Google Developer Policy - April 16, 2020

Costruiamo insieme lo store di app e giochi più affidabile al mondo

La tua innovazione è alla base del nostro successo comune, ma comporta anche delle responsabilità. Le presenti Norme del programma per gli sviluppatori, insieme al Contratto di distribuzione per gli sviluppatori, ci garantiscono di poter continuare a offrire le app più innovative e affidabili a oltre un miliardo di persone nel mondo, tramite Google Play. Ti invitiamo a leggere le nostre norme riportate sotto oppure in una visualizzazione stampa.

Contenuti con limitazioni

Il servizio Google Play viene utilizzato ogni giorno da persone di tutto il mondo per accedere ad app e giochi. Prima di inviare un'app, occorre stabilire se è adatta a Google Play e se è conforme alle leggi locali.

Rischi per i bambini

Le app con contenuti che sessualizzano i minori sono soggette alla rimozione immediata dallo Store. Sono vietate le app che attirano i bambini, ma contengono temi per adulti.

Se veniamo a conoscenza di contenuti con immagini pedopornografiche, li segnaliamo alle autorità competenti ed eliminiamo gli Account Google delle persone coinvolte nella distribuzione.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Contenuti di natura sessuale

Sono vietate le app che contengono o promuovono contenuti di natura sessuale, come la pornografia, o contenuti o servizi destinati a essere sessualmente gratificanti. I contenuti che

implicano nudità possono essere consentiti se il loro scopo principale è educativo, documentaristico, scientifico o artistico e non sono fini a se stessi.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Eventuali rappresentazioni di nudo in cui il soggetto è nudo o vestito minimamente e dove l'abbigliamento non sarebbe accettabile in un contesto pubblico appropriato.
- Rappresentazioni, animazioni o illustrazioni di atti sessuali o pose sessualmente allusive.
- Contenuti raffiguranti accessori sessuali o fetish.
- Contenuti osceni o profani.
- Contenuti che raffigurano, descrivono o promuovono la pornografia con animali.
- App che promuovono servizi di intrattenimento sessuale, di escort o altri servizi che potrebbero essere interpretati come un'offerta di atti sessuali in cambio di un compenso.

Incitamento all'odio

Non sono ammesse le app che promuovono la violenza o incitano all'odio verso individui o gruppi di persone in base alla loro razza o etnia di origine, religione, disabilità, età, nazionalità, condizione di reduce di guerra, anzianità, identità/orientamento sessuale, genere o altre caratteristiche associate a discriminazione o emarginazione sistematica.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Raccolte di asserzioni volte a dimostrare che un gruppo protetto è inumano, inferiore o degno di odio.
- App che contengono teorie su un gruppo protetto con caratteristiche negative (ad es. spregevole, corrotto, malvagio e così via) o che affermano esplicitamente o implicitamente che tale gruppo rappresenta una minaccia.
- Contenuti o discorsi che mirano a incoraggiare gli altri a credere che determinate persone debbano essere odiate o discriminate perché fanno parte di un gruppo protetto.

Violenza

Non sono ammesse le app che raffigurano o agevolano scene di violenza gratuita o altre attività pericolose.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Raffigurazioni esplicite o descrizioni di scene di violenza realistica o minacce di violenza nei confronti di persone o animali.

App che promuovono l'autolesionismo, il suicidio, i disturbi alimentari, i giochi di soffocamento o altri atti che possono comportare lesioni gravi o morte.

Contenuti di natura terroristica

Non consentiamo alle organizzazioni terroristiche di pubblicare app su Google Play per alcuno scopo, incluso il reclutamento.

Non sono ammesse le app con contenuti di natura terroristica, ad esempio contenuti che promuovono atti terroristici, incitano alla violenza o commemorano attacchi terroristici. Se si vogliono pubblicare contenuti correlati al terrorismo a scopo didattico, documentaristico, scientifico o artistico, è necessario fornire informazioni sufficienti per consentire agli utenti di comprenderne il contesto.

Eventi sensibili

Sono vietate le app prive della dovuta sensibilità nei confronti di calamità naturali, atrocità, conflitti, decessi o altri eventi tragici oppure le app che sfruttano tali eventi.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Mancanza di tatto in relazione alla morte per suicidio, overdose, cause naturali e così via di una persona o di un gruppo di persone.
Negazione di un grande evento tragico.
Trarre profitto da un evento tragico senza fornire alcun vantaggio concreto per le vittime.

Bullismo e molestie

Non sono ammesse le app che contengono o favoriscono minacce, molestie o atti di bullismo.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Vessazione di vittime di conflitti internazionali o religiosi.
Contenuti con tentativi di sfruttamento di terzi, inclusi estorsione, ricatto e così via.
Pubblicazione di contenuti finalizzati alla pubblica umiliazione di un soggetto.
Attacchi rivolti alle vittime di un evento tragico o ai loro amici e familiari.

Prodotti pericolosi

Sono vietate le app che favoriscono la vendita di esplosivi, armi da fuoco, munizioni o determinati accessori per armi.

Alcuni accessori con limitazioni sono, ad esempio, quelli che consentono a un'arma da fuoco di simulare colpi automatici o che trasformano un'arma da fuoco in arma

automatica (ad esempio bump stock, grilletti a manovella, dispositivi Drop In Auto Sear, kit di conversione) e caricatori o cinture che possono contenere più di 30 munizioni.

Sono vietate le app che danno istruzioni per la produzione di esplosivi, armi da fuoco, munizioni, accessori per armi da fuoco con limitazioni o altre armi. Sono incluse le istruzioni per trasformare un'arma da fuoco in arma automatica o con capacità di simulazione di colpi automatici.

Marijuana

Sono vietate le app che favoriscono la vendita di marijuana o derivati della marijuana, indipendentemente dalla loro legalità o meno.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Permettere agli utenti di ordinare marijuana attraverso una funzionalità del carrello degli acquisti in-app.
- Aiutare gli utenti a organizzare la consegna o il prelievo di marijuana.
- Favorire la vendita di prodotti contenenti THC.

Tabacco e alcol

Sono vietate le app che favoriscono la vendita di tabacco (comprese le sigarette elettroniche) o che incoraggiano l'uso irresponsabile di alcol o tabacco.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Raffigurare o incoraggiare l'uso o la vendita di alcol o tabacco ai minori.
- Sottintendere che il consumo di tabacco possa migliorare la posizione sociale, sessuale, professionale, intellettuale o atletica.
- Ritrarre in modo favorevole l'eccessivo consumo di alcolici, inclusa la rappresentazione favorevole del binge drinking.

Servizi finanziari

Sono vietate le app che espongono gli utenti a prodotti e servizi finanziari ingannevoli o dannosi.

Nell'ambito delle presenti norme, vengono considerati prodotti e servizi finanziari quelli relativi alla gestione o all'investimento di denaro e criptovalute, incluse le consulenze personalizzate.

Se l'app contiene o promuove prodotti e servizi finanziari, è obbligatorio rispettare le normative statali e locali di ogni area geografica o paese di destinazione dell'app, ad esempio includendo dichiarazioni specifiche richieste dalla legge locale.

Opzioni binarie

Non sono ammesse app che forniscono agli utenti la possibilità di scambiare opzioni binarie.

Criptovalute

Sono vietate le app che consentono il mining di criptovaluta sui dispositivi. Sono consentite le app che gestiscono da remoto il mining di criptovaluta.

Prestiti personali

Definiamo "prestito personale" l'atto occasionale di prestare denaro, realizzato da persona fisica, organizzazione o persona giuridica a beneficio di un consumatore singolo e non destinato a finanziare l'acquisto di una immobilizzazione o l'istruzione personale. Per decidere in piena consapevolezza se richiedere un prestito personale, i consumatori interessati necessitano di informazioni su qualità, caratteristiche, commissioni, rischi e benefici del prodotto finanziario.

> Alcuni esempi: prestiti personali, prestiti con anticipo sullo stipendio, prestiti peer-to-peer e prestito con titolo di proprietà dell'auto in garanzia
> Non inclusi: mutui, prestiti per l'acquisto di un'auto, prestiti scolastici, linee di credito rotative (ad esempio, carte di credito e linee di credito personali)

Le app per la concessione di prestiti personali devono divulgare le seguenti informazioni nei rispettivi metadati:

> Il periodo minimo e massimo per il rimborso
> Il TAEG, che generalmente include il tasso di interesse più commissioni e altri costi annui o altro tasso analogo, calcolato in base alla normativa locale
> Un esempio rappresentativo del costo totale del prestito, comprese tutte le commissioni applicabili

Sono vietate le app che promuovono prestiti personali che richiedono il rimborso completo in 60 giorni o meno dalla data di emissione (i cosiddetti "prestiti personali a breve termine"). Questa norma si applica ad app che offrono prestiti direttamente, generatori di lead e app che mettono in comunicazione i consumatori con istituti di credito di terze parti.

Prestiti personali con TAEG elevato

Negli Stati Uniti sono vietate le app per prestiti personali con un TAEG pari o superiore al 36%. Le app per prestiti personali negli Stati Uniti devono indicare il TAEG massimo, calcolato in base alla normativa Truth in Lending Act (TILA).

Questa norma si applica ad app che offrono prestiti direttamente, generatori di lead e app che mettono in comunicazione i consumatori con istituti di credito di terze parti.

Giochi e scommesse

Sono ammessi contenuti, servizi e annunci che promuovono i giochi a distanza online purché soddisfino determinati requisiti. Inoltre sono ammesse le app sui Daily Fantasy Sport che soddisfano determinati requisiti.

App di giochi a distanza

(Attualmente consentite solo in Regno Unito, Irlanda e Francia)

Contenuti e servizi che promuovono giochi e scommesse online sono consentiti se soddisfano i seguenti requisiti:

- Lo sviluppatore deve completare la procedura di iscrizione per poter distribuire l'app su Play.
- L'app deve essere conforme a tutte le leggi vigenti e agli standard di settore relativi ai paesi in cui viene distribuita.
- Lo sviluppatore deve disporre di una licenza per i giochi a distanza valida per ogni paese in cui viene distribuita l'app.
- Agli utenti minorenni non è consentito giocare a distanza tramite l'app.
- L'app non deve poter essere utilizzata nei paesi non coperti dalla licenza per i giochi a distanza fornita dallo sviluppatore.
- L'app NON deve essere acquistabile come app a pagamento su Google Play, né utilizzare la fatturazione in-app di Google Play.
- L'app deve essere scaricabile e installabile gratuitamente dallo Store.
- L'app deve avere la classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC.
- L'app e la relativa scheda devono visualizzare chiaramente le informazioni sul gioco a distanza responsabile.

In tutti gli altri paesi non sono ammessi contenuti o servizi che favoriscano i giochi a distanza online inclusi, a titolo esemplificativo, i casinò online, le scommesse sportive e le lotterie o i giochi di abilità che offrono premi in denaro o di altro tipo.

