoals een link naar een ongeschikte APK die buiten Google Play wordt gehost.
- U bent als enige verantwoordelijk voor het bepalen van de wettigheid van uw app op de getargete locatie. Apps waarvan wordt vastgesteld dat ze onwettig zijn op de locaties waar ze zijn gepubliceerd, worden verwijderd.

Denial of Service (DoS)

Code die, zonder medeweten van de gebruiker, een DoS-aanval (Denial of Service) uitvoert of deel uitmaakt van een gedistribueerde DoS-aanval tegen andere systemen en bronnen.

Dit kan bijvoorbeeld worden gedaan door een groot aantal HTTP-verzoeken te sturen om overmatige belasting op externe servers te produceren.

Schadelijke downloaders

Code die zelf niet schadelijk is, maar andere PHA's downloadt.

In de volgende gevallen kan code een schadelijke downloader zijn:

- Er is reden om aan te nemen dat de code is gemaakt om PHA's te verspreiden en de code heeft PHA's gedownload of bevat code waarmee apps kunnen worden gedownload en geïnstalleerd, of
- Ten minste vijf procent van de apps die door de code worden gedownload zijn PHA's met een minimum drempel van 500 waargenomen app-downloads (25 waargenomen PHA-downloads).

Grote browsers en apps voor het delen van bestanden worden niet beschouwd als schadelijke downloaders op voorwaarde dat het volgende van toepassing is:

- Ze genereren geen downloads zonder interactie van de gebruiker, en
- Alle PHA-downloads worden gestart door gebruikers die hiervoor toestemming hebben gegeven.

Niet-Android-dreiging

Code die niet-Android-dreigingen bevat.

Deze apps kunnen geen schade toebrengen aan de Android-gebruiker of het Android-apparaat, maar bevatten componenten die mogelijk schadelijk zijn voor andere platforms.

Phishing

Code die doet alsof deze afkomstig is van een betrouwbare bron, verzoekt om de verificatie- of factureringsgegevens van een gebruiker en deze gegevens doorstuurt naar een derde. Deze categorie is ook van toepassing op code die de overdracht van inloggegevens van gebruikers onderschept tijdens de overdracht.

Veelvoorkomende doelen van phishing zijn onder meer bankgegevens, creditcardnummers en inloggegevens van online accounts voor sociale netwerken en games.

Misbruik van hogere rechten

Code die de integriteit van het systeem in gevaar brengt door de sandbox van de app te doorbreken, rechten op een hoger niveau te verkrijgen of toegang tot belangrijke beveiligingsgerelateerde functies te wijzigen of uit te schakelen.

Voorbeelden hiervan zijn:

- een app die het rechtenmodel van Android schendt of inloggegevens (zoals OAuth-tokens) steelt uit andere apps,
- apps die functies misbruiken om te voorkomen dat ze worden verwijderd of gestopt,
- een app die SELinux uitschakelt.

Apps die zich rechten toe-eigenen en apparaten rooten zonder toestemming van de gebruiker, worden geclassificeerd als root-apps.

Gijzelsoftware

Code die de gedeeltelijke of uitgebreide controle van een apparaat of gegevens op een apparaat overneemt en vereist dat de gebruiker een betaling uitvoert of een actie onderneemt om de controle te herstellen.

Sommige gijzelsoftware versleutelt gegevens op het apparaat en vraagt om een betaling om gegevens te ontsleutelen en/of gebruik te kunnen maken van de beheerdersfuncties, zodat deze niet kunnen worden verwijderd door een normale gebruiker. Voorbeelden hiervan zijn:

- een gebruiker de toegang tot zijn of haar apparaat ontzeggen en vragen om geld om de controle van de gebruiker te herstellen,
- gegevens op het apparaat versleutelen en vragen om een betaling, ogenschijnlijk om de gegevens te ontsleutelen,
- gebruikmaken van de beheerdersfuncties voor het apparaatbeleid en verwijdering door de gebruiker blokkeren.

Code die wordt verstrekt bij het apparaat waarvan het primaire doel uitbesteed apparaatbeheer is, kan worden uitgesloten van de categorie 'gijzelsoftware', mits deze voldoet aan de vereisten voor beveiligde vergrendeling en beheer en beschikt over toereikende kennisgevingen en toestemmingsvereisten voor gebruikers.

Rooten

Code waarmee het apparaat wordt geroot.

Er is een verschil tussen niet-schadelijke en schadelijke root-code. Niet-schadelijke root-apps laten de gebruiker bijvoorbeeld van tevoren weten dat ze het apparaat gaan rooten en voeren geen andere mogelijk schadelijke acties uit die van toepassing zijn op andere PHA-categorieën.

Schadelijke root-apps laten de gebruiker niet weten dat ze het apparaat gaan rooten of stellen de gebruiker van tevoren op de hoogte van het rooten maar voeren ook andere acties uit die van toepassing zijn op andere PHA-categorieën.

Spam

Code die ongevraagde berichten stuurt naar de contacten van de gebruiker of het apparaat gebruikt als relayservice voor spamberichten.

Spyware

Code die persoonsgegevens verstuurt vanaf het apparaat zonder toereikende kennisgeving of toestemming.

De overdracht van de volgende informatie zonder kennisgeving of op een manier die de gebruiker niet verwacht, is bijvoorbeeld voldoende om als spyware te worden beschouwd:

- Contactenlijst
- Foto's of andere bestanden die op een SD-kaart staan of die geen eigendom zijn van de app
- Content uit gebruikersmail
- Gesprekslijst
- Sms-lijst
- Internetgeschiedenis of browserbookmarks van de standaardbrowser
- Informatie afkomstig uit de /data/-directories van andere apps.

Gedrag dat kan worden beschouwd als het bespioneren van de gebruiker, kan ook worden gemarkeerd als spyware. Bijvoorbeeld audio opnemen of gesprekken vastleggen die op de telefoon binnenkomen of app-gegevens stelen.

Trojaans paard

Code die goedaardig lijkt te zijn, zoals een game die zegt alleen een game te zijn, maar toch ongewenste acties uitvoert tegen de gebruiker.

Deze indeling wordt meestal gebruikt in combinatie met andere PHA-categorieën. Een Trojaans paard beschikt over een onschadelijke component en een verborgen schadelijke component. Een voorbeeld is een game die op de achtergrond en zonder medeweten van de gebruiker premium sms-berichten verstuurt vanaf het apparaat van de gebruiker.

Opmerkingen over ongebruikelijke apps

Nieuwe en zeldzame apps kunnen worden ingedeeld als 'ongebruikelijk' als Google Play Protect niet voldoende informatie heeft om ze als beveiligd in te delen. Dit houdt niet in dat de app noodzakelijkerwijs schadelijk is, maar zonder nadere beoordeling kan deze ook niet worden ingedeeld als beveiligd.

Opmerkingen over de categorie 'backdoor'

De malwarecategorie 'backdoor' is gebaseerd op de manier waarop de code actief is. Code wordt geclassificeerd als een backdoor als deze gedrag mogelijk maakt waardoor de code in een van de andere malwarecategorieën zou worden ingedeeld als deze automatisch wordt uitgevoerd. Als een app bijvoorbeeld toestaat dat code dynamisch wordt geladen en de dynamisch geladen code sms-berichten extraheert, wordt deze ingedeeld als backdoor-malware.

Als een app echter toestaat dat code willekeurig wordt uitgevoerd en we geen reden hebben om aan te nemen dat de uitvoering van deze code is toegevoegd om schadelijk gedrag uit te voeren, wordt de app behandeld als een app met een kwetsbaarheid en niet als backdoor-malware. De ontwikkelaar wordt dan gevraagd een patch te ontwikkelen.

Ongewenste mobiele software

Dit beleid is gebaseerd op het Google-beleid voor ongewenste software door de principes voor het Android-ecosysteem en de Google Play Store te beschrijven. Software die deze principes schendt, kan schadelijk zijn voor de gebruikerservaring en wij zullen stappen ondernemen om gebruikers er tegen te beschermen.

Ongewenste mobiele software

Bij Google geloven we dat als we ons richten op de gebruiker, de rest vanzelf volgt. In onze softwareprincipes en het beleid voor ongewenste software geven we algemene aanbevelingen voor software die een goede gebruikerservaring biedt. Dit beleid is gebaseerd op het Google-beleid voor ongewenste software door de principes voor het Android-ecosysteem en de Google Play Store te beschrijven. Software die deze principes schendt, kan schadelijk zijn voor de gebruikerservaring en wij zullen stappen ondernemen om gebruikers er tegen te beschermen.

Zoals vermeld in het beleid voor ongewenste software, hebben we vastgesteld dat de meeste ongewenste software een of meer van dezelfde basiskenmerken heeft:

- De software is misleidend, de waardepropositie wordt niet nagekomen.
- Er wordt geprobeerd gebruikers over te halen de software te installeren of de software wordt samen met een ander programma geïnstalleerd.
- De software stelt de gebruiker niet op de hoogte van alle hoofdfuncties en andere belangrijke functies.
- De software beïnvloedt het systeem van de gebruiker op onverwachte manieren.
- De software verzamelt of verstuurt persoonlijke gegevens zonder medeweten van de gebruiker.
- De software verzamelt of verstuurt persoonlijke gegevens zonder een veilige afhandeling (bijvoorbeeld overdracht via HTTPS).
- De software wordt als onderdeel van een pakket geleverd (samen met andere software) en de aanwezigheid van die software wordt niet bekendgemaakt.

Op mobiele apparaten is software code in de vorm van een app, binair bestand, frameworkaanpassing, enz. We ondernemen actie tegen code die deze principes schendt om software die schadelijk is voor het software-ecosysteem of die de gebruikerservaring verstoort te voorkomen.

Hieronder gebruiken we het beleid voor ongewenste software als basis om de toepasselijkheid ervan uit te breiden naar mobiele software. Net als bij dat beleid zullen we dit beleid voor mobiele ongewenste software blijven verfijnen om nieuwe vormen van misbruik aan te pakken.

Transparant gedrag en duidelijke openbaarmakingen

Alle code moet beloften die aan de gebruiker zijn gedaan waarmaken. Apps moeten alle meegedeelde functionaliteit bieden. Apps mogen gebruikers niet in verwarring brengen.

- Apps moeten duidelijk zijn over de functionaliteit en doelen.
- Leg de gebruiker expliciet en duidelijk uit welke systeemwijzigingen door de app worden aangebracht. Stel gebruikers in staat alle belangrijke installatieopties en wijzigingen te bekijken en goed te keuren.
- Software mag de status van het apparaat van de gebruiker niet verkeerd weergeven aan de gebruiker, bijvoorbeeld door te claimen dat het systeem zich in een kritieke beveiligingsstatus bevindt of is geïnfecteerd met virussen.
- Gebruik geen ongeldige activiteit die is bedoeld om meer advertentieverkeer en/of meer conversies te genereren.
- We staan geen apps toe die gebruikers misleiden door zich voor te doen als iemand anders (bijvoorbeeld een andere ontwikkelaar, bedrijf, entiteit) of een andere app. Wek niet de indruk dat uw app is gerelateerd aan of geautoriseerd door iemand anders.

Voorbeelden van schendingen:

- Advertentiefraude
- Nabootsing van identiteit

Bescherm gebruikersgegevens

Wees duidelijk en transparant over de toegang, het gebruik, de verzameling en het delen van persoonlijke en gevoelige gebruikersgegevens. Het gebruik van gebruikersgegevens moet voldoen aan alle relevante beleidsregels voor gebruikersgegevens, indien van toepassing, en alle voorzorgsmaatregelen nemen om de gegevens te beschermen.

- Bied gebruikers de mogelijkheid om akkoord te gaan met de verzameling van hun gegevens voordat u deze vanaf het apparaat verzamelt en verstuurt, inclusief gegevens over accounts van derden, e-mail, telefoonnummer, geïnstalleerde apps, bestanden, locatie en andere persoonlijke en gevoelige gegevens waarvan de gebruiker niet verwacht dat deze worden verzameld.
- Persoonlijke en gevoelige gebruikersgegevens die worden verzameld, moeten beveiligd worden verwerkt en moeten worden verstuurd via moderne cryptografie (bijvoorbeeld via HTTPS).
- Software, inclusief mobiele apps, mag alleen persoonlijke en gevoelige gebruikersgegevens naar servers sturen voor zover dit verband houdt met de functionaliteit van de app.

Voorbeelden van schendingen:

- Gegevensverzameling (zie Spyware)
- Misbruik van beperkte rechten

Voorbeeld van beleid voor gebruikersgegevens:

- *Beleid voor gebruikersgegevens van Google Play*
- *Beleid betreffende GMS-vereisten voor gebruikersgegevens*
- *Beleid voor gebruikersgegevens van de Google API-service*

De mobiele functionaliteit niet schaden

De gebruikerservaring moet eenvoudig en begrijpelijk zijn en gebaseerd op duidelijke keuzes die de gebruiker heeft gemaakt. De functionaliteit moet een duidelijke waardepropositie bevatten voor de gebruiker en de geadverteerde of gewenste gebruikerservaring niet verstoren.

- Geef geen advertenties weer die op onverwachte manieren aan gebruikers worden weergegeven, waardoor bijvoorbeeld de bruikbaarheid van apparaatfuncties wordt belemmerd of verstoord, of die buiten de trigger-omgeving van de app worden weergeven zonder gemakkelijk te kunnen worden gesloten en voldoende toestemming en toeschrijving.
- Apps mogen andere apps of de bruikbaarheid van het apparaat niet verstoren.
- De verwijdering, indien van toepassing, moet duidelijk zijn.
- Mobiele software mag geen prompts van het besturingssysteem van het apparaat of andere apps nabootsen. Onderdruk geen meldingen van andere apps of van het besturingssysteem voor de gebruiker, met name meldingen die de gebruiker informeren over wijzigingen in het besturingssysteem.