Annunci di giochi a distanza nelle app distribuite su Play

Gli annunci che promuovono i giochi a distanza online sono consentiti se soddisfano i seguenti requisiti:

- L'app e l'annuncio (inclusi gli inserzionisti di annunci di giochi a distanza) devono essere conformi a tutte le leggi vigenti e agli standard di settore relativi ai paesi in cui viene visualizzato l'annuncio di giochi a distanza.
- L'annuncio deve rispettare i requisiti di licenza locali per tutti i prodotti e servizi relativi ai giochi a distanza promossi.
- L'app non deve mostrare annunci di giochi a distanza a utenti di età comprovata inferiore a 18 anni.

L'app non deve essere iscritta al programma Per la famiglia.
L'app non deve essere rivolta a utenti di età inferiore a 18 anni.
L'annuncio deve visualizzare chiaramente le informazioni sul gioco a distanza responsabile nella pagina di destinazione, nella scheda stessa dell'app pubblicizzata o all'interno dell'app stessa.
L'app che pubblica un annuncio di giochi a distanza non deve essere un'app di simulazione di giochi a distanza (un gioco di intrattenimento senza giochi a distanza con soldi reali).

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App "KIDS 123" contenente un annuncio che promuove servizi di giochi a distanza

App di Daily Fantasy Sport (DFS)

Sono ammesse le app di Daily Fantasy Sport (DFS) purché soddisfino i seguenti requisiti:

L'accesso e la distribuzione dell'app devono essere consentiti solo negli Stati Uniti; le app di DFS che scelgono come target giurisdizioni al di fuori degli Stati Uniti devono stabilire l'idoneità tramite la procedura per le app di giochi a distanza con soldi reali.
Lo sviluppatore deve completare la procedura di iscrizione a DFS ed essere accettato per poter distribuire l'app su Play.
L'app deve essere conforme a tutte le leggi vigenti e agli standard di settore relativi a qualsiasi stato o territorio degli Stati Uniti in cui viene distribuita.
Lo sviluppatore deve disporre di una licenza valida per ciascuno stato o territorio degli Stati Uniti in cui è richiesta una licenza per le app di Daily Fantasy Sport;
Agli utenti minorenni non è consentito scommettere o eseguire transazioni finanziarie tramite l'app;
L'app non deve poter essere utilizzata negli stati o territori degli Stati Uniti in cui lo sviluppatore non possiede la licenza richiesta per le app di Daily Fantasy Sport;
L'app non deve poter essere utilizzata negli stati o territori degli Stati Uniti in cui le app di Daily Fantasy Sport non sono legali.
L'app NON deve essere acquistabile come app a pagamento su Google Play, né utilizzare la fatturazione in-app di Google Play.
L'app deve essere scaricabile e installabile gratuitamente dallo Store.
L'app deve avere la classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC.
L'app e la relativa scheda devono visualizzare chiaramente le informazioni sul gioco a distanza responsabile.

Attività illecite

Sono vietate le app che favoriscono o promuovono attività illegali.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Agevolazione della vendita o dell'acquisto di sostanze stupefacenti illegali o di farmaci con obbligo di prescrizione medica senza prescrizione medica.
- Raffigurazione o istigazione al consumo o alla vendita di droghe, alcol e tabacco ai minorenni.
- Istruzioni per coltivare o produrre sostanze stupefacenti illegali.

Contenuti generati dagli utenti

I contenuti generati dagli utenti sono contenuti che gli utenti pubblicano in un'app e che sono visibili o accessibili ad almeno un sottoinsieme di utenti dell'app. Per contenuti discutibili si intendono i contenuti che violano le nostre norme.

Le app che contengono o prevedono l'uso di contenuti generati dagli utenti devono:

- Richiedere agli utenti l'accettazione dei termini e condizioni d'uso dell'app e/o delle norme relative agli utenti prima che gli utenti possano creare o caricare contenuti di questo tipo;
- Definire quei contenuti generati dagli utenti che sono considerati discutibili, in modo coerente con lo spirito delle norme del programma per gli sviluppatori di Google Play, nonché vietare tali contenuti generati dagli utenti attraverso i termini e le condizioni d'uso e/o le norme relative agli utenti dell'app;
- Moderare i contenuti generati dagli utenti in modo costante, efficace e solido, nonché coerente e soddisfacente rispetto ai tipi di contenuti generati dagli utenti ospitati dall'app;
- Offrire un sistema in-app facile da usare per segnalare e rimuovere eventuali contenuti discutibili generati dagli utenti;
    - Nel caso delle app di live streaming, tutti quei contenuti problematici generati dagli utenti devono essere rimossi quanto prima, se non in tempo reale; e
- Rimuovere o bloccare gli utenti molesti che violano i termini e condizioni d'uso dell'app e/o i criteri relativi agli utenti;
- Fornire protezioni per impedire che la monetizzazione in-app incoraggi comportamenti discutibili dell'utente.

Le app il cui scopo principale è la pubblicazione di contenuti discutibili generati dagli utenti saranno rimosse da Google Play. Analogamente, le app il cui fine è quello di essere utilizzate principalmente per ospitare contenuti discutibili generati dagli utenti, oppure di diventare note come luogo in cui prosperano tali contenuti, saranno rimosse da Google Play.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Promozione di contenuti generati dagli utenti sessualmente espliciti, inclusa l'implementazione di funzionalità a pagamento che incoraggiano principalmente la condivisione di contenuti discutibili.
App con contenuti generati dagli utenti prive di sufficienti misure di salvaguardia da minacce, molestie o atti di bullismo, in particolare nei confronti di minorenni.
Post, foto o commenti all'interno di un'app il cui scopo principale è molestare o prendere di mira un'altra persona, che viene sottoposta a maltrattamenti e attacchi crudeli o che viene derisa.
App che non procedono ripetutamente alla risoluzione dei reclami degli utenti relativi ai contenuti discutibili.

Sostanze non approvate

Google Play non consente app che promuovono o vendono sostanze non approvate, a prescindere da qualsiasi rivendicazione di legittimità. Esempi:

Tutte le voci di questo elenco non esaustivo di prodotti farmaceutici e integratori vietati
Prodotti contenenti efedra
Prodotti contenenti gonadotropina corionica umana (hCG) in relazione alla perdita di peso o al controllo del peso o se pubblicizzati in combinazione con steroidi anabolizzanti
Integratori a base di erbe e dietetici che contengono principi attivi farmaceutici o ingredienti pericolosi
Indicazioni false o fuorvianti sulla salute, comprese le dichiarazioni che lasciano intendere che un prodotto è efficace quanto farmaci con obbligo di prescrizione medica o sostanze controllate
Prodotti approvati da enti non autorizzati dalla legge, pubblicizzati in modo da implicarne la sicurezza o l'efficacia nel prevenire o curare una malattia o disturbo di salute
Prodotti che sono stati oggetto di un'azione o di un avviso da parte di un'autorità legislativa o regolamentare
Prodotti i cui nomi possono essere confusi con quelli di sostanze controllate oppure di prodotti farmaceutici o integratori non approvati

Per ulteriori informazioni sui prodotti farmaceutici e sugli integratori non approvati o fuorvianti che monitoriamo, visita la pagina www.legitscript.com.

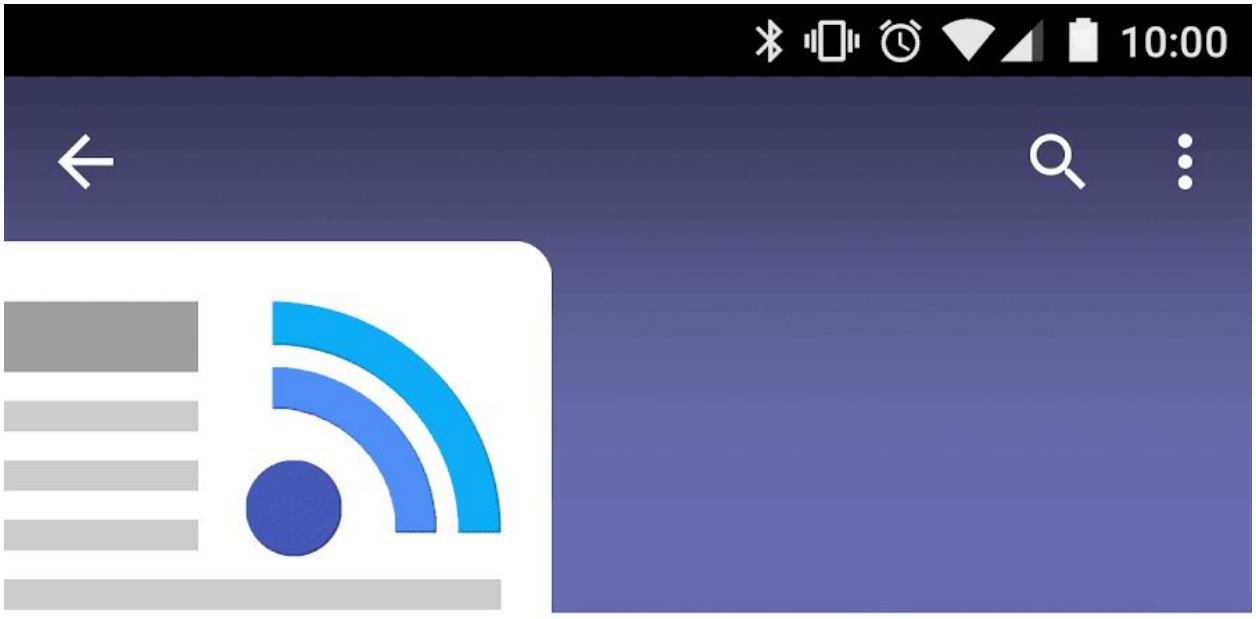
Furto d'identità e proprietà intellettuale

Quando gli sviluppatori copiano il lavoro di qualcun altro o ingannano gli utenti, arrecano danno a questi ultimi e alla community di sviluppatori. È vietato fare un uso fuorviante o illegittimo del lavoro di altre persone.

Furto d'identità

Sono vietate le app che utilizzano il brand, il titolo, il logo o il nome di un'altra app o entità in modo ingannevole per gli utenti. Non tentare di sottintendere una raccomandazione o una relazione inesistente con un'altra entità. Potrebbe trattarsi di furto d'identità anche se non c'è la volontà di ingannare, pertanto è necessario prestare attenzione quando viene fatto riferimento a brand di proprietà altrui. Questo vale anche se il brand non è ancora presente su Google Play. Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Sviluppatori che suggeriscono un'affiliazione inesistente con un'altra entità:



RSS News Aggregator

Google Developer

Everyone

INSTALL

100 MILLION
Downloads

4.1
161,251

News & Magazines

Similar

All the best news, aggregated in one spot!

WHAT'S NEW

- Push notifications now enabled.
- Customize your feed based on your current location!

① Il nome dello sviluppatore indicato per l'app suggerisce una relazione ufficiale con Google, che in realtà non esiste.
Titoli e icone di app molto simili a quelli di prodotti o servizi esistenti, che potrebbero trarre in inganno gli utenti:

App che dichiarano di essere le app ufficiali di un'entità affermata, anche se in realtà non lo sono. Titoli quali "App ufficiale di Justin Bieber" sono vietati senza le autorizzazioni o i diritti necessari.
App che violano le linee guida per il brand Android.

Proprietà intellettuale

Sono vietati gli account sviluppatore e le app che violano i diritti di proprietà intellettuale di altri (inclusi i diritti relativi a marchi, copyright, brevetti, segreti industriali e altri diritti di proprietà). Sono inoltre vietate le app che istigano o inducono alla violazione di diritti di proprietà intellettuale.

Risponderemo a chiare notifiche di presunta violazione del copyright. Per ulteriori informazioni o per presentare una richiesta ai sensi del DMCA (Digital Millennium Copyright Act, Legge statunitense sul copyright), consulta le procedure di Google relative al copyright.

Per presentare un reclamo relativo alla vendita o alla promozione di articoli contraffatti all'interno di un'app, invia una notifica di contraffazione.

I proprietari di marchi che ritengono che su Google Play sia presente un'app che viola i loro diritti sul marchio sono invitati a risolvere la questione contattando direttamente lo sviluppatore. Qualora non riescano a giungere a una soluzione con lo sviluppatore, i proprietari di marchi sono invitati a inviare un reclamo relativo al marchio utilizzando questo modulo.

Se si dispone della documentazione scritta che dimostra l'autorizzazione a utilizzare la proprietà intellettuale di terze parti nella propria app o scheda dello Store (ad esempio marchi,

loghi e risorse grafiche), contattare il team di Google Play prima di inviare i contenuti per assicurarsi che l'app non venga rifiutata per violazione di una proprietà intellettuale.

Utilizzo non autorizzato di contenuti protetti da copyright

Le app che violano il copyright sono vietate. Anche la modifica di contenuti protetti da copyright potrebbe essere considerata una violazione. Agli sviluppatori potrebbe essere chiesto di fornire prove a dimostrazione dei loro diritti di utilizzo dei contenuti protetti da copyright.

È opportuno prestare attenzione quando vengono utilizzati contenuti protetti da copyright per dimostrare la funzionalità della propria app. In genere l'approccio più sicuro consiste nel creare contenuti originali.

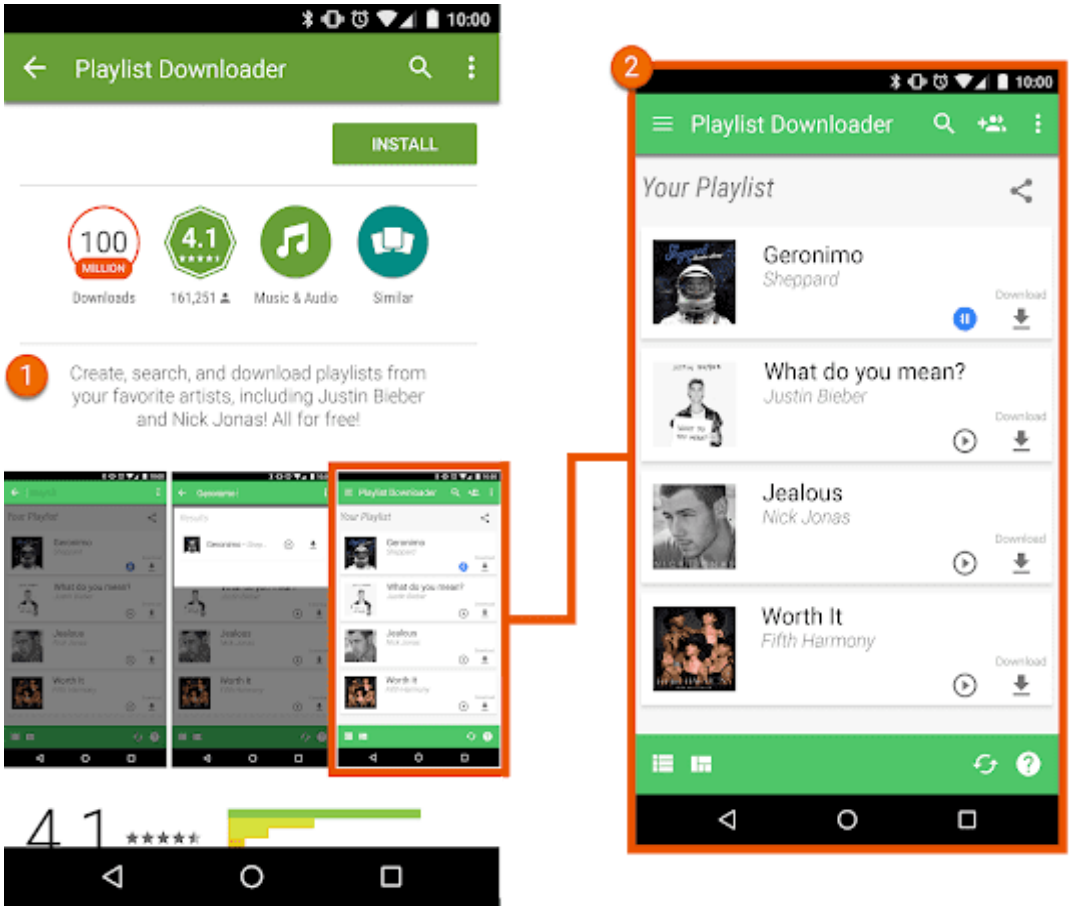
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Immagini di copertina di album musicali, videogiochi e libri.
- Immagini di marketing di film, programmi TV o videogiochi.
- Artwork o immagini di fumetti, cartoni animati, film, video musicali o programmi TV.
- Loghi di università e di squadre sportive professionali.
- Foto recuperate dall'account dei social media di un personaggio pubblico.
- Immagini professionali di personaggi pubblici.
- Riproduzioni o "fan art" indistinguibili dall'opera originale protetta da copyright.
- App con tavole armoniche che consentono di ascoltare clip audio di contenuti protetti da copyright.
- Riproduzioni o traduzioni complete di libri che non sono di pubblico dominio.

Istigazione alla violazione del copyright

Le app che inducono o istigano alla violazione del copyright sono vietate. Prima di pubblicare un'app, occorre capire se potrebbe istigare alla violazione del copyright e, se necessario, rivolgersi a un consulente legale.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- App di streaming che consentono agli utenti di scaricare una copia locale di contenuti protetti da copyright senza autorizzazione.
- App che esortano gli utenti a riprodurre in streaming e scaricare opere protette da copyright, inclusi video e musica, violando così la legge sul copyright vigente:



① La descrizione nella scheda di questa app esorta gli utenti a scaricare contenuti protetti da copyright senza autorizzazione.
② Lo screenshot nella scheda dell'app esorta gli utenti a scaricare contenuti protetti da copyright senza autorizzazione.

Violazione dei marchi

Le app che violano i marchi di altre persone sono vietate. Un marchio è una parola, un simbolo o una combinazione di entrambi che identifica l'origine di un bene o servizio. Una volta acquisito, un marchio conferisce al proprietario diritti esclusivi per il suo utilizzo rispetto a determinati beni o servizi.

La violazione di un marchio consiste nell'utilizzo improprio o non autorizzato di un marchio identico o simile a un altro, in modo tale da creare confusione in merito all'origine del prodotto che rappresenta. Se l'app utilizza marchi di un'altra parte in un modo che rischia di creare confusione, tale app potrebbe essere sospesa.

Contraffazione

Sono vietate le app che vendono o promuovono la vendita di articoli contraffatti. Gli articoli contraffatti contengono un marchio o un logo identico o sostanzialmente non distinguibile da un marchio esistente. Questi articoli imitano gli elementi distintivi del brand del prodotto nel tentativo di essere confusi con il prodotto originale del proprietario del brand.

Privacy, sicurezza e comportamento ingannevole

Ci impegniamo a fornire un ambiente sicuro per i nostri utenti e a proteggere la loro privacy. Le app ingannevoli, dannose o finalizzate all'utilizzo improprio o illecito di reti, dispositivi o dati personali sono severamente vietate.

Dati utente

Devi essere trasparente in merito alla modalità di gestione dei dati utente (ovvero le informazioni fornite da un utente o quelle raccolte relative a un utente, incluse le informazioni del dispositivo). Ciò significa comunicare l'accesso, la raccolta, l'uso e la condivisione dei dati da parte dell'app e limitare l'uso dei dati alle finalità comunicate. Inoltre, se l'app gestisce dati utente personali o sensibili, fai riferimento anche ai requisiti aggiuntivi nella sezione "Informazioni personali e sensibili" di seguito. Tali requisiti di Google Play si aggiungono ai requisiti previsti dalle leggi vigenti in materia di privacy e protezione dei dati.

Informazioni personali e sensibili

I dati utente personali e sensibili includono, a titolo esemplificativo, informazioni che consentono l'identificazione personale, dati finanziari e di pagamento, dati di autenticazione, rubrica, contatti, posizione del dispositivo, dati relativi a SMS e chiamate, dati di microfono e videocamera, nonché altri dati sensibili del dispositivo o sull'utilizzo. Se l'app gestisce dati utente sensibili, devi:

- Limitare l'accesso, la raccolta, l'utilizzo e la condivisione di dati personali o sensibili acquisiti tramite l'app a scopi direttamente correlati alla fornitura e al miglioramento delle funzionalità dell'app (ad esempio, funzionalità attese dall'utente che siano documentate e sponsorizzate nella descrizione dell'app nel Play Store). Le app che estendono l'utilizzo di questi dati per la pubblicazione di annunci devono essere conformi alle nostre Norme relative agli annunci.
- Pubblicare le norme sulla privacy sia nel relativo campo in Play Console sia all'interno dell'app stessa. Le norme sulla privacy, insieme a eventuali informative in-app, devono spiegare in modo esauriente in che modo l'app accede, raccoglie, utilizza e condivide i dati utente. Le norme sulla privacy devono indicare i tipi di dati personali e sensibili a cui

l'app accede, che raccoglie, utilizza e condivide, nonché i tipi di soggetti con cui vengono condivisi dati utente personali o sensibili.
Gestire tutti i dati utente personali o sensibili in sicurezza, inclusa la trasmissione mediante metodi moderni di crittografia (ad esempio, tramite HTTPS).
Utilizzare una richiesta di autorizzazioni di runtime, laddove disponibile, prima di accedere ai dati controllati tramite autorizzazioni Android.
Non vendere dati utente personali o sensibili.

Requisito relativo all'obbligo di consenso e alla posizione ben visibile dell'informativa

Nei casi in cui gli utenti potrebbero ragionevolmente non aspettarsi, come stabilito a esclusiva discrezione di Play, che i loro dati utente personali o sensibili siano richiesti per fornire o migliorare le funzionalità conformi alle norme o la funzionalità generale dell'app, sarà necessario soddisfare i seguenti requisiti:

Fornire un'informativa in-app relativa ad accesso, raccolta, utilizzo e condivisione dei dati. L'informativa in-app:

Deve trovarsi all'interno dell'app, non soltanto su un sito web o nella descrizione dell'app stessa.
Deve essere mostrata durante il normale utilizzo dell'app e non deve richiedere all'utente di aprire un menu o le impostazioni.
Deve descrivere i dati a cui l'app ha accesso o che raccoglie.
Deve spiegare in che modo i dati verranno utilizzati e/o condivisi.
Non può essere inserita esclusivamente nelle norme sulla privacy o nei termini di servizio; e inoltre
Non può essere inclusa in altre informative non correlate alla raccolta di dati personali o sensibili.