Voorbeelden van schendingen:

- Storende advertenties
- Onbevoegd gebruik of nabootsing van systeemfuncties

Advertentiefraude

Advertentiefraude is ten strengste verboden. Advertentie-interacties die worden gegenereerd om een advertentienetwerk te laten geloven dat verkeer afkomstig is van oprechte interesse van gebruikers, is advertentiefraude, een vorm van ongeldig verkeer. Advertentiefraude kan het gevolg zijn van ontwikkelaars die advertenties op verboden manieren implementeren, zoals verborgen advertenties weergeven, automatisch op advertenties klikken, informatie wijzigen of aanpassen of op een andere manier gebruikmaken van niet-menselijke acties (spiders, bots, enzovoort) of menselijke activiteiten die zijn bedoeld om ongeldig advertentieverkeer te produceren. Ongeldig verkeer en advertentiefraude zijn schadelijk voor adverteerders, ontwikkelaars en gebruikers en leiden tot langdurig verlies van vertrouwen in het ecosysteem van mobiele advertenties.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Een app die advertenties weergeeft die niet zichtbaar zijn voor de gebruiker.
- Een app die automatisch klikken op advertenties genereert zonder de bedoeling van de gebruiker of die gelijkwaardig netwerkverkeer genereert om op frauduleuze wijze kliktegoeden te verstrekken.

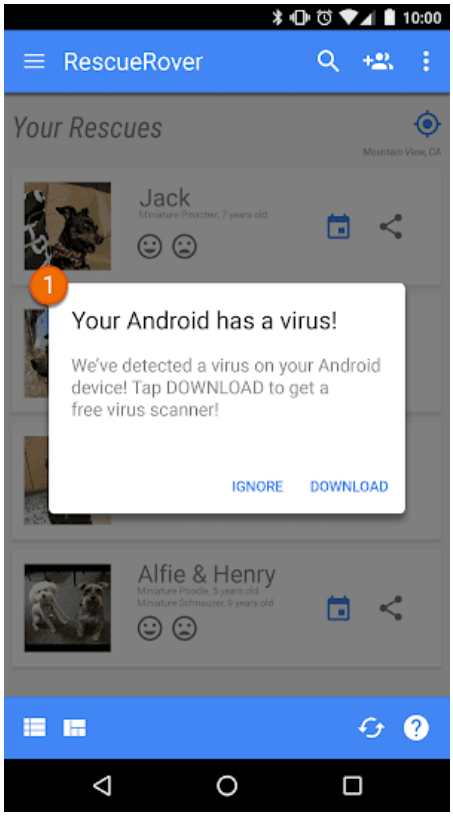
- Een app die onjuiste klikken voor installatietoeschrijving verstuurt om betaald te worden voor installaties die niet afkomstig zijn van het netwerk van de afzender.
- Een app die advertenties weergeeft als de gebruiker zich niet in de app-interface bevindt.
- Valse verklaringen over de advertentievoorraad door een app, bijvoorbeeld een app die communiceert met advertentienetwerken dat deze wordt uitgevoerd op een iOS-apparaat terwijl deze daadwerkelijk wordt uitgevoerd op een Android-apparaat. Een app die een onjuiste voorstelling geeft van de pakketnaam waarmee inkomsten worden gegenereerd.

Onbevoegd gebruik of nabootsing van systeemfuncties

We staan geen apps of advertenties toe die de systeemfunctionaliteit nabootsen of verstoren, zoals meldingen en waarschuwingen. Meldingen op systeemniveau mogen alleen worden gebruikt voor de integrale functies van een app, zoals de app van een luchtvaartmaatschappij die de gebruiker informeert over speciale aanbiedingen of een game die de gebruiker informeert over speciale aanbiedingen in de game.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps of advertenties die worden weergegeven door middel van een systeemmelding of -waarschuwing.



① De systeemmelding die in deze app wordt getoond, wordt gebruikt om een advertentie weer te geven.

Zie voor meer voorbeelden met advertenties het advertentiebeleid.

Nabootsing van identiteit

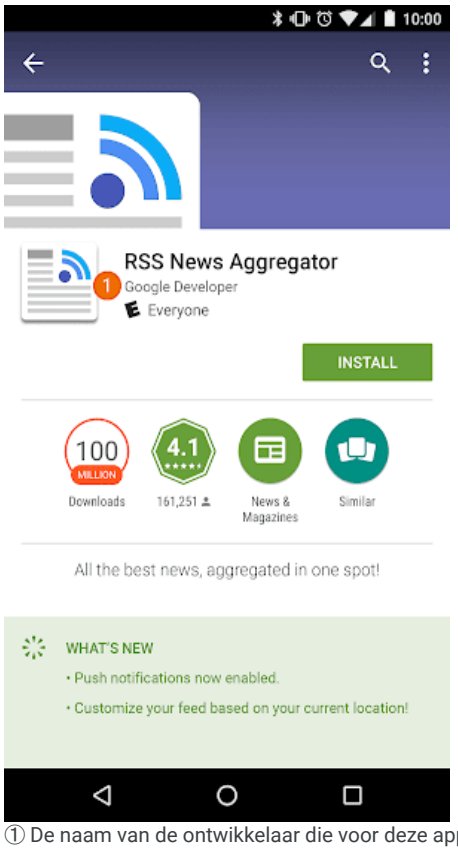
Als ontwikkelaars zich voordoen als anderen of de apps van anderen, worden gebruikers misleid en wordt de ontwikkelaarscommunity geschaad. We verbieden apps die gebruikers misleiden door zich voor te doen als iemand anders.

Nabootsing van identiteit

We staan geen apps toe die gebruikers misleiden door zich voor te doen als iemand anders (bijvoorbeeld een ander(e) ontwikkelaar, bedrijf, entiteit) of een andere app. Wek niet de indruk dat uw app is gerelateerd aan of geautoriseerd door iemand anders als dat niet zo is. Zorg ervoor dat u geen app-iconen, beschrijvingen, titels of in-app-elementen gebruikt die gebruikers kunnen misleiden over de relatie van uw app met iemand anders of een andere app.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

Ontwikkelaars die ten onrechte een relatie met een ander bedrijf/andere ontwikkelaar impliceren:

- 

① De naam van de ontwikkelaar die voor deze app wordt vermeld, suggereert een officiële relatie met Google, ook al bestaat een dergelijke relatie niet.

- De titel en iconen van een app lijken zo veel op die van bestaande producten of services dat gebruikers kunnen worden misleid:

Inkomsten genereren en advertenties

Google Play ondersteunt verschillende strategieën om inkomsten te genereren ten gunste van ontwikkelaars en gebruikers, waaronder betaalde distributie, in-app-producten, abonnementen en op advertenties gebaseerde modellen. We verplichten u te voldoen aan dit beleid om zo de beste gebruikerservaring te verzekeren.

Betalingen

Apps die gebruikmaken van in-store- of in-app-aankopen, moeten voldoen aan de volgende richtlijnen:

In-store-aankopen: Ontwikkelaars die kosten in rekening brengen voor apps en downloads vanuit Google Play, moeten gebruikmaken van het betaalsysteem van Google Play.

In-app-aankopen:

- Ontwikkelaars die producten aanbieden binnen een game die is gedownload van Google Play of die toegang biedt tot gamecontent, moeten in-app-facturering via Google Play gebruiken als betaalmethode.
- Ontwikkelaars die producten aanbieden in een andere app-categorie die wordt gedownload van Google Play, moeten in-app-facturering via Google Play gebruiken als betaalmethode, uitgezonderd in de volgende gevallen:
  - in gevallen waarbij de betaling uitsluitend voor fysieke producten is,

- in gevallen waarbij de betaling is bedoeld voor digitale content die buiten de app zelf kan worden gebruikt (zoals het kopen van muziek die ook in andere muziekspelers kan worden afgespeeld).
- Virtuele in-app-valuta's mogen alleen worden gebruikt in de app of gametitel waarin ze zijn gekocht.
- Ontwikkelaars mogen gebruikers niet misleiden omtrent de apps die ze verkopen of de services, producten, content of functionaliteit die ze in de apps zelf verkopen. Als uw productbeschrijving op Google Play verwijst naar in-app-functies waarvoor specifieke of aanvullende kosten gelden, moet uw beschrijving gebruikers duidelijk laten weten dat een betaling is vereist voor toegang tot die functies.
- Apps die mechanismen aanbieden om willekeurige virtuele items te ontvangen bij een aankoop (zogenoemde 'lootboxes'), moeten vóór de aankoop duidelijk vermelden hoe groot de kans is om de items te ontvangen.

Hier volgen enkele voorbeelden van producten die worden ondersteund door in-app-facturering via Google Play:

- **Virtuele gameproducten**, waaronder munten, edelstenen, extra levens of beurten, speciale items of materiaal/uitrusting, personages of avatars, extra levels of speeltijd.
- **App-functionaliteit of -content**, zoals een app zonder advertenties of nieuwe functies die niet beschikbaar zijn in de gratis versie.
- **Abonnementsservices**, zoals het streamen van muziek, video's, boeken of andere mediaservices; digitale publicaties, ook in combinatie met een fysieke editie; en sociale netwerkservices.
- **Cloudsoftwareproducten**, waaronder services voor dataopslag, zakelijke productiviteitssoftware en boekhoudsoftware.

Hier volgen enkele voorbeelden van producten die momenteel niet worden ondersteund door in-app-facturering via Google Play:

- **Handelswaar voor de detailhandel**, zoals boodschappen, kleding, huishoudelijke artikelen en elektronica.
- **Servicekosten**, waaronder taxi- en transportservices, schoonmaakservices, maaltijdbezorgservices, vliegtickets en tickets voor evenementen.
- **Eenmalige lidmaatschapskosten of terugkerende kosten**, waaronder een sportschoollidmaatschap, loyaliteitsprogramma's of clubs die accessoires, kleding of andere fysieke producten aanbieden.
- **Eenmalige betalingen**, waaronder peer-to-peer-betalingen, online veilingen en donaties.
- **Elektronische betaling van facturen**, waaronder creditcardrekeningen, rekeningen van nutsbedrijven en services van kabel- of telecombedrijven.

Houd er rekening mee dat we de Google Pay API aanbieden voor apps die fysieke producten en services verkopen. Ga voor meer informatie naar onze Google Pay-ontwikkelaarspagina.

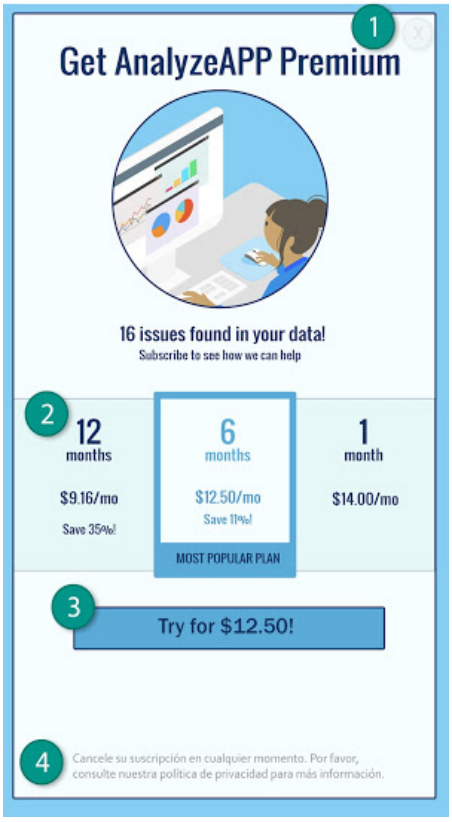
Abonnementen

Als ontwikkelaar mag u gebruikers niet misleiden over de abonnementsservices of -content die u aanbiedt binnen uw app. Het is uiterst belangrijk dat u in promoties in de app of op startschermen duidelijk communiceert over wat u aanbiedt.

In uw app: U moet transparant zijn over uw aanbieding. Dit houdt onder meer in dat u duidelijk moet zijn over de voorwaarden van de aanbieding, de kosten van het abonnement, hoe vaak u factureert en of gebruikers een abonnement nodig hebben om de app te kunnen gebruiken. Gebruikers moeten deze informatie zonder extra handelingen kunnen bekijken.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Maandabonnementen waarbij de gebruiker niet wordt geïnformeerd over de automatische maandelijkse verlenging en de kosten die daaruit voortkomen.
- Jaarabonnementen waarbij de meest zichtbare prijs de kosten per maand weergeeft.
- Abonnementsprijzen en -voorwaarden die niet volledig zijn gelokaliseerd.
- In-app-promoties die niet duidelijk aangeven dat een gebruiker toegang heeft tot de content zonder een abonnement (indien beschikbaar).
- SKU-namen die niet duidelijk maken wat de aard van het abonnement is, zoals 'Kosteloze proefperiode' voor een abonnement waarvan de verlenging telkens automatisch in rekening wordt gebracht.



① De knop 'Sluiten' is niet duidelijk zichtbaar en gebruikers begrijpen mogelijk niet dat ze toegang tot de functionaliteit hebben zonder het aangeboden abonnement te accepteren.

② De aanbieding geeft alleen de kosten per maand weer en gebruikers begrijpen mogelijk niet dat de kosten voor zes maanden in rekening wordt gebracht op het moment dat ze zich abonneren.

③ De aanbieding geeft alleen de introductieprijs weer en gebruikers begrijpen mogelijk niet welk bedrag automatisch in rekening worden gebracht na afloop van de introductieperiode.

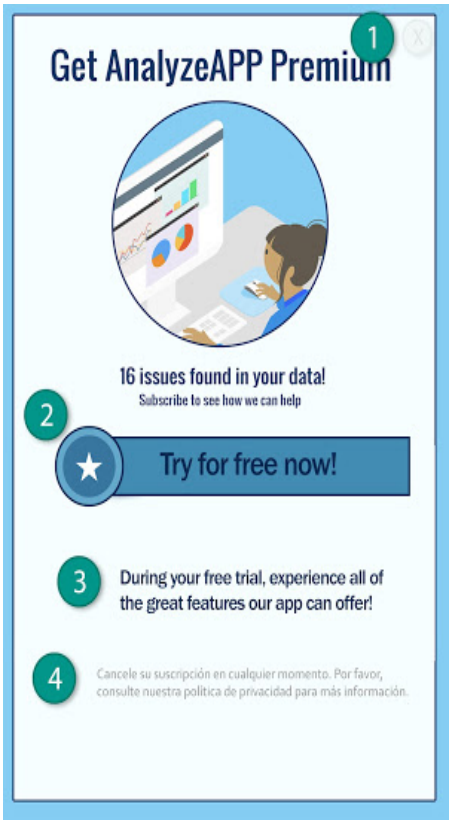
④ De aanbieding moet zijn gelokaliseerd in dezelfde taal als de algemene voorwaarden zodat gebruikers de volledige aanbieding kunnen begrijpen.

Kosteloze proefperioden en introductieaanbiedingen

Voordat een gebruiker wordt aangemeld voor uw abonnement: u moet een duidelijke en nauwkeurige beschrijving geven van de voorwaarden van uw aanbieding, waaronder de duur, de prijzen en een beschrijving van de toegankelijke content of services. Laat uw gebruikers weten hoe en wanneer een kosteloze proefperiode wordt omgezet in een betaald abonnement, hoeveel het betaalde abonnement kost. Vermeld ook dat ze het abonnement kunnen opzeggen als ze niet willen worden overgezet naar een betaald abonnement.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Aanbiedingen waarbij niet duidelijk wordt aangegeven hoelang de kosteloze proefperiode of de introductieprijs duurt.
- Aanbiedingen waarbij niet duidelijk wordt aangegeven dat de gebruiker automatisch wordt overgezet naar een betaald abonnement aan het einde van de aanbiedingsperiode.
- Aanbiedingen waarbij niet duidelijk wordt aangegeven dat een gebruiker toegang heeft tot content zonder een proefperiode (indien beschikbaar).
- Aanbiedingsprijzen en -voorwaarden die niet volledig zijn gelokaliseerd.



① De knop 'Sluiten' is niet duidelijk zichtbaar en gebruikers begrijpen mogelijk niet dat ze toegang tot de functionaliteit hebben zonder zich aan te melden voor een kosteloze proefperiode.

② De aanbieding benadrukt de kosteloze proefperiode en gebruikers begrijpen mogelijk niet dat aan het einde van de kosteloze proefperiode automatisch een bedrag in rekening wordt gebracht.

③ In de aanbieding staat geen proefperiode vermeld en gebruikers begrijpen mogelijk niet hoe lang de kosteloze toegang tot abonnementscontent duurt.

④ De aanbieding moet zijn gelokaliseerd in dezelfde taal als de algemene voorwaarden zodat gebruikers de volledige aanbieding kunnen begrijpen.

Abonnementen beheren en opzeggen

Als ontwikkelaar moet u ervoor zorgen dat uw app duidelijk kenbaar maakt hoe een gebruiker een abonnement kan beheren of opzeggen.

Het is uw verantwoordelijkheid om gebruikers te informeren over wijzigingen in uw abonnements-, opzeggings- en teruggavebeleid en ervoor te zorgen dat uw beleid voldoet aan de toepasselijke wetgeving.

Advertenties

We staan geen apps toe die misleidende of storende advertenties bevatten. Advertenties mogen alleen worden weergegeven binnen de app waarin ze worden getoond. We beschouwen apps die worden weergegeven in uw app als onderdeel van uw app. De in uw app getoonde advertenties moeten voldoen aan al onze beleidsregels. Klik hier voor het beleid voor kansspeladvertenties.

Gebruik van locatiegegevens voor advertenties

Apps die het gebruik van op rechten gebaseerde locatiegegevens van het apparaat uitbreiden voor de weergave van advertenties, vallen onder het beleid voor persoonlijke en gevoelige gegevens en moeten ook voldoen aan de volgende vereisten:

- Het gebruik of de verzameling van op rechten gebaseerde locatiegegevens van het apparaat voor advertentiedoeleinden moet duidelijk zijn voor de gebruiker en vastgelegd in het verplichte privacybeleid van de app, met inbegrip van links naar de privacybeleidsregels van advertentienetwerken die van toepassing zijn op het gebruik van locatiegegevens.

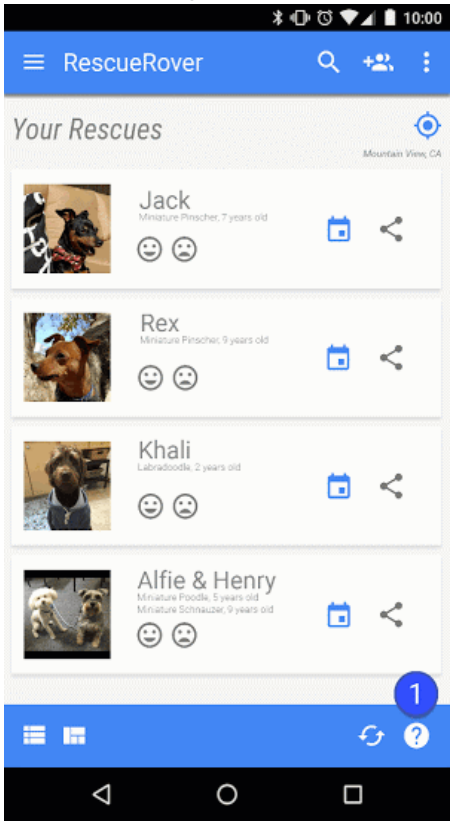
- In overeenstemming met de vereisten voor locatierechten mogen locatierechten alleen worden opgevraagd voor de uitvoering van de betreffende functies of services in uw app en mogen niet vragen om locatierechten van het apparaat uitsluitend voor het gebruik van advertenties.

Misleidende advertenties

Advertenties mogen de gebruikersinterface van een app of meldings- of waarschuwingselementen van een besturingssysteem niet simuleren of nabootsen. Het moet duidelijk zijn voor de gebruiker welke app een advertentie weergeeft.

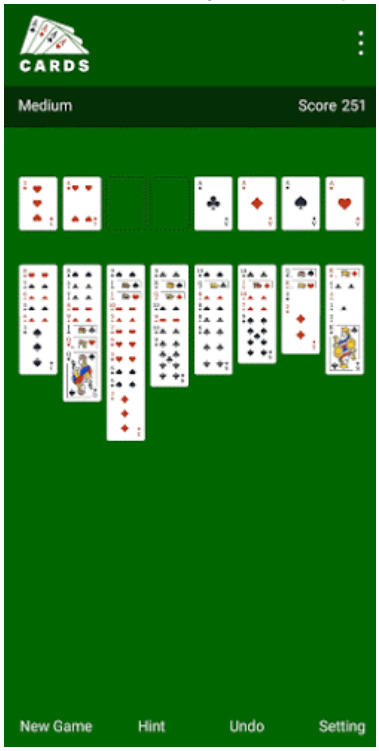
Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

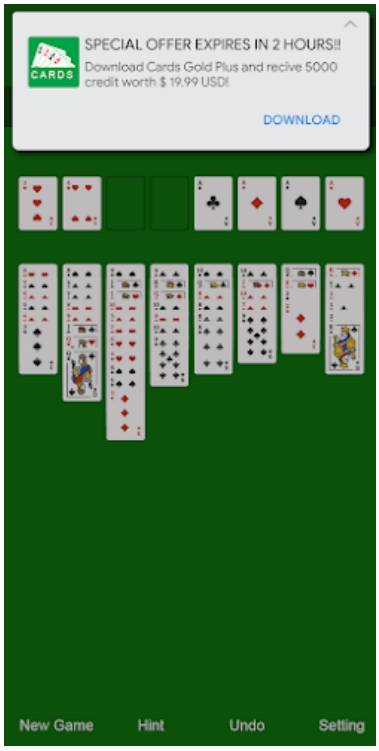
- Advertenties die de gebruikersinterface van een app nabootsen:



① Het vraagtekenicoon in deze app is een advertentie die de gebruiker omleidt naar een externe bestemmingspagina.

- Advertenties die een systeemmelding nabootsen:



- 

De voorbeelden hierboven geven advertenties weer die verschillende systeemmeldingen nabootsen.

Inkomsten genereren met een vergrendelingsscherm

Tenzij de app exclusief is bedoeld als vergrendelingsscherm, mogen apps geen advertenties of functies introduceren waarmee inkomsten worden gegenereerd via het vergrendelde scherm van een apparaat.

Storende advertenties

Storende advertenties zijn advertenties die op onverwachte manieren aan gebruikers worden weergegeven, die kunnen leiden tot onbedoelde klikken of die de bruikbaarheid van apparaatfuncties belemmeren of verstoren.

Uw app kan een gebruiker niet dwingen op een advertentie te klikken of persoonlijke gegevens voor advertentiedoeleinden te verstrekken voordat hij of zij een app volledig kan gebruiken. Interstitial-advertenties mogen

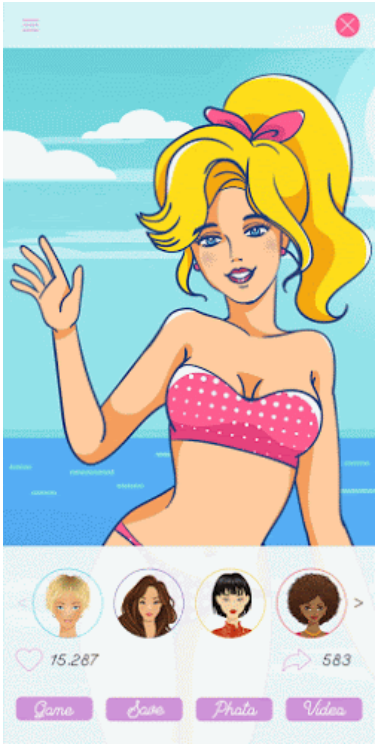
alleen worden weergegeven in de app die ze weergeeft. Als uw app interstitial-advertenties of andere advertenties weergeeft die het normale gebruik verstoren, moeten ze eenvoudig te sluiten zijn zonder dat dit tot problemen leidt.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

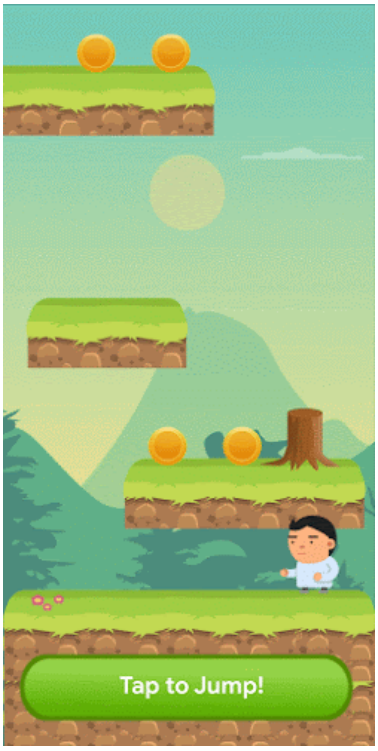
- Advertenties die het volledige scherm beslaan of normaal gebruik verstoren en geen duidelijke middelen bieden om de advertentie te sluiten:

① Deze advertentie heeft geen knop om te sluiten.

- Advertenties die de gebruiker dwingen door te klikken met een valse sluitknop, of door advertenties plotseling weer te geven in gedeelten van de app waar de gebruiker meestal op een andere functie tikt.



Een advertentie die een valse knop 'Sluiten' gebruikt



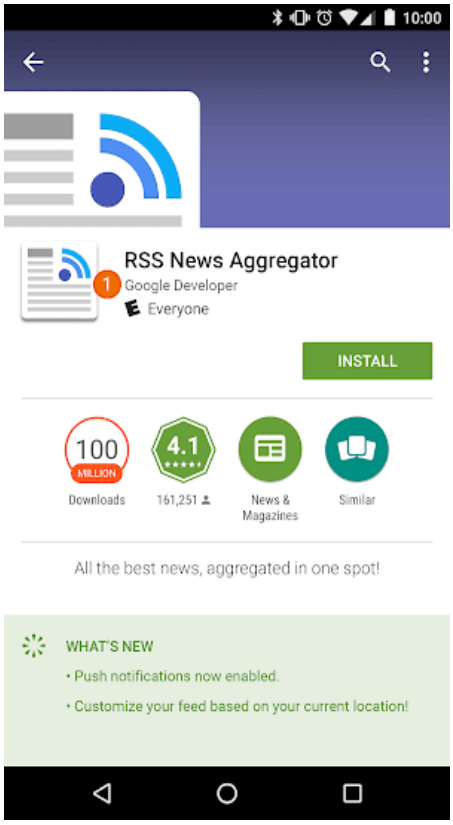
Een advertentie die plotseling wordt weergegeven in een gebied waar de gebruiker gewend is te tikken voor in-app-functies

Apps, advertenties van derden of apparaatfunctionaliteit verstoren

Advertenties die zijn gekoppeld aan uw app, mogen andere apps, advertenties of de werking van het apparaat niet verstoren, waaronder systeem- of apparaatknoppen en -poorten. Dit geldt onder andere voor overlays, bijbehorende functies en advertentieblokken met een widget. Advertenties mogen alleen worden weergegeven binnen de app waarin ze worden getoond.