L'informativa in-app della tua app deve essere inclusa con e precedere immediatamente una richiesta di consenso dell'utente e, laddove possibile, un'autorizzazione di runtime associata. Non è permesso accedere o raccogliere dati personali o sensibili senza il consenso dell'utente. La richiesta di consenso dell'app:

Deve presentare la finestra di dialogo per il consenso in modo chiaro e inequivocabile.
Deve richiedere l'accettazione tramite l'intervento dell'utente (ad esempio toccare per accettare o selezionare una casella di controllo).
Non deveconsiderare l'uscita dalla finestra contenente l'informativa (ad esempio tocco fuori dalla finestra o pressione del pulsante Home o Indietro) come un atto di consenso; e inoltre
Non deve utilizzare messaggi con scadenza o chiusura automatica.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Un'app che ha accesso all'insieme di app installate dall'utente e che non considera questi dati come personali o sensibili e soggetti alle norme sulla privacy e ai requisiti sulla Trasmissione sicura e sulla Posizione in evidenza dell'informativa.
Un'app che accede ai dati del telefono dell'utente o della rubrica di contatti e non considera questi dati come personali o sensibili e soggetti alle norme sulla privacy e ai requisiti sulla Trasmissione sicura e sulla Posizione in evidenza dell'informativa.
Un'app che registra la schermata dell'utente e che non tratta tali dati come personali o sensibili e soggetti alle norme sulla privacy.
Un'app che rileva la posizione del dispositivo e non ne spiega in modo esauriente l'utilizzo nel rispetto dei requisiti sopra indicati.

Limitazioni di accesso ai dati sensibili

Oltre ai requisiti precedenti, esistono requisiti relativi ad attività specifiche che vengono riportati nella tabella qui sotto.

Attività	Requisito
L'app gestisce informazioni finanziarie, dati di pagamento o numeri di documenti ufficiali	L'app non deve mai rendere pubblici eventuali dati utente personali o sensibili relativi ad attività finanziarie o di pagamento oppure numeri di documenti ufficiali.
L'app gestisce dati della rubrica o dei contatti non di pubblico dominio	Non è consentita la pubblicazione o la divulgazione non autorizzata di contatti non di pubblico dominio di altre persone.
L'app contiene funzionalità di sicurezza o antivirus, ad esempio funzioni antivirus, antimalware o relative alla sicurezza	L'app deve pubblicare norme sulla privacy che, insieme a eventuali informative in-app, spieghino quali dati utente vengono raccolti e trasmessi nell'app, come vengono utilizzati e con chi vengono condivisi.

EU-U.S. Privacy Shield (scudo UE-USA per la privacy)

In caso di accesso, utilizzo o elaborazione di informazioni personali rese disponibili da Google che identificano l'utente in modo diretto o indiretto e provengono dall'Unione europea o dalla Svizzera ("Informazioni personali dell'UE"), lo sviluppatore è tenuto a:

Rispettare tutte le leggi, le direttive, i regolamenti e le norme vigenti in materia di privacy nonché di sicurezza e protezione dei dati.
Accedere, utilizzare o elaborare Informazioni personali dell'UE solo per scopi conformi al consenso rilasciato dalla persona cui tali informazioni fanno riferimento.

Implementare misure organizzative e tecniche appropriate per proteggere le Informazioni personali dell'UE da perdita, uso improprio, accesso non autorizzato o illegale, divulgazione, alterazione e distruzione. Infine,
Fornire un livello di protezione pari a quello richiesto dai Principi del Privacy Shield (scudo per la privacy).

Lo sviluppatore è tenuto a monitorare regolarmente il rispetto di queste condizioni. Se in qualsiasi momento non potesse rispettare queste condizioni (o se esiste un rischio elevato di non poterle rispettare), è tenuto a informarci immediatamente inviando un'email all'indirizzo data-protection-office@google.com e a interrompere subito l'elaborazione delle Informazioni personali dell'UE o adottare misure ragionevoli e appropriate per ripristinare un adeguato livello di protezione.

Autorizzazioni

Le richieste di autorizzazione devono avere un senso per gli utenti. Lo sviluppatore può richiedere solo le autorizzazioni necessarie per implementare funzionalità o servizi esistenti della sua app che vengono promossi nella sua scheda del Play Store. Non può utilizzare le autorizzazioni che consentono l'accesso ai dati dell'utente o del dispositivo per funzionalità o scopi non dichiarati, non implementati o non consentiti. I dati personali o sensibili accessibili previa autorizzazione non possono mai essere venduti.

Richiedi le autorizzazioni di accesso ai dati all'interno del contesto (tramite Auth incrementale), affinché gli utenti capiscano perché tali autorizzazioni sono necessarie. Utilizza i dati solo per gli scopi a cui l'utente ha acconsentito. Se in un secondo momento vuoi utilizzare i dati per altri scopi, devi prima chiedere agli utenti e accertarti che siano d'accordo con gli usi aggiuntivi.

Autorizzazioni limitate

In aggiunta a quanto sopra, le autorizzazioni limitate sono autorizzazioni definite come Firma o Pericolosa nella nostra documentazione per sviluppatori e sono soggette alle restrizioni e ai requisiti aggiuntivi riportati di seguito:

I dati utente o del dispositivo sensibili a cui si accede tramite Autorizzazioni limitate possono essere trasferiti a terze parti esclusivamente se necessario per fornire o migliorare le funzionalità o i servizi esistenti nell'app da cui sono stati raccolti i dati. È possibile trasferire i dati anche come necessario per rispettare le leggi vigenti o nell'ambito di una fusione, un'acquisizione o una vendita di attività, fornendo agli utenti adeguato preavviso ai sensi di legge. Tutti gli altri tipi di trasferimenti o vendite dei dati utente sono vietati.
Se gli utenti rifiutano una richiesta di Autorizzazione limitata, è necessario rispettare la loro decisione. Gli utenti non possono essere manipolati o forzati a concedere autorizzazioni non fondamentali. È necessario compiere un ragionevole sforzo per supportare gli utenti che non concedono l'accesso ad autorizzazioni sensibili, ad

esempio consentendo loro di inserire manualmente un numero di telefono se hanno limitato l'accesso ai registri chiamate.

Alcune Autorizzazioni limitate potrebbero essere soggette a requisiti aggiuntivi, come descritto di seguito. L'obiettivo di queste restrizioni è tutelare la privacy degli utenti. Potremmo concedere limitate eccezioni ai requisiti che seguono in rari casi in cui le app forniscano una funzionalità molto interessante o fondamentale e non esistano metodi alternativi per fornire tale funzionalità. Le eccezioni richieste vengono valutate in base al potenziale impatto sulla privacy o sulla sicurezza degli utenti.

Autorizzazioni SMS e Registro chiamate

Le Autorizzazioni SMS e Registro chiamate sono considerate dati utente personali e sensibili soggetti alle norme relative a Informazioni personali e sensibili e alle seguenti restrizioni:

Autorizzazione limitata	**Requisito**
Gruppo di autorizzazioni Registro chiamate (ad esempio READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Deve essere registrato e attivo come gestore predefinito del telefono o dell'assistente sul dispositivo.
Gruppo di autorizzazioni SMS (ad esempio, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Deve essere registrato e attivo come gestore predefinito di SMS o dell'assistente sul dispositivo.

Le app prive di funzionalità di gestore predefinito di SMS, telefono o assistente non possono dichiarare l'uso di queste autorizzazioni nel file manifest, incluso testo segnaposto. Inoltre, le app devono essere registrate attivamente come gestore predefinito di SMS, telefono o assistente prima di chiedere agli utenti di accettare le autorizzazioni di cui sopra e devono interrompere immediatamente l'utilizzo dell'autorizzazione qualora non siano più il gestore predefinito. Le eccezioni e gli usi consentiti sono disponibili in questa pagina del Centro assistenza.

Le app possono utilizzare l'autorizzazione (e tutti i dati da questa derivati) solo per fornire la funzionalità principale e approvata dell'app. La funzionalità principale è definita come lo scopo primario dell'app e può comprendere un insieme di funzionalità di base, che devono essere tutte documentate e promosse in evidenza nella descrizione dell'app. Senza la funzionalità o le funzionalità di base, l'app non funziona o è inutilizzabile. Il trasferimento, la condivisione o l'uso autorizzato mediante licenza di questi dati deve avvenire solo ed esclusivamente allo scopo di fornire funzionalità o servizi fondamentali all'interno dell'app e il loro uso non deve mai essere esteso a nessun altro scopo (ad esempio per migliorare altre app o servizi, per scopi pubblicitari o di marketing). Non è possibile utilizzare metodi alternativi (incluse altre autorizzazioni, API o

fonti di terze parti) per ricavare i dati attribuiti alle autorizzazioni relative al registro chiamate o agli SMS.

Autorizzazioni di accesso alla posizione

Aggiornamento del 16 aprile 2020: ci rendiamo conto che la conformità alle Norme sulla posizione richiederà ad alcuni sviluppatori un certo sforzo, pertanto prevediamo una tempistica ampia per apportare le dovute modifiche. Per visualizzare tempistiche e altri aggiornamenti, visita il nostro Centro assistenza.

La posizione del dispositivo è considerata un dato utente personale e sensibile soggetto alle norme relative a Informazioni personali e sensibili e ai seguenti requisiti:

> Le app non possono accedere ai dati protetti dalle autorizzazioni di accesso alla posizione (ad esempio, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) quando non sono più necessari per offrire le funzionalità o i servizi inclusi nell'app.
> Lo sviluppatore non dovrebbe mai richiedere agli utenti le autorizzazioni di accesso alla posizione esclusivamente a scopi pubblicitari o di analisi. Le app che estendono l'utilizzo autorizzato di questi dati per la pubblicazione di annunci devono essere conformi alle nostre Norme relative agli annunci.
> Le app devono richiedere l'ambito minimo necessario (ad esempio, generico anziché specifico e in primo piano anziché in background) per fornire la funzionalità o il servizio corrente che richiede la posizione; inoltre, per gli utenti deve essere ragionevolmente prevedibile che la funzionalità o il servizio richieda il livello di posizione richiesto. Ad esempio, eventuali app che richiedano o accedano alla posizione in background senza una giustificazione convincente potranno essere rifiutate.
> La posizione in background può essere utilizzata soltanto per fornire funzioni utili all'utente e attinenti alla funzionalità di base dell'app.

Le app possono accedere alla posizione usando l'autorizzazione di accesso al servizio in primo piano (che prevede per l'app soltanto l'accesso in primo piano, ad esempio "durante l'uso") se l'uso:

> È stato iniziato come continuazione di un'azione avviata dall'utente nell'app e inoltre
> Cessa immediatamente dopo che il caso d'uso previsto dell'azione avviata dall'utente viene completato dall'applicazione.

Le app progettate specificatamente per bambini e ragazzi devono essere conformi alle norme del programma Per la famiglia.