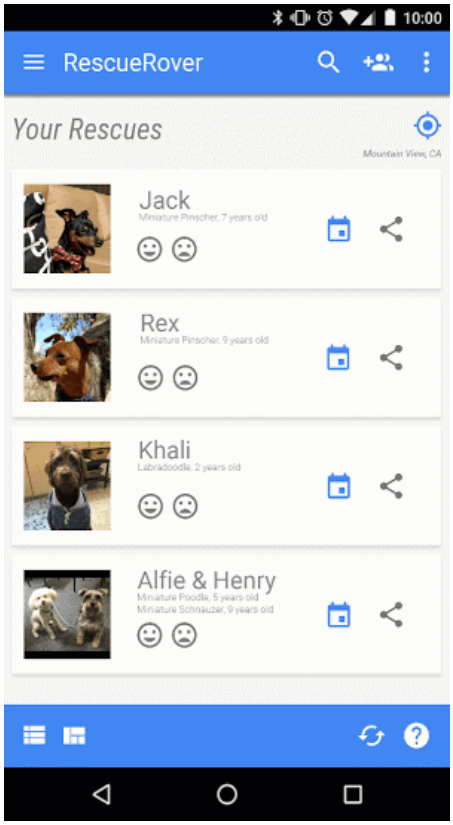
Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Advertenties die worden weergegeven buiten de app waarin ze worden getoond:



Beschrijving: De gebruiker gaat naar het startscherm vanuit deze app, en er wordt plotseling een advertentie weergegeven op het startscherm.

- Advertenties die worden geactiveerd door de startknop of andere functies die uitdrukkelijk zijn ontworpen om de app te verlaten:

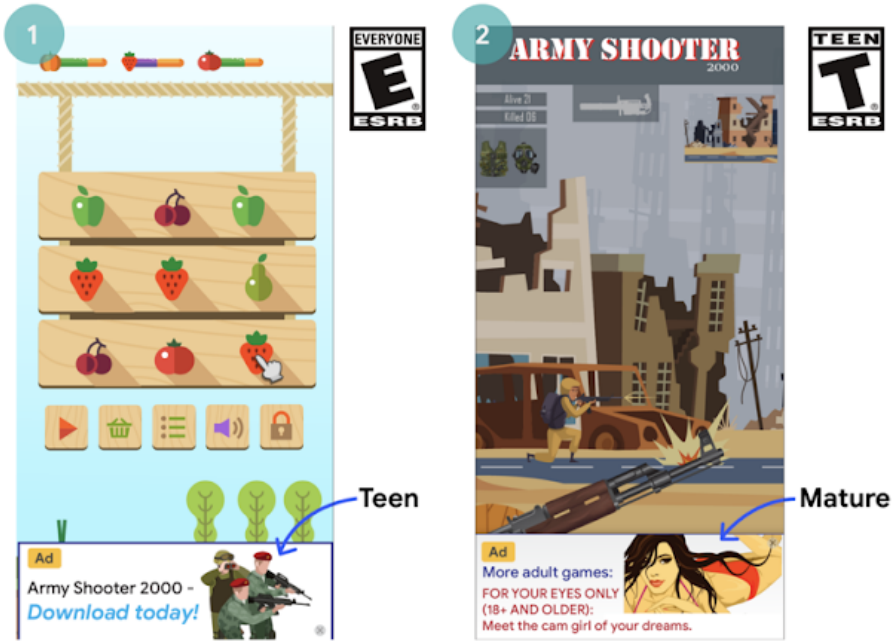


Beschrijving: De gebruiker probeert de app te verlaten en naar het startscherm te gaan, maar de verwachte gang van zaken wordt verstoord door een advertentie.

Ongepaste advertenties

De advertenties die worden weergegeven in je app, moeten geschikt zijn voor de beoogde doelgroep van je app, ook als de content op zich voldoet aan ons beleid.

Hieronder volgt een voorbeeld van een veelvoorkomende schending:



① Deze advertentie (Tieners) is ongepast voor de beoogde doelgroep van deze app (7+)
② Deze advertentie (Volwassenen) is ongepast voor de beoogde doelgroep van deze app (12+)

Gebruik van de Android-advertentie-ID

In Google Play-services versie 4.0 zijn nieuwe API's geïntroduceerd, evenals een ID die is bedoeld voor gebruik door advertentie- en analyseleveranciers. U vindt de gebruiksvoorwaarden voor deze ID hieronder.

- **Gebruik**. De Android-advertentie-ID mag alleen worden gebruikt voor advertentie- en gebruikersanalyse. De status van de instelling 'Afmelden voor op interesses gebaseerd adverteren' of 'Afmelden voor personalisatie van advertenties' moet worden geverifieerd bij elke toegang tot de ID.
- **Koppeling aan persoonlijk identificeerbare informatie of andere ID's**
  - Advertentiegebruik: de advertentie-ID mag niet voor advertentiedoeleinden worden gekoppeld aan permanente apparaat-ID's (zoals SSAID, MAC-adres, IMEI, enzovoort). De advertentie-ID mag alleen na uitdrukkelijke toestemming van de gebruiker worden gekoppeld aan persoonlijk identificeerbare informatie.
  - Gebruik van Analytics: De advertentie-ID mag alleen na uitdrukkelijke toestemming van de gebruiker worden gekoppeld aan persoonlijk identificeerbare informatie of aan een permanente apparaat-ID (zoals SSAID, MAC-adres, IMEI, enzovoort).
- **Selecties van gebruikers respecteren**. Bij opnieuw instellen mag een nieuwe advertentie-ID niet zonder uitdrukkelijke toestemming van de gebruiker worden gekoppeld aan een eerdere advertentie-ID of gegevens die zijn afgeleid van een eerdere advertentie-ID. Bovendien moet u de instelling 'Afmelden voor op interesses gebaseerd adverteren' of 'Afmelden voor personalisatie van advertenties' van een gebruiker respecteren. Als een gebruiker deze instelling heeft ingeschakeld, mag u de advertentie-ID niet gebruiken om gebruikersprofielen voor advertentiedoeleinden te maken of om gepersonaliseerde advertenties op gebruikers te targeten. Toegestane activiteiten omvatten contextueel adverteren, frequentielimieten, het bijhouden van conversies, rapportage en beveiliging en fraudedetectie.
- **Transparantie voor gebruikers**. Het feit dat de advertentie-ID wordt verzameld en gebruikt en dat u deze voorwaarden naleeft, moet openbaar worden gemaakt aan gebruikers in een privacymelding die voldoet aan de wettelijke vereisten. Raadpleeg ons beleid voor gebruikersgegevens voor meer informatie over onze privacynormen.
- **Gebruiksvoorwaarden naleven**. De advertentie-ID mag alleen worden gebruikt in overeenstemming met deze voorwaarden. Dit geldt ook voor derden waarmee u deze advertentie-ID deelt tijdens het uitvoeren van uw zakelijke werkzaamheden. Alle apps die worden geüpload naar of gepubliceerd op Google Play moeten de advertentie-ID (indien beschikbaar op een apparaat) in plaats van andere apparaat-ID's gebruiken voor advertentiedoeleinden.

Advertentieprogramma voor gezinnen

Als u advertenties weergeeft in uw app en de doelgroep ook kinderen omvat, zoals beschreven in het Gezinsbeleid, moet u advertentie-SDK's gebruiken die beschikken over zelfgecertificeerde naleving van het beleid van Google Play, met inbegrip van de onderstaande certificeringsvereisten voor advertentie-SDK's. Als de doelgroep van uw app zowel kinderen als oudere gebruikers omvat, moet u maatregelen voor het controleren van de leeftijd invoeren en ervoor zorgen dat advertenties die aan kinderen worden weergegeven, uitsluitend afkomstig zijn van een van deze zelfgecertificeerde advertentie-SDK's. Apps in het programma 'Gemaakt voor gezinnen' mogen uitsluitend zelfgecertificeerde advertentie-SDK's gebruiken.

Het gebruik van door Google Play gecertificeerde advertentie-SDK's is alleen vereist als u advertentie-SDK's gebruikt om advertenties weer te geven aan kinderen. Het volgende is toegestaan zonder de zelfcertificering van een advertentie-SDK bij Google Play. U bent er echter nog steeds verantwoordelijk voor dat uw gebruik van advertentiecontent en uw gegevensverzameling het beleid over gebruikersgegevens en het gezinsbeleid naleven:

- Eigen advertenties, waarbij u SDK's gebruikt om crosspromotie van uw apps of andere eigen media en merchandising te beheren
- Afsluiten van directe deals met adverteerders, waarbij u SDK's gebruikt voor voorraadbeheer

Certificeringsvereisten voor advertentie-SDK's

- Definieer wat aanstootgevende advertentiecontent en wat aanstootgevend gedrag inhoudt en verbied deze in de voorwaarden of het beleid van de advertentie-SDK. De definities moeten voldoen aan het programmabeleid voor ontwikkelaars van Play.
- Ontwikkel een methode om uw advertentiemateriaal te classificeren overeenkomstig speciale leeftijdsgroepen. Leeftijdsgroepen moeten in elk geval groepen omvatten voor iedereen en voor volwassenen. De classificeringsmethode moet overeenkomen met de methode die Google levert aan SDK's zodra die het onderstaande interesseformulier hebben ingevuld.
- Maak het voor uitgevers mogelijk om, per verzoek of per app, een behandeling van content die bedoeld is voor kinderen aan te vragen voor de weergave van advertenties. Deze behandeling moet voldoen aan de toepasselijke wet- en regelgeving, zoals de Amerikaanse Children's Online Privacy and Protection Act (COPPA) en de Algemene verordening gegevensbescherming (AVG) van de EU. Google Play vereist dat advertentie-SDK's gepersonaliseerde advertenties, op interesses gebaseerd adverteren en remarketing uitschakelen als onderdeel van de behandeling van content die bedoeld is voor kinderen.
- Sta uitgevers toe advertentie-indelingen te selecteren die voldoen aan het beleid voor advertenties voor gezinnen en inkomsten genereren van Play en voldoen aan de vereisten van het programma 'Goedgekeurd door docenten'.
- Zorg ervoor dat als realtime bieden wordt gebruikt om advertenties weer te geven aan kinderen, het advertentiemateriaal is beoordeeld en dat de privacyindicatoren worden bekendgemaakt aan de bieders.
- Verstrek Google voldoende informatie, zoals informatie die is vermeld op het onderstaande interesseformulier, om te verifiëren of de advertentie-SDK voldoet aan alle certificeringsvereisten en reageer tijdig op eventuele latere verzoeken om informatie.

Opmerking: Advertentie-SDK's moeten de weergave van advertenties ondersteunen die voldoet aan alle relevante wet- en regelgeving betreffende kinderen die mogelijk van toepassing is op hun uitgevers.

Bemiddelingsvereisten voor weergaveplatforms als deze advertenties weergeven aan kinderen:

- gebruik alleen door Google Play gecertificeerde advertentie-SDK's of voer waarborgen in om ervoor te zorgen dat alle via bemiddeling weergegeven advertenties voldoen aan deze vereisten, en
- geef noodzakelijke informatie door aan bemiddelingsplatforms om de classificatie voor advertentiecontent en eventueel toepasselijke behandeling van content die bedoeld is voor kinderen aan te geven.

Ontwikkelaars kunnen hier een lijst van zelfgecertificeerde advertentie-SDK's vinden.

Ontwikkelaars kunnen ook dit interesseformulier delen met advertentie-SDK's die zelfgecertificeerd willen worden.

Winkelvermelding en promotie

De promotie en zichtbaarheid van uw app zijn van grote invloed op de kwaliteit van de winkel. Vermijd spamachtige winkelvermeldingen, promoties van lage kwaliteit en activiteiten om de zichtbaarheid van de app op Google Play kunstmatig te verhogen.

App-promotie

We staan geen apps toe die direct of indirect betrokken zijn bij of profiteren van promotiepraktijken die misleidend of schadelijk zijn voor gebruikers of de ontwikkelaarsomgeving. Dit omvat tevens apps die het volgende gedrag vertonen:

het gebruik van misleidende advertenties op websites, in apps of in andere services, waaronder meldingen die lijken op systeemmeldingen en -waarschuwingen,
- promotie- of installatietactieken waarbij gebruikers worden omgeleid naar Google Play of die apps downloaden zonder dat de gebruiker hier bewust voor kiest,
- ongevraagde promotie via sms-services.

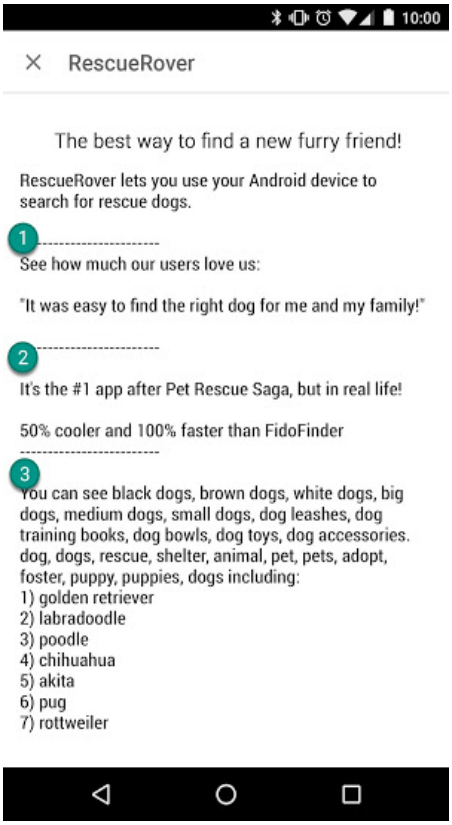
Het is uw verantwoordelijkheid om ervoor te zorgen dat advertentienetwerken of partners die zijn gekoppeld aan uw app, voldoen aan dit beleid en geen verboden promotiepraktijken gebruiken.