Utilizzo illecito di dispositivi e reti

Sono vietate le app che interrompono, danneggiano, interferiscono con il funzionamento o accedono in modo non autorizzato al dispositivo dell'utente, altri dispositivi o computer, server, reti, API (Application Programming Interface, interfaccia di programmazione di un'applicazione)

o servizi, inclusi, a titolo esemplificativo, altre app sul dispositivo, servizi di Google o la rete di un operatore autorizzato.

Le app su Google Play devono rispettare i requisiti di ottimizzazione del sistema Android predefiniti e documentati nelle Norme fondamentali sulla qualità delle app per Google Play.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App che bloccano o interferiscono con un'altra app mostrando annunci.
App che alterano il gameplay di altre app.
App che facilitano la compromissione di servizi, software o hardware, l'elusione di misure di sicurezza o che forniscono istruzioni a riguardo.
App che utilizzano o accedono a un servizio o a un'API con modalità che costituiscono una violazione dei relativi termini di servizio.
App che tentano di aggirare le misure di gestione dell'alimentazione del sistema e che non sono idonee a essere autorizzate.
App che facilitano servizi proxy verso terzi possono farlo solo laddove questo sia lo scopo principale dell'app proposto all'utente.

Comportamento dannoso

Sono vietate le app che carpiscono dati, monitorano in segreto o danneggiano gli utenti o che sono dannose in altro modo.

Un'app distribuita tramite Google Play non può essere modificata, sostituita o aggiornata utilizzando metodi diversi dal meccanismo di aggiornamento di Google Play. Un'app non può inoltre scaricare codice eseguibile (ad esempio file dex, JAR e .so) da una fonte diversa da Google Play. Questa limitazione non riguarda il codice che viene eseguito su una macchina virtuale e ha accesso limitato alle API Android (ad esempio JavaScript in una WebView o in un browser).

È possibile scaricare risorse aggiuntive delle app (ad esempio, asset relativi a giochi) solo quando necessarie all'utilizzo dell'app da parte dell'utente. Le risorse scaricate devono essere conformi a tutte le norme di Google Play e, prima di iniziare il download, l'app dovrebbe informare gli utenti e mostrare in maniera chiara le dimensioni del download.

Le app di sorveglianza e spyware commerciale sono esplicitamente proibite su Google Play. Solo le app conformi alle norme, progettate e commercializzate esclusivamente per il monitoraggio dei genitori o la gestione aziendale, possono essere distribuite nello Store con funzioni di tracciamento e reporting, purché siano pienamente conformi ai requisiti descritti di seguito.

I componenti seguenti sono espressamente vietati:

Virus, trojan horse, malware, spyware o altro software dannoso.
App che agevolano o rimandano alla distribuzione o all'installazione di software dannoso.
App o SDK che scaricano codice eseguibile, ad esempio file dex o codice nativo, da una fonte diversa da Google Play.
App che introducono o sfruttano vulnerabilità di sicurezza.
App che carpiscono i dati di autenticazione degli utenti (ad esempio nomi utente o password) o che imitano altri siti web o app per indurre con l'inganno gli utenti a comunicare informazioni personali o dati di autenticazione.
Le app non devono mostrare dati reali o non verificati relativi a individui o entità non consenzienti, ad esempio numeri telefonici, contatti, indirizzi o informazioni personali.
App che installano altre app su un dispositivo senza previo consenso dell'utente.
App con download facilitati da Rete CDN (Content Delivery Network) che non informano l'utente e non specificano le dimensioni del download prima dello stesso.
App ideate per raccogliere di nascosto dati sull'utilizzo del dispositivo, ad esempio app spyware commerciali.

App che monitorano o tengono traccia del comportamento di un utente su un dispositivo devono rispettare i seguenti requisiti:

Le app non devono essere presentate come soluzioni per spionaggio o sorveglianza segreta.
Le app non devono nascondere o mascherare il comportamento di monitoraggio oppure tentare di ingannare gli utenti in merito a tale funzionalità.
È necessario presentare agli utenti una notifica costante e un'icona univoca che identifichi in modo chiaro l'app.
Le app e le relative schede su Google Play non devono consentire in alcun modo di attivare o accedere a funzionalità che violano i presenti termini, ad esempio link che rimandano a un APK non conforme non ospitato su Google Play.
Sei l'unico responsabile della determinazione della legalità della tua app nel relativo paese di destinazione. Le app ritenute illegali nelle località in cui vengono pubblicate verranno rimosse.

Scopri il nostro Programma App Security Improvement per ulteriori informazioni sui problemi di sicurezza più recenti segnalati agli sviluppatori su Google Play. Puoi trovare informazioni dettagliate su vulnerabilità e soluzioni nel link della pagina di assistenza di ogni campagna.

Comportamento ingannevole

Sono vietate le app che cercano di ingannare gli utenti o di favorire comportamenti disonesti, incluse a titolo esemplificativo ma non esaustivo tutte le app il cui funzionamento sia determinato essere impossibile. Le app devono contenere comunicazioni, descrizioni e immagini/video precisi relativi alla loro funzionalità in ogni parte dei metadati e offrire le prestazioni ragionevolmente attese dall'utente. Non devono cercare di imitare funzionalità e

avvisi del sistema operativo o di altre app. Eventuali modifiche alle impostazioni del dispositivo non devono essere apportate all'insaputa e senza il consenso dell'utente e devono poter essere agevolmente ripristinate dall'utente stesso.

Dichiarazioni ingannevoli

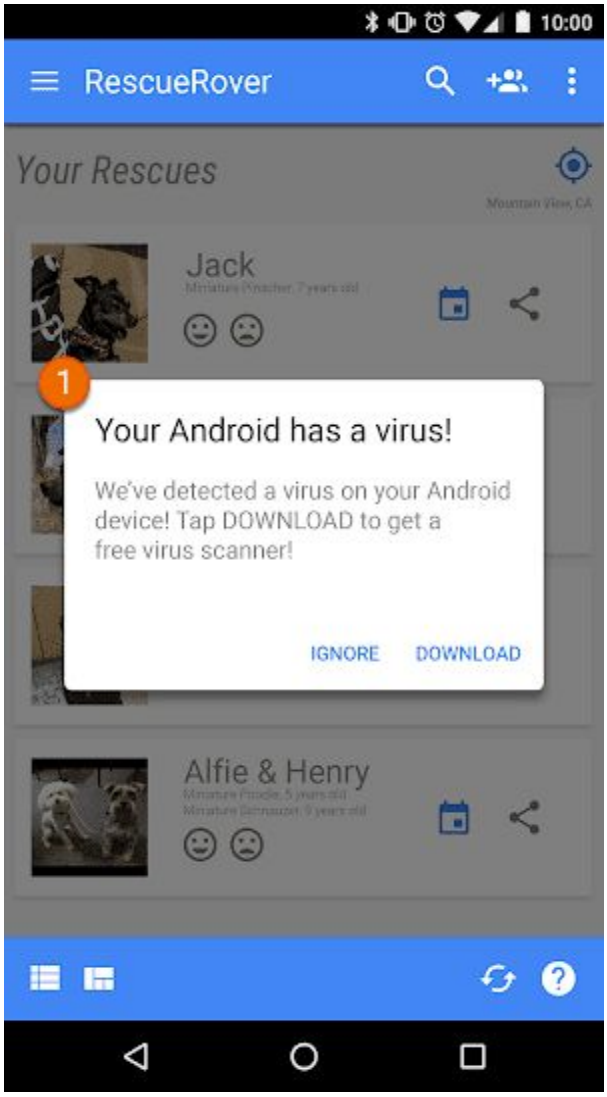
Non sono ammesse le app contenenti informazioni o dichiarazioni false o fuorvianti, neanche nella descrizione, nel titolo, nell'icona e negli screenshot.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- App contenenti rappresentazioni ingannevoli oppure descrizioni non precise e chiare in merito alla loro funzionalità:
  - Un'app contenente una descrizione e alcuni screenshot che suggeriscono che si tratta di un gioco di corse automobilistiche quando, in realtà, si tratta di un gioco di puzzle per cui viene utilizzata l'immagine di un'auto.
  - Un'app presentata come un'app antivirus, ma che in realtà contiene soltanto una guida di testo che spiega come rimuovere i virus.
- Nomi di app o sviluppatori che rappresentano in modo ingannevole il rispettivo stato o rendimento su Google Play (ad esempio, dichiarare di far parte delle categorie "Da non perdere", "App numero uno", "Più vendute").
- App con contenuti o funzionalità mediche o relative alla salute che sono ingannevoli o potenzialmente dannose.
- App che dichiarano di avere funzionalità che in realtà non è possibile implementare.
- App classificate in modo errato.
- Contenuti manifestamente ingannevoli che potrebbero interferire con processi di voto.
- App che dichiarano, contrariamente al vero, un'affiliazione con entità governative o di offrire o facilitare servizi governativi per i quali non sono autorizzate.

Utilizzo non autorizzato o imitazione di funzionalità di sistema

Non sono consentiti annunci o app che imitano o interferiscono con le funzionalità di sistema, ad esempio notifiche o avvisi. È possibile utilizzare le notifiche a livello di sistema soltanto per funzionalità integranti di un'app, ad esempio l'app di una compagnia aerea che avvisa gli utenti di promozioni speciali o un gioco che avvisa gli utenti di promozioni in-game.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App o annunci che vengono pubblicati tramite una notifica o un avviso di sistema:



① La notifica di sistema mostrata in questa app viene utilizzata per pubblicare un annuncio.

Per altri esempi relativi agli annunci, leggere le Norme relative agli annunci.

Modifiche ingannevoli alle impostazioni del dispositivo

Sono vietate le app che apportano modifiche alle impostazioni o alle funzionalità del dispositivo dell'utente al di fuori dell'app, all'insaputa e senza il consenso dell'utente. Le impostazioni e funzionalità del dispositivo includono: impostazioni del sistema e del browser, segnalibri, scorciatoie, icone, widget e la presentazione di app nella schermata Home.

Sono inoltre vietate:

App che modificano le impostazioni o funzionalità del dispositivo con il consenso dell'utente, ma con modalità che non consentono un facile ripristino.
App o annunci che modificano le impostazioni o funzionalità del dispositivo come servizio per terze parti o per scopi pubblicitari.
App che inducono con l'inganno gli utenti a rimuovere o disattivare app di terze parti oppure a modificare impostazioni o funzionalità del dispositivo.
App che esortano o incoraggiano gli utenti a rimuovere o disattivare app di terze parti oppure a modificare impostazioni o funzionalità del dispositivo, se non nell'ambito di un servizio di sicurezza verificabile.

Favorire comportamenti disonesti

Non sono ammesse le app che aiutino gli utenti a ingannare altri o che siano in qualsiasi modo ingannevoli dal punto di vista funzionale incluse, a titolo esemplificativo ma non esaustivo, app che generano o favoriscono la generazione di carte d'identità, codici fiscali, passaporti, diplomi, carte di credito e patenti di guida. Le app devono contenere comunicazioni, titoli, descrizioni e immagini/video accurati in relazione alla loro funzionalità e/o ai loro contenuti e funzionare nel modo ragionevolmente e fedelmente atteso dall'utente.

Le app eventualmente indicate come "scherzi" o "aventi scopi di intrattenimento" (o altri termini similari) non sono esenti dall'applicazione delle nostre norme.

Contenuti multimediali manipolati

Sono vietate le app che promuovono o contribuiscono a creare informazioni o dichiarazioni false o fuorvianti trasmesse attraverso immagini, video e/o testo. Sono vietate le app che vengano determinate promuovere o perpetuare immagini, video e/o testo oggettivamente fuorvianti o ingannevoli, che potrebbero causare danni in relazione a un evento sensibile, a questioni politiche, a problemi sociali o altre questioni di pubblico interesse.

Le app che manipolano o alterano contenuti multimediali, al di là delle modifiche accettabili da un punto di vista editoriale allo scopo di migliorare qualità o chiarezza, devono visualizzare i contenuti alterati in modo evidente o con un watermark, laddove all'utente medio possa non essere chiaro che tali contenuti sono stati alterati. Eccezioni possono essere contemplate nel caso di questioni di interesse pubblico oppure di satira o parodia evidenti.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App che aggiungono un personaggio pubblico a una dimostrazione durante un evento politicamente sensibile.
App che utilizzano personaggi pubblici o contenuti multimediali correlati a un evento sensibile per pubblicizzare la capacità di alterazione di contenuti multimediali all'interno della scheda dello Store di un'app.

App che alterano clip multimediali per simulare un notiziario.

Rappresentazione ingannevole

Non sono consentiti app o account sviluppatore che commettano furti d'identità a danno di persone o di organizzazioni oppure che nascondano o rappresentino in modo ingannevole informazioni sulla propria proprietà o sul proprio scopo principale. Non sono consentiti account sviluppatore o app che intraprendono attività coordinate allo scopo di ingannare gli utenti. Sono inclusi, a titolo esemplificativo, gli account sviluppatore o le app che travisano o nascondono il proprio paese di origine e sono rivolti agli utenti di un altro paese.

Malware

Le nostre norme sul Malware sono semplici: l'ecosistema Android, incluso il Google Play Store, e i dispositivi degli utenti dovrebbero essere privi di comportamenti dannosi, come i malware. Sulla base di questo principio fondamentale, ci impegniamo per offrire un ecosistema Android sicuro per i nostri utenti e i loro dispositivi.

Si definisce malware qualsiasi codice che potrebbe mettere a rischio un dispositivo, un utente o i suoi dati. Il termine malware include, a titolo esemplificativo ma non esaustivo, applicazioni potenzialmente dannose, modifiche di framework o programmi binari, appartenenti a varie categorie, ad esempio app di spyware, phishing o trojan. L'elenco delle categorie viene completato e aggiornato continuamente da Google.

Sebbene siano diversi per tipologia e capacità, i malware in genere hanno uno dei seguenti obiettivi:

Compromettere l'integrità del dispositivo dell'utente.
Assumere il controllo del dispositivo dell'utente.
Attivare operazioni controllate a distanza affinché un utente malintenzionato possa accedere, utilizzare o altrimenti sfruttare un dispositivo infetto.
Trasmettere dati personali o credenziali dal dispositivo senza adeguata comunicazione e senza il consenso dell'utente.
Diffondere spam o comandi dal dispositivo infetto per colpire altri dispositivi o reti.
Defraudare l'utente.

La modifica di un framework, un programma binario o un'app può essere potenzialmente dannosa e pertanto generare comportamenti dannosi, anche in modo non intenzionale. Ciò avviene perché le modifiche di framework, programmi binari o app possono dar luogo a funzionamenti diversi in base a una serie di variabili. Pertanto, ciò che è dannoso per un dispositivo Android potrebbe non porre alcun rischio per un altro. Ad esempio, un dispositivo con la versione più recente di Android non è interessato da app dannose che utilizzano API deprecate per eseguire comportamenti dannosi, ma un dispositivo con una delle prime versioni di Android potrebbe essere a rischio. Modifiche di app, programmi binari o framework vengono

segnalate come malware o app potenzialmente dannose se rappresentano un rischio evidente per alcuni o per tutti i dispositivi Android e gli utenti.

Le categorie di malware indicate di seguito riflettono la nostra profonda convinzione secondo cui gli utenti dovrebbero capire come il loro dispositivo viene sfruttato e contribuire alla sicurezza di un ecosistema che garantisca innovazioni valide e un'esperienza utente affidabile.

Visita Google Play Protect per ulteriori informazioni.

Backdoor

Codice che consente l'esecuzione su un dispositivo di operazioni controllate a distanza, indesiderate e potenzialmente dannose.

Queste operazioni potrebbero includere un comportamento che, se eseguito automaticamente, determinerebbe l'inclusione della modifica a framework, programmi binari o app in una delle altre categorie di malware. In generale, con il termine backdoor si descrive la modalità con cui un'operazione potenzialmente dannosa può verificarsi su un dispositivo, pertanto il termine non corrisponde esattamente a categorie quali frode di fatturazione o spyware commerciale. Conseguentemente, un sottoinsieme di backdoor, in determinate circostanze, viene considerato da Google Play Protect come una vulnerabilità.

Frode di fatturazione

Codice che effettua addebiti automatici agli utenti in modo intenzionalmente ingannevole.

La frode di fatturazione su dispositivi mobili può essere: frode tariffaria, SMS fraudolento o chiamata fraudolenta.

SMS fraudolento

Codice che effettua addebiti agli utenti per l'invio di SMS a pagamento senza il loro consenso o che cerca di camuffare le sue attività SMS nascondendo gli accordi di divulgazione o gli SMS dell'operatore di telefonia mobile che informano gli utenti degli addebiti o che confermano gli abbonamenti.

Esiste del codice che, anche se tecnicamente comunica il comportamento di invio degli SMS, introduce un comportamento aggiuntivo che consente l'SMS fraudolento. Ecco alcuni esempi: nascondere parti di un accordo di divulgazione agli utenti o renderle illeggibili ed eliminare condizionalmente gli SMS dell'operatore di telefonia mobile che informano gli utenti degli addebiti o confermano un abbonamento.

Chiamata fraudolenta

Codice che effettua addebiti agli utenti chiamando numeri a pagamento senza il consenso degli utenti.

Frode tariffaria

Codice che induce con l'inganno gli utenti ad abbonarsi a contenuti o ad acquistarli tramite il loro conto telefonico.

La frode tariffaria include qualsiasi tipo di fatturazione ad eccezione di SMS e chiamate verso numerazioni a sovrapprezzo. Ecco alcuni esempi: fatturazione diretta con l'operatore, punto di accesso wireless (WAP) e trasferimento di credito tra dispositivi mobili. La frode WAP è uno dei tipi di frode tariffaria più usati. Chi attua questo tipo di frode potrebbe indurre con l'inganno gli utenti a fare clic su un pulsante in un componente WebView trasparente caricato in modo invisibile. Questa azione avvia un abbonamento ricorrente e l'email o l'SMS di conferma vengono spesso compromessi per evitare che gli utenti si accorgano della transazione finanziaria.

Spyware commerciale

Codice che trasmette informazioni personali dal dispositivo senza un'adeguata comunicazione o senza il consenso e non visualizza una notifica persistente in merito allo svolgimento di tale operazione.

Le app spyware commerciali trasmettono dati a una parte diversa dal fornitore di app potenzialmente dannose. I genitori potrebbero usare forme lecite di queste app per monitorare i loro figli. Tuttavia, queste app non possono essere usate per monitorare una persona (ad esempio il coniuge) a sua insaputa o senza il suo consenso se non viene visualizzata una notifica persistente durante la trasmissione dei dati.

Denial of service (DoS)

Codice che, a insaputa dell'utente, esegue un attacco denial of service (DoS) o fa parte di un attacco DoS distribuito contro altri sistemi e risorse.

Ad esempio, l'attacco potrebbe consistere nell'invio di un volume elevato di richieste HTTP per sovraccaricare server remoti.

Downloader ostili

Codice che non è potenzialmente dannoso di per sé, ma che scarica altre app potenzialmente dannose.

Il codice potrebbe essere un downloader ostile se:

> Esiste motivo di ritenere che sia stato creato per diffondere app potenzialmente dannose e che abbia scaricato tali app o che contenga codice che potrebbe scaricare e installare app; oppure

Almeno il 5% delle app scaricate dal codice è formato da app potenzialmente dannose con una soglia minima di 500 download di app osservate (25 download di app potenzialmente dannose osservate).

I principali browser e app per la condivisione di file non sono considerati downloader ostili se:

Non favoriscono download senza interazione dell'utente; e
Tutti i download di app potenzialmente dannose vengono attivati da utenti consenzienti.

Minaccia non Android

Codice contenente minacce non Android.

Queste app non possono danneggiare l'utente o il dispositivo Android, ma contengono componenti potenzialmente dannosi per altre piattaforme.

Phishing

Codice che finge di provenire da una fonte affidabile, richiede le credenziali per l'autenticazione o i dati di fatturazione dell'utente e invia tali dati a una terza parte. Questa categoria, inoltre, si applica al codice che intercetta la trasmissione delle credenziali dell'utente in transito.

Tra gli obiettivi di phishing comuni, credenziali bancarie, numeri di carte di credito e credenziali di account online per social network e giochi.

Abuso di privilegio elevato

Codice che compromette l'integrità del sistema violando la sandbox dell'app, ottenendo privilegi elevati o modificando o disattivando l'accesso alle principali funzioni correlate alla sicurezza.

Tra gli esempi possibili:

Un'app che viola il modello di autorizzazioni Android o sottrae le credenziali (ad esempio, i token OAuth) da altre app.
App che abusano di funzionalità per evitare di essere disinstallate o arrestate.
Un'app che disattiva SELinux.

Le app di escalation dei privilegi che eseguono il rooting dei dispositivi senza l'autorizzazione dell'utente sono classificate come app di rooting.

Ransomware

Codice che assume il controllo parziale o totale di un dispositivo o dei dati su un dispositivo ed esige dall'utente un pagamento o un'azione per rilasciare il controllo.

Alcuni tipi di ransomware criptano i dati sul dispositivo ed esigono un pagamento per decriptare i dati e/o sfruttano le funzionalità di amministratore del dispositivo in modo che il ransomware non possa essere rimosso da un utente medio. Tra gli esempi possibili:

Impedire all'utente di accedere al dispositivo ed esigere denaro in cambio del ripristino del controllo da parte dell'utente.
Criptare i dati sul dispositivo ed esigere un pagamento, verosimilmente in cambio della decriptazione dei dati.
Sfruttare le funzionalità di Gestione norme del dispositivo e bloccare la rimozione da parte dell'utente.

Eventuale codice distribuito con il dispositivo la cui finalità primaria sia la gestione di un dispositivo sovvenzionato può essere escluso dalla categoria del ransomware, a condizione che soddisfi i requisiti per la gestione e il blocco sicuri, nonché i requisiti di comunicazione e consenso adeguati da parte dell'utente.