Metadata

We staan geen apps toe met misleidende, onjuist opgemaakte, niet-beschrijvende, irrelevante, buitensporige of ongepaste metadata, met inbegrip van, maar niet beperkt tot, de beschrijving van de app, de naam van de ontwikkelaar, de titel, het icoon, screenshots en promotieafbeeldingen. Ontwikkelaars moeten een duidelijke en goed geformuleerde beschrijving van hun app geven. We staan ook geen niet-herleidbare of anonieme gebruikerservaringen toe in de beschrijving van de app.

In aanvulling op de hier vermelde vereisten is het op grond van specifiek beleid voor ontwikkelaars in Play mogelijk noodzakelijk om aanvullende metadata-informatie te verstrekken.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:



① Niet-herleidbare of anonieme gebruikerservaringen
② Gegevensvergelijking van apps of merken
③ Blokken met woorden en verticale/horizontale lijsten met woorden

Hier volgen enkele voorbeelden van ongepaste tekst, afbeeldingen of video's in uw vermelding:

- Afbeeldingen of video's met seksueel suggestieve content. Vermijd suggestieve afbeeldingen met borsten, billen, genitaliën of andere geseksualiseerde lichaamsdelen of content, ongeacht of deze geïllustreerd of echt zijn.
- Het gebruik van grof, vulgair of ander taalgebruik dat ongepast is voor een algemeen publiek in de winkelvermelding van uw app.
- Extreem geweld dat prominent wordt afgebeeld in app-iconen, promotieafbeeldingen of video's.
- Afbeeldingen van illegaal drugsgebruik. Zelfs content voor educatieve, wetenschappelijke, artistieke of documentairedoeleinden in de winkelvermelding moet geschikt zijn voor alle leeftijden.

Hieronder vindt u enkele praktische tips:

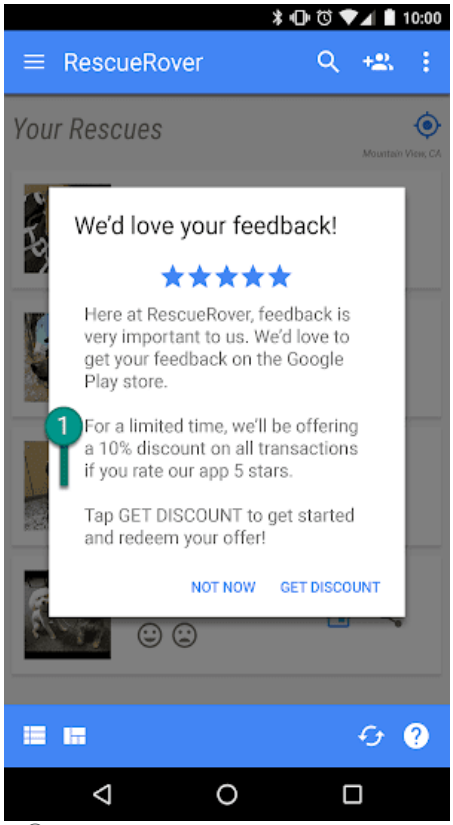
- Benadruk wat er zo goed is aan uw app. Deel interessante feiten over uw app zodat gebruikers begrijpen wat uw app speciaal maakt.
- Zorg ervoor dat de titel en beschrijving van uw app duidelijk de functies van uw app beschrijven.
- Gebruik geen herhaalde of irrelevante zoekwoorden of verwijzingen.
- Houd de beschrijving van uw app kort en duidelijk. Kortere beschrijvingen leiden over het algemeen tot een betere gebruikerservaring, met name op apparaten met een klein scherm. Overmatig lange of gedetailleerde beschrijvingen of beschrijvingen met een verkeerde opmaak of veel herhalingen kunnen in strijd zijn met dit beleid.
- Houd er rekening mee dat uw vermelding geschikt moet zijn voor alle leeftijden. Vermijd het gebruik van ongepaste tekst, afbeeldingen en video's in uw vermelding en houd u aan de bovenstaande richtlijnen.

Gebruikersbeoordelingen, reviews en installaties

Ontwikkelaars mogen de plaatsing van een app op Google Play niet proberen te manipuleren. Dit omvat, maar is niet beperkt tot, het kunstmatig laten toenemen van het aantal productbeoordelingen, reviews of installaties aan de hand van onrechtmatige middelen. Hieronder vallen onder andere frauduleuze installaties, reviews en beoordelingen, alsmede installaties, reviews en beoordelingen waarvoor een beloning wordt aangeboden.

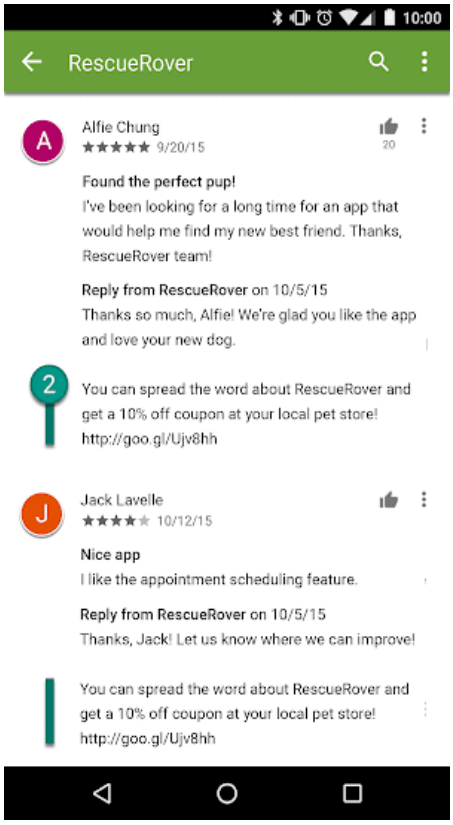
Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Gebruikers vragen uw app te beoordelen en daarvoor een beloning aanbieden:



① Deze melding biedt gebruikers een korting in ruil voor een goede beoordeling.

- Herhaaldelijk indienen van beoordelingen om de plaatsing van de app op Google Play te beïnvloeden.
- Het indienen van beoordelingen met ongepaste content, waaronder partners, kortingsbonnen, gamecodes, e-mailadressen of links naar websites of andere apps of gebruikers stimuleren dit te doen.



② Deze review stimuleert bezoekers om de app RescueRover te promoten door een kortingsbon aan te bieden.

Beoordelingen en reviews zijn benchmarks voor de kwaliteit van een app. Gebruikers zijn afhankelijk van de authenticiteit en relevantie ervan. Hierna volgen enkele praktische tips bij het reageren op reviews van gebruikers:

- houd uw antwoord gericht op de problemen die in de opmerkingen van de gebruiker worden genoemd en vraag niet om een betere beoordeling,
- vermeld verwijzingen naar nuttige hulpbronnen, zoals een supportadres of een pagina met veelgestelde vragen.

Contentclassificaties

Contentclassificaties op Google Play worden geleverd door de International Age Rating Coalition (IARC) en zijn bedoeld om ontwikkelaars te helpen gebruikers op de hoogte te stellen van lokaal relevante contentclassificaties. Regionale IARC-instanties houden richtlijnen aan die worden gebruikt om het volwassenheidsniveau van de content in een app te bepalen. We staan geen apps zonder contentclassificatie toe op Google Play.

Hoe contentclassificaties worden gebruikt

Contentclassificaties worden gebruikt om consumenten (met name ouders) te informeren over potentieel aanstootgevende content in een app. Ze helpen ook om uw content in bepaalde regio's of voor bepaalde gebruikers te filteren of te blokkeren waar dit wettelijk is vereist en om de geschiktheid van uw app voor speciale ontwikkelaarsprogramma's te bepalen.

Hoe contentclassificaties worden toegewezen

Als u een contentclassificatie wilt ontvangen, moet u in de Play Console een vragenlijst voor classificatie invullen over de aard van de content van uw apps. Op basis van uw antwoorden op de vragenlijst wordt een contentclassificatie aan uw app toegewezen die afkomstig is van meerdere classificatie-instanties. Als u een verkeerde voorstelling van de content van uw app geeft, kan dit leiden tot verwijdering of opschorting. Het is dus belangrijk dat u correcte antwoorden opgeeft in de vragenlijst voor contentclassificatie.

U kunt voorkomen dat uw app als 'Niet geclassificeerd' wordt weergegeven door de vragenlijst voor contentclassificatie in te vullen voor elke nieuwe app die wordt ingediend bij de Play Console en voor alle bestaande apps die actief zijn op Google Play.

Als u wijzigingen aanbrengt in de content of functies van uw app die van invloed zijn op de antwoorden op de vragenlijst voor contentclassificatie, moet u een nieuwe vragenlijst voor contentclassificatie indienen via de Play Console.

Ga naar het Helpcentrum voor meer informatie over de verschillende classificatie-instanties en hoe u de vragenlijst voor contentclassificatie moet invullen.

Bezwaar tegen een classificatie

Als u niet akkoord gaat met de contentclassificatie die aan uw app is toegewezen, kunt u rechtstreeks bezwaar indienen bij de IARC-classificatie-instantie via de link in e-mail met uw certificaat.

Nieuws

Apps die de categorie Nieuws selecteren maar content vertonen die niet aan deze vereisten voldoet, zijn niet toegestaan in de categorie Nieuws van de Play Store. Nieuws-apps waarvoor een gebruiker een lidmaatschap moet aanschaffen, moeten voorafgaand aan de aankoop een contentvoorbeeld aan gebruikers bieden.

Nieuws-apps MOETEN:

- voldoende informatie geven over de nieuwsuitgever en zijn bijdragers, waaronder duidelijk de eigenaar, en
- een website of in-app-pagina hebben met geldige contactgegevens voor de nieuwsuitgever.

Het volgende is NIET toegestaan in nieuws-apps:

- ze mogen geen grote spel- en grammaticafouten bevatten,
- ze mogen niet alleen statische content bevatten, en
- ze mogen affiliate marketing of advertentieopbrengst niet als belangrijkste doel hebben.

Apps met verzamelsites voor nieuws moeten transparant zijn over de publicatiebron van de content in de app en elk van de bronnen moet voldoen aan de beleidsvereisten voor Nieuws.

Spam en minimale functionaliteit

Apps moeten gebruikers ten minste een basisfunctionaliteit en een respectvolle gebruikerservaring bieden. Apps die crashen, ander gedrag vertonen dat niet overeenkomt met een functionele gebruikerservaring of die alleen dienen om gebruikers of Google Play te spammen, vormen geen betekenisvolle bijdrage aan onze catalogus.

Spam

We staan geen apps toe die spam versturen naar gebruikers of naar Google Play, zoals apps die gebruikers ongewenste berichten sturen of apps die sterk lijken op andere apps of die van slechte kwaliteit zijn.

Berichtenspam

We staan geen apps toe die sms'jes, e-mails of andere berichten namens de gebruiker versturen zonder de gebruiker de mogelijkheid te bieden de content en ontvangers goed te keuren.

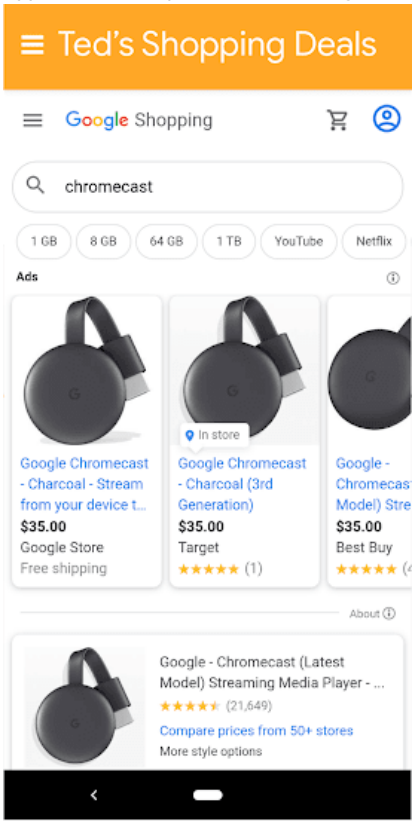
Webweergavespam en partnerspam

We staan geen apps toe die primair tot doel hebben partnerverkeer naar een website te verhogen of een webweergave te geven van een website zonder toestemming van de eigenaar of beheerder van de website.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Een app waarvan de primaire doelstelling is verwijzingsverkeer naar een website te verhogen om credits te ontvangen voor gebruikersaanmeldingen of aankopen op die website.

- Apps waarvan de primaire doelstelling is zonder toestemming een webweergave van een website te bieden:



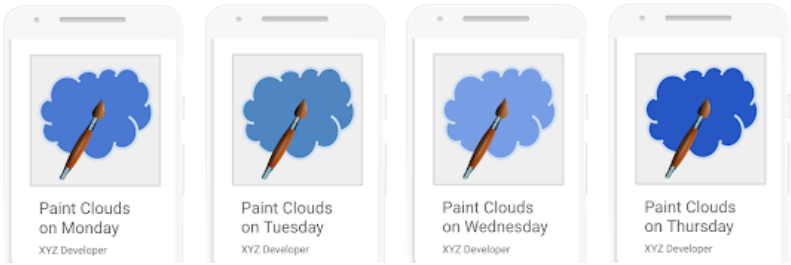
Deze app heet 'Ted's Shopping Deals' en biedt alleen een webweergave van Google Shopping.

Herhaalde content

We staan geen apps toe die slechts dezelfde functionaliteit bieden als andere apps die al aanwezig zijn op Google Play. Apps moeten waardevol zijn voor gebruikers vanwege hun unieke content of services.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Kopiëren van content uit andere apps zonder originele content of waarde toe te voegen.
- Meerdere apps maken die in functionaliteit, content en gebruikerservaring sterk op elkaar lijken. Als deze apps weinig contentvolume hebben, kunt u overwegen één app te maken met daarin alle content.