Rooting

Codice che esegue il rooting del dispositivo.

C'è una differenza tra codice di rooting non dannoso e dannoso. Ad esempio, le app di rooting non dannoso consentono agli utenti di sapere in anticipo che stanno per eseguire il rooting del dispositivo e non eseguono altre azioni potenzialmente dannose che riguardano altre categorie di app potenzialmente dannose.

Le app di rooting dannoso non comunicano agli utenti che stanno per eseguire il rooting del dispositivo e non li informano anticipatamente del rooting; eseguono inoltre altre azioni che riguardano altre categorie di app potenzialmente dannose.

Spam

Codice che invia messaggi non richiesti ai contatti dell'utente o che utilizza il dispositivo per l'inoltro di spam via email.

Spyware

Codice che trasmette dati personali dal dispositivo senza un'adeguata comunicazione o consenso.

Ad esempio, la trasmissione di una qualsiasi delle seguenti informazioni senza comunicazione o in una modalità inaspettata per l'utente può essere già considerata spyware:

Elenco contatti
Fotografie o altri file provenienti dalla scheda SD o che non sono di proprietà dell'app
Contenuti provenienti dall'email dell'utente
Registro chiamate
Registro SMS
Cronologia web o preferiti del browser predefinito
Informazioni provenienti dalle directory /data/ di altre app.

Possono essere definiti spyware anche comportamenti che possono essere considerati come spionaggio a danno dell'utente. Ad esempio, la registrazione di audio o di chiamate ricevute sul telefono o il furto di dati app.

Trojan

Codice apparentemente innocuo, ad esempio un gioco che dichiara di essere esclusivamente tale, ma che esegue azioni indesiderate nei confronti dell'utente.

In genere questa classificazione è utilizzata insieme ad altre categorie di app potenzialmente dannose. Un trojan ha un componente innocuo e un componente dannoso nascosto. Ad esempio, un gioco che invia messaggi SMS premium dal dispositivo dell'utente in background e senza che l'utente ne sia a conoscenza.

Una nota sulle app non comuni

Le app nuove e meno diffuse possono essere classificate come non comuni se Google Play Protect non dispone di informazioni sufficienti per autorizzarle come app sicure. Ciò non significa che l'app è necessariamente dannosa, ma in assenza di un'ulteriore revisione non può nemmeno essere autorizzata come app sicura.

Una nota sulla categoria Backdoor

La classificazione della categoria di malware backdoor si basa sulla modalità con cui il codice agisce. Una condizione necessaria affinché un codice venga classificato come backdoor è che consenta un comportamento che, se eseguito automaticamente, determinerebbe l'inclusione del codice in una delle altre categorie di malware. Ad esempio, se un'app consente il caricamento di codice dinamico e il codice caricato dinamicamente estrae SMS, l'app verrà classificata come malware backdoor.

Tuttavia, se un'app consente l'esecuzione arbitraria di codice e non abbiamo ragione di credere che tale esecuzione sia stata aggiunta al fine di dar luogo a un comportamento malevolo, l'app verrà considerata come contenente una vulnerabilità, anziché essere definita malware backdoor, e allo sviluppatore verrà chiesto di creare una patch per l'app medesima.

Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic qui per leggere le norme relative agli annunci di giochi e scommesse.
Google Play supporta una serie di strategie di monetizzazione a vantaggio di sviluppatori e utenti, inclusi prodotti in-app, distribuzione a pagamento, abbonamenti e modelli basati su annunci. Per poter garantire la migliore esperienza possibile agli utenti, gli sviluppatori sono tenuti a rispettare le presenti norme.

Pagamenti

Le app che offrono acquisti in negozio o in-app devono essere conformi alle linee guida che seguono.

Acquisti in negozio: gli sviluppatori devono addebitare il costo di app e download da Google Play utilizzando il sistema di pagamento di Google Play.

Acquisti in-app:

- Gli sviluppatori che offrono prodotti all'interno di un gioco scaricato da Google Play o che danno accesso ai contenuti di un gioco devono utilizzare la Fatturazione in-app di Google Play come metodo di pagamento.
- Gli sviluppatori che offrono prodotti all'interno di un'altra categoria di app scaricate da Google Play devono utilizzare la Fatturazione in-app di Google Play come metodo di pagamento, tranne nei seguenti casi:
  - Il pagamento riguarda esclusivamente prodotti fisici.
  - Il pagamento riguarda contenuti digitali che potrebbero essere consumati all'esterno dell'app stessa (ad esempio brani che possono essere ascoltati su altri lettori di musica).
- Le valute virtuali in-app devono essere utilizzate soltanto all'interno dell'app o del gioco in cui sono state acquistate.
- Gli sviluppatori non devono ingannare gli utenti in merito alle app o a eventuali servizi, beni, contenuti o funzionalità in-app in vendita. Se la descrizione del prodotto su Google Play fa riferimento a funzionalità in-app a cui viene applicato un costo specifico o aggiuntivo, la descrizione deve indicare in modo chiaro agli utenti che l'accesso a tali funzionalità è a pagamento.
- Le app che offrono meccanismi per ricevere articoli virtuali randomizzati da un acquisto (ad esempio, "loot box") devono indicare chiaramente le probabilità di ricevere tali articoli prima dell'acquisto.

Abbonamenti

Lo sviluppatore non deve fuorviare gli utenti in merito a servizi o contenuti in abbonamento offerti all'interno dell'app. È fondamentale comunicare in modo chiaro in tutte le promozioni in-app o nelle schermate iniziali.

Nell'app: lo sviluppatore deve essere trasparente in merito alla propria offerta. Questo significa, tra le altre cose, indicare esplicitamente i termini dell'offerta, il costo dell'abbonamento, la frequenza del ciclo di fatturazione e se sia necessario un abbonamento per usare l'app. Agli utenti non dovrebbe essere richiesta alcuna ulteriore azione per esaminare le informazioni.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Abbonamenti mensili che non informano gli utenti del fatto che il rinnovo sarà automatico e che l'addebito avverrà ogni mese.
- Abbonamenti annuali che evidenziano il prezzo in termini di costo mensile.
- Termini e prezzi dell'abbonamento localizzati in modo incompleto.
- Promozioni in-app che non spiegano chiaramente che l'utente può accedere ai contenuti anche senza abbonamento (quando disponibile).
- Nomi di SKU che non riflettono in modo accurato il tipo di abbonamento, ad esempio "Prova gratuita" per un abbonamento con addebito con rinnovo automatico.

1

X

Get AnalyzeAPP Premium

16 issues found in your data!

Subscribe to see how we can help

2

12 months

$9.16/mo

Save 35%!

6 months

$12.50/mo

Save 11%!

MOST POPULAR PLAN

1 month

$14.00/mo

3

Try for $12.50!

① Il pulsante Ignora non è chiaramente visibile e gli utenti potrebbero non comprendere che possono accedere alla funzionalità senza accettare l'offerta dell'abbonamento.

② Il prezzo dell'offerta viene visualizzato solo in termini di costo mensile e gli utenti potrebbero non comprendere che verrà addebitato loro il costo semestrale in un'unica soluzione al momento della sottoscrizione dell'abbonamento.

③ L'offerta mostra solo il prezzo di lancio e gli utenti potrebbero non comprendere la cifra che verrà loro addebitata automaticamente al termine del periodo di lancio.

④ L'offerta deve essere localizzata nella stessa lingua dei termini e condizioni, in modo tale che gli utenti possano comprendere l'offerta completa.

Prove gratuite e offerte di lancio

Prima che un utente attivi l'abbonamento offerto dall'app: lo sviluppatore deve specificare in modo chiaro e preciso i termini della sua offerta includendo la durata, i prezzi e una descrizione dei contenuti o dei servizi accessibili. Lo sviluppatore deve assicurarsi di informare l'utente di quando e come una prova gratuita si convertirà in un abbonamento a pagamento, di quanto costerà tale abbonamento e del fatto che l'utente potrà annullare la prova gratuita qualora non voglia che si converta in un abbonamento a pagamento.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Offerte che non spiegano chiaramente quanto durerà la prova gratuita o il prezzo di lancio.
- Offerte che non spiegano chiaramente che, al termine del periodo dell'offerta, per l'utente verrà automaticamente attivato un abbonamento a pagamento.
- Offerte che non spiegano chiaramente che l'utente può accedere ai contenuti senza una prova (quando disponibile).
- Prezzi e termini dell'offerta localizzati in modo incompleto.

1

X

Get AnalyzeAPP Premium

16 issues found in your data!

Subscribe to see how we can help

2

★ Try for free now!

3

During your free trial, experience all of the great features our app can offer!

4

Cancele su suscripción en cualquier momento. Por favor, consulte nuestra política de privacidad para más información.

① Il pulsante Ignora non è chiaramente visibile e gli utenti potrebbero non comprendere che possono accedere alla funzionalità senza iscriversi alla prova gratuita.

② L'offerta mette in evidenza la prova gratuita e gli utenti potrebbero non comprendere che il costo verrà loro addebitato automaticamente alla fine del periodo di prova.

③ L'offerta non specifica il periodo di prova e gli utenti potrebbero non comprendere per quanto tempo durerà il loro accesso gratuito ai contenuti in abbonamento.

④ L'offerta deve essere localizzata nella stessa lingua dei termini e condizioni, in modo tale che gli utenti possano comprendere l'offerta completa.

Gestione e annullamento dell'abbonamento

In qualità di sviluppatore, devi assicurarti che le tue app indichino chiaramente in che modo gli utenti possono gestire o annullare il loro abbonamento.

Se un utente annulla un abbonamento acquistato da un'app su Google Play, le norme di Google prevedono che l'utente non riceva un rimborso per il periodo di fatturazione corrente, ma che continui a ricevere i contenuti in abbonamento per il resto di tale periodo di fatturazione a prescindere dalla data dell'annullamento. L'annullamento da parte dell'utente diventa valido al termine del periodo di fatturazione corrente.

In qualità di fornitore dei contenuti o dell'accesso, puoi implementare norme sui rimborsi più flessibili direttamente con i tuoi utenti. È responsabilità dello sviluppatore informare gli utenti in merito a eventuali modifiche apportate alle norme su abbonamento, annullamento e rimborsi e assicurarsi che tali norme siano conformi alla legge vigente.

Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic qui per leggere le norme relative agli annunci di giochi e scommesse.
Sono vietate le app contenenti annunci ingannevoli o improvvisi. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati. Gli annunci pubblicati nell'app vengono considerati parte dell'app e devono essere conformi a tutte le nostre norme. Fai clic qui per leggere le norme relative agli annunci di giochi e scommesse.

Utilizzo dei dati sulla posizione per gli annunci

Le app che estendono l'utilizzo dei dati sulla posizione del dispositivo basati sull'autorizzazione per la pubblicazione di annunci sono soggette alle norme relative a Informazioni personali e dati sensibili e devono inoltre soddisfare i seguenti requisiti:

> L'utilizzo o la raccolta per scopi pubblicitari di dati sulla posizione del dispositivo basati sull'autorizzazione devono essere chiari all'utente e documentati nelle norme sulla privacy obbligatorie dell'app, incluso il collegamento a eventuali norme sulla privacy di reti pubblicitarie pertinenti, relative all'utilizzo dei dati sulla posizione.