Gemaakt voor advertenties

We staan geen apps toe die als primair doel het weergeven van advertenties hebben.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps waarbij interstitial-advertenties worden geplaatst na elke gebruikersactie, waaronder, maar niet beperkt tot, klikken, vegen, enzovoort.

Minimale functionaliteit

Zorg ervoor dat uw app een stabiele, inclusieve en responsieve gebruikerservaring biedt.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps die ontworpen zijn om niets te doen of geen functie hebben

Defecte functionaliteit

We staan geen apps toe die crashen, geforceerd worden afgesloten, vastlopen of anderszins abnormaal functioneren.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps die **niet worden geïnstalleerd**
- Apps die worden geïnstalleerd, maar **niet worden geladen**
- Apps die worden geladen, maar **niet reageren**

Andere programma's

Apps die zijn ontworpen voor andere Android-producten en worden gedistribueerd via Google Play, moeten niet alleen voldoen aan het contentbeleid dat elders in dit Beleidscentrum is beschreven, maar kunnen ook vallen onder programmaspecifieke beleidsvereisten. Neem de onderstaande lijst door om te bepalen of een of meer van deze beleidsregels van toepassing zijn op uw app.

Android Instant-apps

Met Android Instant-apps willen we een prettige, probleemloze gebruikerservaring bieden en tegelijkertijd voldoen aan de hoogste normen op het gebied van privacy en beveiliging. Ons beleid is ontworpen om dat doel te ondersteunen.

Ontwikkelaars die ervoor kiezen Android Instant-apps te distribueren via Google Play, moeten voldoen aan het volgende beleid, in aanvulling op al het andere programmabeleid voor ontwikkelaars van Google Play.

Identiteit

Voor instant-apps met inlogfunctionaliteit moeten ontwikkelaars Smart Lock voor wachtwoorden integreren.

Linkondersteuning

Ontwikkelaars van Android Instant-apps moeten links voor andere apps correct ondersteunen. Als de instant-app of geïnstalleerde app van de ontwikkelaar links bevatten die potentieel kunnen leiden naar een instant-app, moet de ontwikkelaar gebruikers naar die instant-app sturen in plaats van bijvoorbeeld de links vast te leggen in een WebView.

Technische specificaties

Ontwikkelaars moeten voldoen aan de technische specificaties en vereisten voor Android Instant-apps die worden geleverd door Google, die van tijd tot tijd kunnen worden aangepast, waaronder de specificaties en vereisten die worden vermeld in onze openbare documentatie.

App-installatie aanbieden

De instant-app kan de installeerbare app aanbieden aan de gebruiker, maar dit mag niet het primaire doel van de instant-app zijn. Als installatie wordt aangeboden, is het volgende van toepassing:

- Ontwikkelaars moeten het Material Design-icoon 'app downloaden' en het label 'installeren' gebruiken voor de installatieknop.
- Ontwikkelaars mogen niet meer dan twee of drie impliciete installatieprompts opnemen in hun instant-app.
- Ontwikkelaars mogen geen banner of andere, op een advertentie lijkende techniek gebruiken om een installatieprompt aan gebruikers te presenteren.

U kunt meer informatie over instant-apps en richtlijnen voor de gebruikerservaring (UX) vinden in de praktische tips voor de gebruikerservaring.

Apparaatstatus wijzigen

Instant-apps mogen geen wijzigingen op het apparaat van de gebruiker aanbrengen die langer van kracht zijn dan de sessie van de instant-app. Instant-apps mogen bijvoorbeeld niet de achtergrond van de gebruiker wijzigen of een widget aan het startscherm toevoegen.

App-zichtbaarheid

Ontwikkelaars moeten ervoor zorgen dat instant-apps zichtbaar zijn voor de gebruiker, zodat de gebruiker zich ervan bewust is dat de instant-app op zijn apparaat wordt uitgevoerd.

Apparaat-ID's

Instant-apps mogen geen toegang hebben tot apparaat-ID's die (1) blijven bestaan nadat de instant-app niet meer wordt gebruikt en (2) niet kunnen worden gereset door de gebruiker. Voorbeelden hiervan zijn onder andere:

- Serienummer van build
- MAC-adressen van netwerkchips
- IMEI, IMSI

Instant-apps mogen toegang hebben tot het telefoonnummer als dit is verkregen met de runtime-machtiging. De ontwikkelaar mag niet proberen de gebruiker te identificeren aan de hand van deze ID's of andere middelen.

Netwerkverkeer

Netwerkverkeer dat afkomstig is uit de instant-app, moet worden versleuteld met een TLS-protocol zoals HTTPS.

Gezinnen

Google Play heeft een uitgebreid platform waar ontwikkelaars content van hoge kwaliteit kunnen aanbieden die geschikt is voor alle leeftijden. Voordat een app wordt ingediend bij het programma 'Gemaakt voor gezinnen' of een app die kinderen target wordt ingediend bij de Google Play Store, moet u ervoor zorgen dat uw app geschikt is voor kinderen en voldoet aan alle relevante wetgeving.

Lees meer over het proces voor gezinnen en bekijk de interactieve checklist op Academy for App Success.

Apps voor kinderen en gezinnen ontwerpen

Steeds meer mensen gebruiken technologie als handige aanvulling op het gezinsleven en ouders zoeken veilige content van hoge kwaliteit die ze met hun kinderen kunnen delen. Mogelijk ontwerpt u apps die specifiek voor kinderen zijn of misschien trekt uw app gewoon de aandacht van kinderen. Google Play wil u helpen ervoor te zorgen dat uw app veilig is voor alle gebruikers, inclusief gezinnen.

Het woord 'kinderen' kan verschillende betekenissen hebben in verschillende landen en in verschillende contexten. Het is belangrijk dat u contact opneemt met uw juridisch adviseur om te bepalen welke verplichtingen en/of leeftijdsbeperkingen van toepassing kunnen zijn op uw app. U weet het beste hoe uw app werkt, dus we vertrouwen erop dat u ons helpt ervoor te zorgen dat apps op Google Play veilig zijn voor gezinnen.

Apps die specifiek zijn ontworpen voor kinderen, moeten deelnemen aan het programma 'Gemaakt voor gezinnen'. Als uw app zowel kinderen als oudere doelgroepen target, kunt u nog steeds deelnemen aan het programma 'Gemaakt voor gezinnen'. Alle apps die zich aanmelden voor het programma 'Gemaakt voor gezinnen', komen in aanmerking voor beoordeling in het programma 'Goedgekeurd door docenten', maar we kunnen niet garanderen dat uw app wordt opgenomen in het programma 'Goedgekeurd door docenten'. Als u besluit niet deel te nemen aan het programma 'Gemaakt voor gezinnen', moet u nog steeds voldoen aan de onderstaande vereisten voor het Google Play-gezinsbeleid, het programmabeleid voor ontwikkelaars van Google Play en de distributieovereenkomst voor ontwikkelaars.

Vereisten voor Play Console

Doelgroep en content

In het gedeelte Doelgroep en content van de Google Play Console moet u de doelgroep voor uw app aangeven voordat u deze publiceert. Dit doet u door deze te selecteren in de lijst met leeftijdsgroepen. Als u ervoor kiest afbeeldingen en terminologie op te nemen in uw app die kunnen worden beschouwd als getarget op kinderen, kan dit, ongeacht wat u aangeeft in de Google Play Console, van invloed zijn op de beoordeling van uw opgegeven doelgroep door Google Play. Google Play behoudt zich het recht voor om een eigen beoordeling uit te voeren van de app-gegevens die u verstrekt om te bepalen of de door u opgegeven doelgroep juist is.

Als u een doelgroep selecteert die alleen uit volwassenen bestaat, maar Google vaststelt dat dit onjuist is omdat uw app zowel kinderen als volwassenen target, heeft u de mogelijkheid om aan gebruikers duidelijk te maken dat uw app kinderen niet target door in te stemmen het gebruik van een waarschuwingslabel.

Selecteer alleen meer dan één leeftijdsgroep voor de doelgroep van uw app als u uw app heeft ontworpen en ervoor heeft gezorgd dat uw app geschikt is voor gebruikers in de geselecteerde leeftijdsgroep. Voor apps die zijn ontworpen voor baby's, peuters en kleuters, moet bijvoorbeeld alleen de leeftijdsgroep '5 jaar en jonger' zijn geselecteerd als beoogde leeftijdsgroep voor die apps. Als uw app is ontworpen voor een specifiek klasniveau, kiest u de leeftijdsgroep die daar het

best bij past. U mag alleen leeftijdsgroepen selecteren die zowel volwassenen als kinderen omvatten als u uw app daadwerkelijk heeft ontwikkeld voor alle leeftijden.

Updates in het gedeelte 'Doelgroep en content'

U kunt de informatie over uw app altijd updaten in het gedeelte 'Doelgroep en content' in de Google Play Console. Er is een app-update vereist voordat deze informatie wordt weergegeven in de Google Play Store. Eventuele wijzigingen die u aanbrengt in dit gedeelte van de Google Play Console kunnen echter ook voordat een app-update wordt ingediend worden beoordeeld op naleving van het beleid.

We raden u ten zeerste aan uw bestaande gebruikers te informeren als u de getargete leeftijdsgroep van uw app wijzigt of begint met het gebruik van advertenties of in-app-aankopen. Dit kunt u doen in het gedeelte 'Wat is er nieuw' van de winkelvermeldingspagina van uw app of via meldingen in de app.

Verkeerde voorstelling in Play Console

Een verkeerde voorstelling van enige informatie over uw app in de Play Console, zoals in het gedeelte 'Doelgroep en content', kan leiden tot verwijdering of opschorting van uw app. Het is dus belangrijk om de juiste informatie te verstrekken.

Beleidsvereisten voor gezinnen

Als kinderen een van de doelgroepen voor uw app zijn, moet u voldoen aan de volgende vereisten. Als u niet voldoet aan deze vereisten, kan uw app worden verwijderd of opgeschort.

1. **App-content:** De content van een app die toegankelijk is voor kinderen, moet geschikt zijn voor kinderen.
2. **Antwoorden in Google Play Console:** U moet de vragen in de Google Play Console over uw app correct beantwoorden en deze antwoorden updaten zodat deze eventuele wijzigingen in uw app nauwkeurig weergeven.
3. **Advertenties:** Als uw app advertenties weergeeft aan kinderen of aan gebruikers van een onbekende leeftijd, zorgt u voor het volgende:
   - er wordt uitsluitend gebruikgemaakt van door Google Play gecertificeerde advertentie-SDK's om advertenties weer te geven aan die gebruikers,
   - de advertenties die worden weergegeven aan deze gebruikers, maken geen gebruik van op interesses gebaseerd adverteren (advertenties getarget op individuele gebruikers die beschikken over bepaalde kenmerken op basis van hun online browsegedrag) of remarketing (advertenties die zijn getarget op individuele gebruikers op basis van eerdere interactie met een app of website),
   - de advertenties die worden weergegeven aan deze gebruikers bevatten content die geschikt is voor kinderen,
   - de advertenties die worden weergegeven aan deze gebruikers voldoen aan de vereisten inzake advertentie-indeling voor gezinnen,
   - alle toepasselijke wet- en regelgeving en branchenormen die betrekking hebben op advertenties voor kinderen worden nageleefd.
4. **Gegevensverzameling:** Als via uw app persoonlijke en gevoelige informatie over kinderen wordt verzameld, moet u dat bekendmaken, ook als dit gebeurt met behulp van API's en SDK's die worden aangeroepen of gebruikt in uw app. Gevoelige informatie over kinderen omvat onder meer, maar is niet beperkt tot, verificatiegegevens, gegevens van microfoon- en camerasensoren, apparaatgegevens, Android-ID, gebruiksgegevens voor advertenties en advertentie-ID.
5. **API's en SDK's:** U moet ervoor zorgen dat uw app eventuele API's en SDK's naar behoren uitvoert.
   - Apps die uitsluitend kinderen targeten, mogen geen API's of SDK's bevatten die niet zijn goedgekeurd voor gebruik in op kinderen gerichte services. Dit zijn onder meer 'Inloggen bij Google' (of een andere Google API-service die toegang heeft tot gegevens die zijn gekoppeld aan een Google-account), Google Play-gameservices en eventuele andere API-services die gebruikmaken van OAuth-technologie voor verificatie en machtiging.
   - Apps die zowel kinderen als oudere doelgroepen targeten, mogen geen API's of SDK's implementeren die niet zijn goedgekeurd voor gebruik in op kinderen gerichte services, tenzij ze worden gebruikt achter een neutraal leeftijdsscherm of zodanig worden geïmplementeerd dat er geen gegevens worden verzameld over kinderen (door bijvoorbeeld 'Inloggen bij Google' als optionele functie aan te bieden). Apps die zowel kinderen als oudere doelgroepen targeten, mogen niet vereisen dat gebruikers inloggen of app-content openen via een API of SDK die niet is goedgekeurd voor gebruik in op kinderen gerichte services.
6. **Privacybeleid:** U moet op uw pagina met de winkelvermelding van uw app een link plaatsen naar een privacybeleid. Deze link moet beschikbaar zijn zo lang als de app in de Google Play Store aangeboden wordt en moet linken naar een privacybeleid dat, onder andere, een nauwkeurige beschrijving geeft van de procedures voor het verzamelen en gebruiken van gegevens in uw app.
7. **Speciale beperkingen:**
   - Als uw app gebruikmaakt van augmented reality, moet u bij het starten van het AR-gedeelte onmiddellijk een veiligheidswaarschuwing weergeven. Deze waarschuwing moet het volgende bevatten:
     - een geschikte melding over het belang van ouderlijk toezicht,

- een herinnering om bewust te blijven van fysieke gevaren in de echte wereld (bijvoorbeeld om zich bewust te zijn van de omgeving).
- U mag niet vereisen dat gebruikers van uw app een apparaat nodig hebben waarvan het gebruik door kinderen wordt afgeraden (zoals Daydream of Oculus).

8. **Juridische naleving:** U moet ervoor zorgen dat uw app, inclusief eventuele API's of SDK's die uw app aanroept of gebruikt, voldoet aan de Amerikaanse Children's Online Privacy and Protection Act (COPPA), de Algemene verordening gegevensbescherming (AVG) van de EU en eventuele andere toepasselijke wet- en regelgeving.

Hieronder vindt u enkele voorbeelden van veelvoorkomende schendingen:

- Apps die in de winkelvermelding spellen voor kinderen promoten, maar waarvan de app-content alleen geschikt is voor volwassenen.
- Apps die API's met servicevoorwaarden implementeren die het gebruik ervan in op kinderen gerichte apps verbieden.
- Apps die het gebruik van alcohol, tabak of andere verdovende middelen idealiseren.
- Apps die echte of gesimuleerde kansspelen bevatten.
- Apps met geweld, bloedvergieten of schokkende content die niet geschikt is voor kinderen.
- Apps die datingservices leveren of seksueel of huwelijksadvies aanbieden.
- Apps die links bevatten naar websites met content die in strijd is met het programmabeleid voor ontwikkelaars van Google Play.
- Apps die advertenties voor volwassenen weergeven (zoals gewelddadige content, seksuele content, content met betrekking tot kansspelen) aan kinderen. Raadpleeg het beleid voor advertenties voor gezinnen en het genereren van inkomsten voor meer informatie over het Google Play-beleid inzake advertenties, in-app-aankopen en commerciële content voor kinderen.

Het programma 'Gemaakt voor gezinnen'

Apps die specifiek zijn ontworpen voor kinderen, moeten deelnemen aan het programma 'Gemaakt voor gezinnen'. Als uw app is ontworpen voor iedereen, waaronder kinderen en gezinnen, kunt u ook een aanvraag indienen om deel te nemen aan het programma.

Voordat uw app wordt geaccepteerd voor het programma, moet deze voldoen aan alle beleidsvereisten voor gezinnen en deelnamevereisten voor 'Gemaakt voor gezinnen'. Ook aan de voorwaarden die worden beschreven in het programmabeleid voor ontwikkelaars van Google Play en de distributieovereenkomst voor ontwikkelaars moet worden voldaan.

Klik hier voor meer informatie over hoe u uw app kunt indienen voor deelname aan het programma.

Deelnamevereisten voor het programma

Alle apps die deelnemen aan het programma 'Gemaakt voor gezinnen' moeten beschikken over app- en advertentiecontent die relevant en geschikt is voor kinderen en moeten voldoen aan alle onderstaande vereisten. Apps die worden geaccepteerd voor het programma 'Gemaakt voor gezinnen' moeten altijd voldoen aan alle programmavereisten. Google Play kan elke app weigeren, verwijderen of opschorten waarvoor wordt vastgesteld dat deze ongeschikt is voor het programma 'Gemaakt voor gezinnen'.

Vereisten voor 'Gemaakt voor gezinnen'

1. Apps moeten de ESRB-classificatie 'Iedereen' of '10 jaar en ouder' of een vergelijkbare classificatie hebben.
2. U moet de interactieve elementen van de app nauwkeurig bekendmaken in de vragenlijst voor contentclassificatie in de Google Play Console, waaronder of:
   - gebruikers interactie kunnen hebben of informatie kunnen uitwisselen,
   - uw app door de gebruiker verstrekte persoonlijke informatie deelt met derden,
   - uw app de fysieke locatie van de gebruiker deelt met andere gebruikers.
3. Als uw app gebruikmaakt van de Android Speech API, moet RecognizerIntent.EXTRA_CALLING_PACKAGE zijn ingesteld op de bijbehorende PackageName.
4. Apps mogen uitsluitend door Google Play gecertificeerde advertentie-SDK's gebruiken.
5. Apps die specifiek ontworpen zijn voor kinderen, mogen niet vragen om locatierechten.
6. Apps moeten de Companion Device Manager (CDM) gebruiken als ze om bluetooth verzoeken, tenzij uw app zich alleen richt op versies van het besturingssysteem die niet werken met de CDM.

Hieronder staan enkele voorbeelden van veelvoorkomende apps die niet in aanmerking komen voor het programma:

- Apps met de ESRB-classificatie 'Iedereen', maar die advertenties voor kansspelcontent bevatten
- Apps voor ouders of verzorgers (zoals voor het bijhouden van borstvoeding of een ontwikkelingsgids)

- Gidsen voor ouders of apps voor apparaatbeheer die uitsluitend bestemd zijn voor gebruik door ouders of verzorgers
- Apps die een app-icoon of een launcher-icoon gebruiken dat niet geschikt is voor kinderen

Categorieën

Als u wordt geaccepteerd voor het programma 'Gemaakt voor gezinnen', kunt u een tweede gezinsspecifieke categorie kiezen die uw app beschrijft. De onderstaande categorieën zijn beschikbaar voor apps die deelnemen aan het programma 'Gemaakt voor gezinnen':

Actie en avontuur: Op actie gerichte apps/games, van eenvoudige racegames en sprookjesavonturen tot andere apps en games die zijn ontworpen om spanning te bieden.

Hersenkrakers: Games die de gebruiker aan het denken zetten, waaronder puzzels, geheugenspellen, quizzen en andere games die het geheugen, de intelligentie of de logica uitdagen.

Creativiteit: Apps en games die creativiteit stimuleren, waaronder teken-apps, schilder-apps, coderingsapps en andere apps en games waarin iets kan worden gemaakt.

Onderwijs: Apps en games die zijn ontworpen met bijdragen van onderwijsdeskundigen (zoals docenten, onderwijsspecialisten, onderzoekers) die het leren stimuleren. Daaronder vallen leren op academisch, sociaal-emotioneel, fysiek en creatief vlak, maar ook het leren van basisvaardigheden in het leven, kritisch denken en probleemoplossing.

Muziek en video: Apps en games met een muzikaal element of videocomponent, van apps voor instrumentsimulatie tot apps die video- en muzikale audiocontent bevatten.

Naspelen: Apps en games waarbij de gebruiker een rol kan spelen, zoals een kok(kin), verzorger/verzorgster, prins/prinses, brandweerman/-vrouw, politieagent(e) of fictief personage.

Advertenties en inkomsten genereren

Het onderstaande beleid is van toepassing op alle advertenties in uw app, waaronder advertenties voor uw apps en apps van derden, aanbiedingen voor in-app-aankopen of andere commerciële content (zoals betaalde productplaatsing) die worden weergegeven aan gebruikers van apps waarop de beleidsvereisten voor gezinnen en/of de deelnamevereisten voor Gemaakt voor gezinnen van toepassing zijn. Alle advertenties, aanbiedingen voor in-app-aankopen en commerciële content in deze apps moeten voldoen aan alle toepasselijke wet- en regelgeving (waaronder eventuele relevante zelfregulerende of brancherichtlijnen).

Google Play behoudt zich het recht voor om apps met zeer agressieve commerciële tactieken te weigeren, te verwijderen of op te schorten.

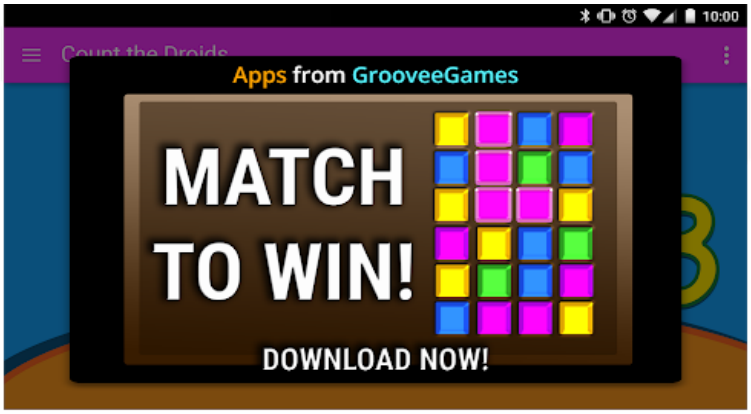
Vereisten voor advertentie-indelingen

Advertenties en aanbiedingen voor in-app-aankopen mogen geen misleidende content bevatten of zijn ontworpen op een manier die leidt tot onbedoelde klikken van kinderen. Het volgende is niet toegestaan:

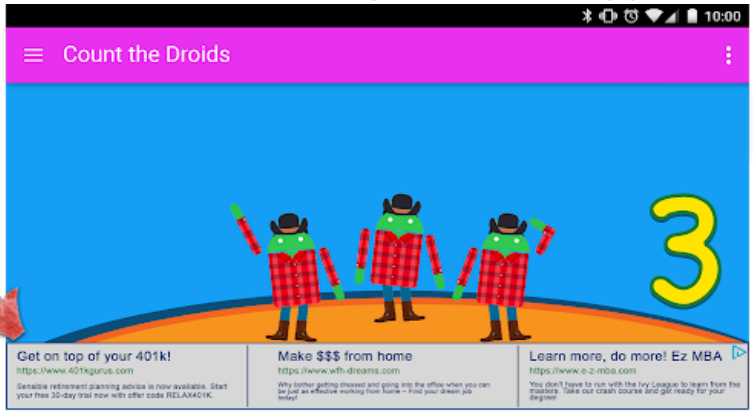
- Storende advertenties, waaronder advertenties die het hele scherm vullen of die het normale gebruik verstoren en geen duidelijke mogelijkheid bieden om de advertentie te sluiten (zoals advertentiemuren)
- Advertenties die het normale app-gebruik of de normale gameplay beïnvloeden en niet na vijf seconden kunnen worden gesloten Advertenties die het normale app-gebruik of de normale gameplay niet verstoren, kunnen langer dan vijf seconden worden weergegeven (bijvoorbeeld videocontent met geïntegreerde advertenties).
- Interstitial-advertenties of aanbiedingen voor in-app-aankopen die onmiddellijk na het starten van de app worden weergegeven.
- Meerdere advertentieplaatsingen op een pagina (bijvoorbeeld banneradvertenties die meerdere aanbiedingen op één plaatsing weergeven of waarin meer dan één banner of videoadvertentie wordt weergegeven, zijn niet toegestaan).
- Advertenties of aanbiedingen voor in-app-aankopen die niet duidelijk te onderscheiden zijn van uw app-content.
- Gebruik van shockerende of emotioneel manipulatieve tactieken om advertentieweergave of in-app-aankopen te stimuleren.
- Geen onderscheid bieden tussen het gebruik van virtuele gamevaluta en echte valuta om in-app-aankopen te doen.

Hieronder staan enkele voorbeelden van veelvoorkomende schendingen van de advertentie-indeling

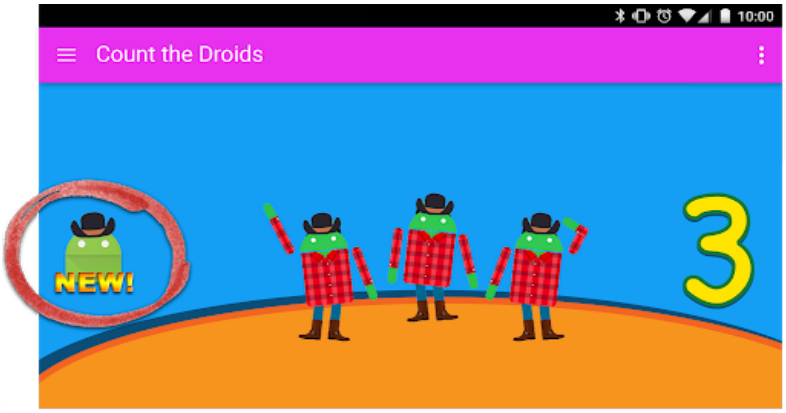
- Advertenties die de vinger van de gebruiker vermijden als deze de advertentie probeert te sluiten
- Advertenties die het apparaatscherm grotendeels vullen zonder de gebruiker een duidelijke optie te geven om de advertentie te sluiten, zoals weergegeven in het onderstaande voorbeeld:



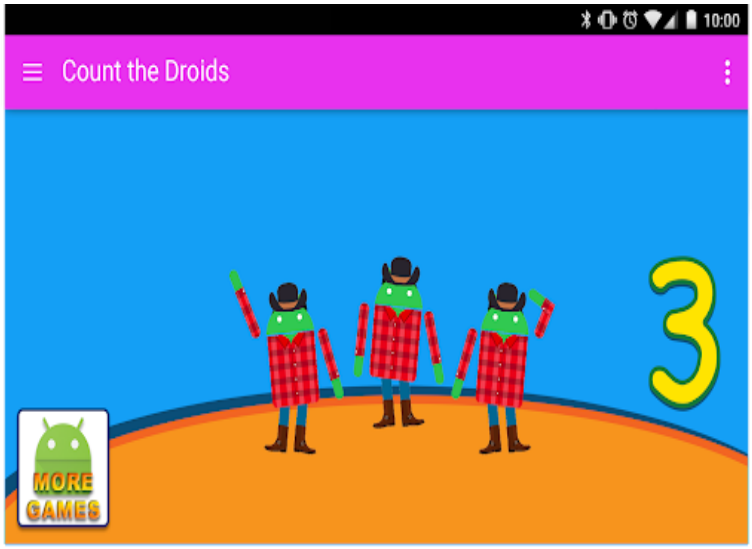
- Banneradvertenties die meerdere aanbiedingen laten zien, zoals weergegeven in het onderstaande voorbeeld:



- Advertenties die door de gebruiker kunnen worden aangezien voor app-content, zoals weergegeven in het onderstaande voorbeeld:



- Knoppen of advertenties die uw andere winkelvermeldingen op Google Play promoten, maar die niet te onderscheiden zijn van app-content, zoals weergegeven in het onderstaande voorbeeld:



Hier volgen enkele voorbeelden van ongepaste advertentiecontent die niet mag worden weergegeven aan kinderen.

- **Ongepaste mediacontent**: Advertenties voor tv-programma's, films, muziekalbums of andere mediakanalen die niet geschikt zijn voor kinderen.
- **Ongepaste videogames en downloadbare software**: Advertenties voor downloadbare software en elektronische videogames die niet geschikt zijn voor kinderen.
- **Illegale of schadelijke stoffen**: Advertenties voor alcohol, tabak, verdovende middelen of andere schadelijke stoffen.
- **Kansspelen**: advertenties voor gesimuleerde kansspelen, wedstrijden of sweepstakes, zelfs als er gratis kan worden deelgenomen.
- **Content voor volwassenen en seksueel suggestieve content**: Advertenties met seksuele, seksueel suggestieve en niet-gezinsvriendelijke content.
- **Dating of relaties**: Advertenties voor datingsites of sites voor volwassen relaties.
- **Gewelddadige content**: Advertenties met gewelddadige en expliciete content die niet geschikt is voor kinderen.

Advertentie-SDK's

Als u advertenties weergeeft in uw app en uw doelgroep alleen kinderen omvat, moet u door Google Play gecertificeerde advertentie-SDK's gebruiken. Als de doelgroep van uw app zowel kinderen als oudere gebruikers omvat, moet u maatregelen voor het controleren van de leeftijd invoeren, zoals een neutraal leeftijdsscherm, en ervoor zorgen dat advertenties die aan kinderen worden weergegeven, uitsluitend afkomstig zijn van door Google Play gecertificeerde advertentie-SDK's. Apps in het programma 'Gemaakt voor gezinnen' mogen uitsluitend zelfgecertificeerde advertentie-SDK's gebruiken.

Raadpleeg de pagina met het programmabeleid van advertenties voor gezinnen voor meer details over deze vereisten en voor een actuele lijst met goedgekeurde advertentie-SDK's.

Als u AdMob gebruikt, raadpleegt u het Helpcentrum van AdMob voor meer informatie over de producten.

Het is uw verantwoordelijkheid om ervoor te zorgen dat uw app voldoet aan alle vereisten ten aanzien van advertenties, in-app-aankopen en commerciële content. Neem contact op met uw aanbieder van advertentie-SDK's voor meer informatie over het betreffende contentbeleid en advertentiepraktijken.

In-app-aankopen

Google Play verifieert alle gebruikers nogmaals voorafgaand aan eventuele in-app-aankopen in apps die deelnemen aan het programma 'Gemaakt voor gezinnen'. Deze maatregel helpt ervoor te zorgen dat de financieel verantwoordelijke partij, en niet kinderen, de aankopen goedkeuren.

Handhaving

Het voorkomen van een beleidsschending is altijd beter dan het beheren ervan, maar als er toch sprake is van een schending, willen we dat ontwikkelaars begrijpen hoe ze ervoor kunnen zorgen dat hun app aan het beleid voldoet. Laat het ons weten als u schendingen ziet of vragen heeft over het beheren van een schending.

Beleidsdekking

Ons beleid is van toepassing op content die in uw app wordt weergegeven of waarnaar met links in de app wordt verwezen, advertenties die aan gebruikers worden weergegeven in de app en door gebruikers gegenereerde content die in de app wordt gehost of waarnaar wordt gelinkt. Verder is het contentbeleid van toepassing op content in uw ontwikkelaarsaccount die openbaar wordt weergegeven op Google Play, waaronder uw ontwikkelaarsnaam en de bestemmingspagina van uw vermelde ontwikkelaarswebsite.

We staan geen apps toe die gebruikers andere apps laten installeren op hun apparaat. Apps die toegang bieden tot andere apps, games of software zonder installatie, waaronder functies en functionaliteit die worden aangeboden door derden, moeten ervoor zorgen dat alle content waartoe zij toegang geven voldoet aan alle beleidsrichtlijnen van Google Play en deze apps kunnen tevens het voorwerp zijn van aanvullende beleidsreviews.

De termen die in dit beleid worden gedefinieerd, hebben dezelfde betekenis als in de distributieovereenkomst voor ontwikkelaars (DDA). De content van uw app moet niet alleen voldoen aan dit beleid en de distributieovereenkomst voor ontwikkelaars, maar moet ook worden beoordeeld op basis van onze richtlijnen voor contentclassificatie.

Als we beoordelen of we apps willen opnemen in of verwijderen uit Google Play, houden we rekening met een aantal factoren, inclusief, maar niet beperkt tot, een patroon van schadelijk gedrag of een hoog risico op misbruik. We identificeren het risico op misbruik, waaronder, maar niet uitsluitend, items als eerdere schendingen, feedback van gebruikers en het gebruik van populaire merken, personages en andere bedrijfsmiddelen.

Hoe Google Play Protect werkt

Google Play Protect controleert apps wanneer u deze installeert. De functie scant ook regelmatig uw apparaat. Als er een potentieel schadelijke app wordt gevonden, kan Google Play Protect het volgende doen:

- U een melding sturen. Als u de app wilt verwijderen, tikt u op de melding en vervolgens op Verwijderen.
- De app uitschakelen totdat u deze verwijdert.
- De app automatisch verwijderen. Als er een schadelijke app wordt gedetecteerd, ontvangt u meestal een melding waarin staat dat de app is verwijderd.

Hoe malwarebescherming werkt

Google beschermt u tegen schadelijke software van derden, URL's en andere beveiligingsproblemen. Hiervoor kan Google informatie ontvangen over het volgende:

- De netwerkverbindingen van uw apparaat.
- Potentieel schadelijke URL's.
- Het besturingssysteem en de apps die op uw apparaat zijn geïnstalleerd via Google Play of andere bronnen.

U kunt een waarschuwing van Google ontvangen over een app of URL die mogelijk onveilig is. Als Google zeker weet dat de app schadelijk is voor apparaten, gegevens of gebruikers, kan de app of URL worden verwijderd of kan de installatie ervan worden geblokkeerd.

U kunt ervoor kiezen sommige van deze beveiligingen uit te schakelen in uw apparaatinstellingen. Google kan echter informatie blijven ontvangen over apps die zijn geïnstalleerd via Google Play. Apps die vanuit andere bronnen op uw apparaat zijn geïnstalleerd, kunnen om veiligheidsredenen nog steeds worden gecontroleerd zonder informatie naar Google te sturen.

Hoe werken privacymeldingen?

U krijgt een melding van Google Play Protect als een app wordt verwijderd uit de Google Play Store omdat de app toegang heeft tot uw persoonlijke informatie en u de app kunt verwijderen.

Handhavingsproces

Als uw app een van onze beleidsregels schendt, nemen we passende maatregelen zoals hieronder beschreven. Daarnaast verstrekken we u via e-mail relevante informatie over de genomen maatregel, samen met instructies over hoe u bezwaar kunt maken als van mening bent dat we ten onrechte maatregelen hebben genomen.

We wijzen u erop dat verwijderings- of administratieve kennisgevingen mogelijk niet alle beleidsschendingen vermelden waarvan sprake is in uw app of app-aanbod. Ontwikkelaars zijn verantwoordelijk voor het verhelpen van beleidsproblemen en het uitvoeren van extra due diligence om te verzekeren dat de rest van de app volledig aan het beleid voldoet. Als u beleidsschendingen niet in al uw apps verhelpt, kan dit leiden tot aanvullende handhavingsmaatregelen.

Herhaalde of ernstige schendingen (zoals malware, fraude en apps die de gebruiker of het apparaat schade kunnen toebrengen) van dit beleid of de distributieovereenkomst voor ontwikkelaars (DDA), leiden tot de beëindiging van afzonderlijke of gerelateerde Google Play-ontwikkelaarsaccounts.

Handhavingsmaatregelen

Verschillende handhavingsmaatregelen kunnen op verschillende manieren van invloed zijn op uw app. In het volgende gedeelte worden de verschillende maatregelen beschreven die Google Play kan nemen en de gevolgen voor uw app en/of uw Google Play-ontwikkelaarsaccount. Deze informatie wordt ook toegelicht in deze video.

Afwijzing

- Een nieuwe app of app-update die ter beoordeling is ingediend, wordt niet beschikbaar gemaakt op Google Play.
- Als een update voor een bestaande app is afgewezen, blijft de app-versie die vóór de update is gepubliceerd, beschikbaar op Google Play.
- Afwijzingen hebben geen invloed op uw toegang tot de bestaande gebruikersinstallaties, statistieken en beoordelingen van een afgewezen app.
- Afwijzingen hebben geen invloed op de reputatie van uw Google Play-ontwikkelaarsaccount.

Opmerking: Probeer een afgewezen app niet opnieuw in te dienen totdat u alle beleidsschendingen heeft verholpen.

Verwijdering

- De app en eerdere versies van de app worden verwijderd van Google Play en kunnen niet meer worden gedownload door gebruikers.
- Omdat de app is verwijderd, kunnen gebruikers de winkelvermelding, gebruikersinstallaties, statistieken en beoordelingen van de app niet zien. Deze informatie wordt hersteld zodra u een beleidsconforme update indient voor de verwijderde app.
- Gebruikers kunnen mogelijk geen in-app-aankopen doen of functies voor in-app-facturering in de app gebruiken totdat een beleidsconforme versie is goedgekeurd door Google Play.
- Verwijderingen hebben niet onmiddellijk invloed op de reputatie van uw Google Play-ontwikkelaarsaccount, maar meerdere verwijderingen kunnen leiden tot opschorting.

Opmerking: Probeer een verwijderde app niet opnieuw te publiceren totdat u alle beleidsschendingen heeft verholpen.

Opschorting

- De app en eerdere versies van die app worden verwijderd van Google Play en kunnen niet meer worden gedownload door gebruikers.
- Opschorting kan plaatsvinden als gevolg van ernstige of meerdere beleidsschendingen, evenals herhaalde afwijzingen of verwijderingen van apps.
- Omdat de app is opgeschort, kunnen gebruikers de winkelvermelding, bestaande gebruikersinstallaties, statistieken en beoordelingen van de app niet zien. Deze informatie wordt hersteld zodra u een beleidsconforme update indient voor de verwijderde app.
- U kunt de APK of app-bundel van een opgeschorte app niet meer gebruiken.
- Gebruikers kunnen geen in-app-aankopen doen of functies voor in-app-facturering in de app gebruiken totdat een beleidsconforme versie is goedgekeurd door Google Play.
- Opschortingen hebben een negatief effect op de reputatie van uw Google Play-ontwikkelaarsaccount. Meerdere waarschuwingen kunnen ertoe leiden dat afzonderlijke en gerelateerde Google Play-ontwikkelaarsaccounts worden beëindigd.

Opmerking: Probeer een opgeschorte app niet opnieuw te publiceren, tenzij Google Play heeft verteld dat u dit kunt doen.

Beperkte zichtbaarheid

- De vindbaarheid van uw app op Google Play is beperkt. Uw app blijft beschikbaar op Google Play en is toegankelijk voor gebruikers met een rechtstreekse link naar de winkelvermelding van de app in Play.
- Als uw app de status beperkte zichtbaarheid heeft, heeft dit geen invloed op de reputatie van uw Google Play-ontwikkelaarsaccount.
- Als uw app de status beperkte zichtbaarheid heeft, heeft dit geen invloed op de mogelijkheid van gebruikers om de bestaande winkelvermelding, gebruikersinstallaties, statistieken en beoordelingen van de app te bekijken.

Beëindiging van account

- Als uw ontwikkelaarsaccount wordt beëindigd, worden alle apps in uw catalogus verwijderd van Google Play en kunt u geen nieuwe apps meer publiceren. Dit betekent ook dat eventuele gerelateerde Google Play-ontwikkelaarsaccounts permanent worden opgeschort.
- Meerdere opschortingen of opschortingen vanwege ernstige beleidsschendingen kunnen ook leiden tot de beëindiging van uw Play Console-account.
- Omdat de apps in het beëindigde account worden verwijderd, kunnen gebruikers de winkelvermelding, bestaande gebruikersinstallaties, statistieken en beoordelingen niet zien.

Opmerking: Elk nieuw account dat u probeert te openen, wordt ook beëindigd (zonder teruggave van de registratiekosten voor ontwikkelaars). Registreer u dus niet voor een nieuw Play Console-account als een van uw andere accounts is beëindigd.

Beleidsschendingen beheren en melden

Bezwaar maken tegen een handhavingsmaatregel

We herstellen apps als er een fout is gemaakt en we hebben vastgesteld dat uw app het programmabeleid van Google Play en de distributieovereenkomst voor ontwikkelaars niet schendt. Als u het beleid zorgvuldig heeft gelezen en van mening bent dat onze beslissing onterecht is, volgt u de instructies in de e-mail met de handhavingsmaatregel om bezwaar te maken tegen onze beslissing.

Aanvullende bronnen

Als u meer informatie nodig heeft over een handhavingsmaatregel of een beoordeling/opmerking van een gebruiker, kunt u de onderstaande bronnen raadplegen of contact met ons opnemen via het Helpcentrum van Google Play. We kunnen u echter geen juridisch advies geven. Als u juridisch advies nodig heeft, neemt u contact op met uw juridisch adviseur.

- App-verificatie en bezwaren
- Een beleidsschending melden
- Contact opnemen met Google Play over het beëindigen van een account of het verwijderen van een app
- Duidelijke waarschuwingen
- Ongepaste apps en reacties melden
- Mijn app is verwijderd van Google Play
- Uitleg van beëindiging van Google Play-ontwikkelaarsaccounts

Meer hulp nodig?

Probeer de volgende stappen:

Contact opnemen

Vertel ons meer zodat we u kunnen helpen