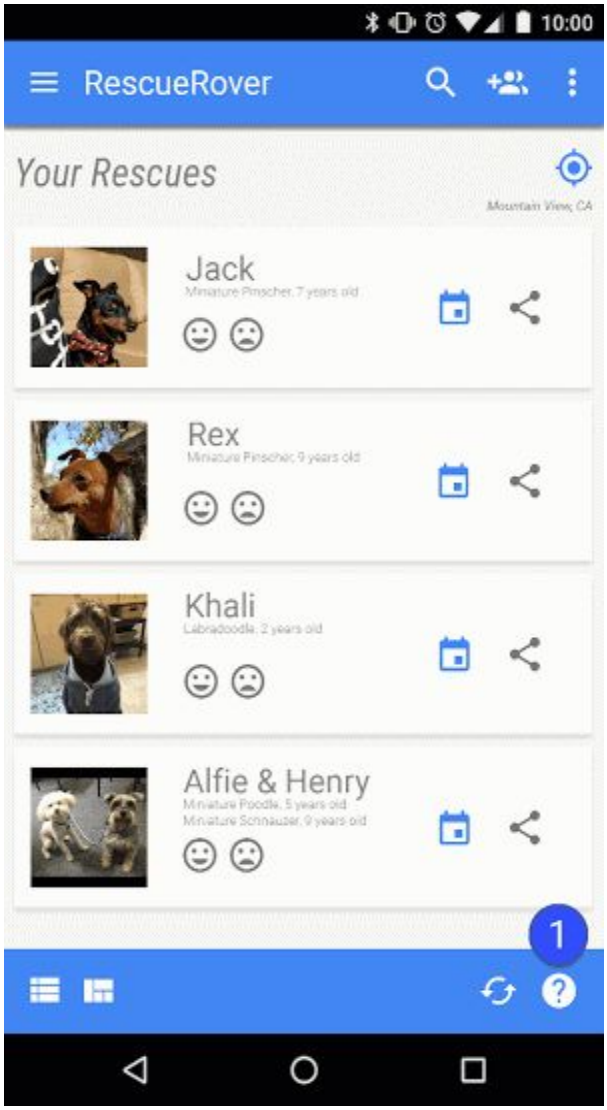
In base ai requisiti relativi alle Autorizzazioni di accesso alla posizione, tali autorizzazioni possono essere richieste esclusivamente per implementare funzionalità o servizi esistenti nell'app e non è possibile richiedere autorizzazioni di accesso alla posizione del dispositivo esclusivamente per l'uso di annunci.

Annunci ingannevoli

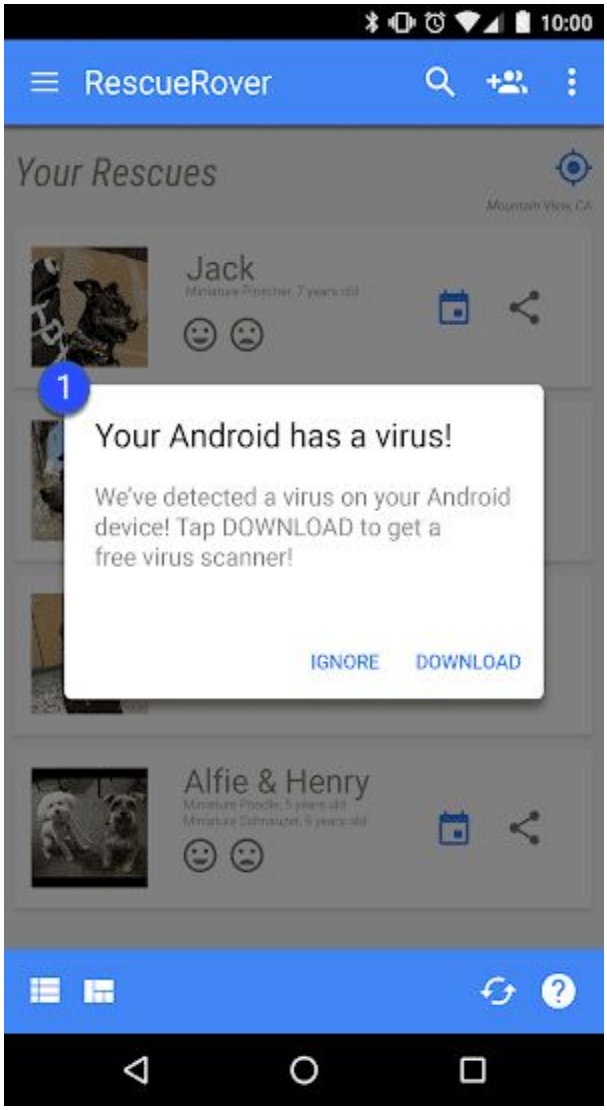
Gli annunci non devono simulare o imitare l'interfaccia utente di app, notifiche o avvisi di un sistema operativo. All'utente deve essere chiaro in quale app è pubblicato ogni annuncio.

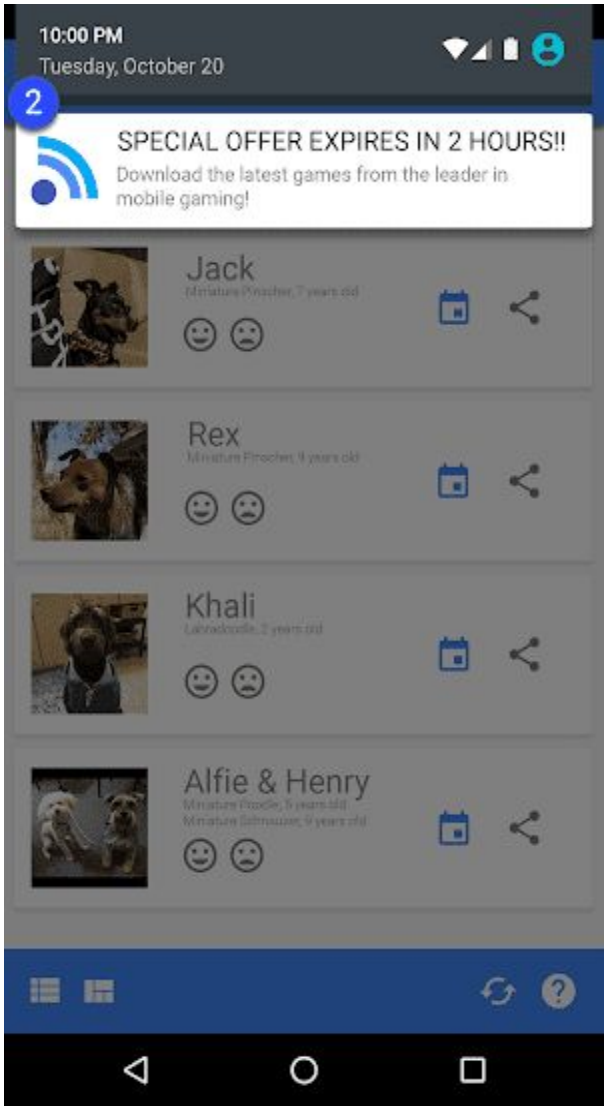
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Annunci che imitano l'interfaccia utente di un'app:



① L'icona a forma di punto interrogativo in questa app è un annuncio che rimanda l'utente a una pagina di destinazione esterna.
Annunci che imitano una notifica di sistema:





① ② Gli esempi in alto mostrano annunci che imitano diverse notifiche di sistema.

Monetizzazione della schermata di blocco

A meno che un'app non abbia esclusivamente la funzione di schermata di blocco, non devono esserci annunci o funzionalità che monetizzano la schermata di blocco di un dispositivo.

Annunci improvvisi

Gli annunci non devono essere mostrati in modo tale da causare clic involontari. È vietato obbligare l'utente a fare clic su un annuncio o a inviare informazioni personali per scopi pubblicitari come condizione per poter utilizzare la funzionalità completa di un'app.

Gli annunci interstitial possono essere mostrati solo all'interno dell'app in cui sono pubblicati. Se nell'app vengono mostrati annunci interstitial o altri annunci che interferiscono con il

normale utilizzo, gli utenti devono poter ignorare facilmente gli annunci senza essere penalizzati.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Annunci che occupano tutto lo schermo o che interferiscono con il normale utilizzo, che non è chiaro come poter ignorare:

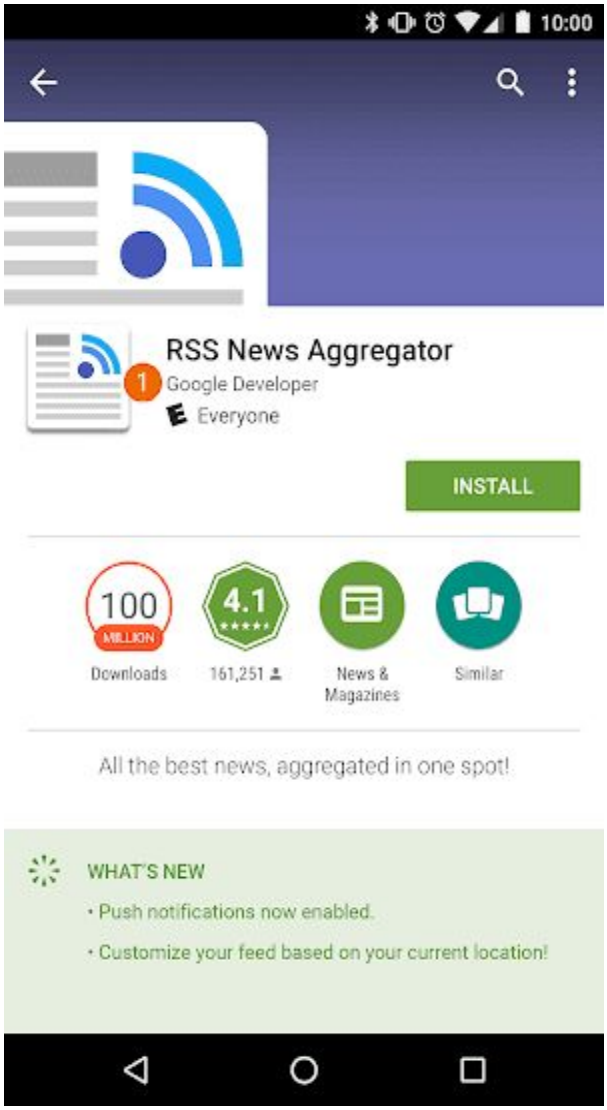
① Non è disponibile un pulsante per ignorare questo annuncio.

Interferenza con app, annunci di terze parti o funzionalità del dispositivo

Gli annunci associati all'app non devono interferire con altre app, altri annunci o con il funzionamento del dispositivo, inclusi pulsanti e porte del sistema o del dispositivo. Sono compresi overlay, funzionalità di supporto e unità pubblicitarie con widget. Gli annunci possono essere visualizzati soltanto all'interno dell'app in cui vengono pubblicati.

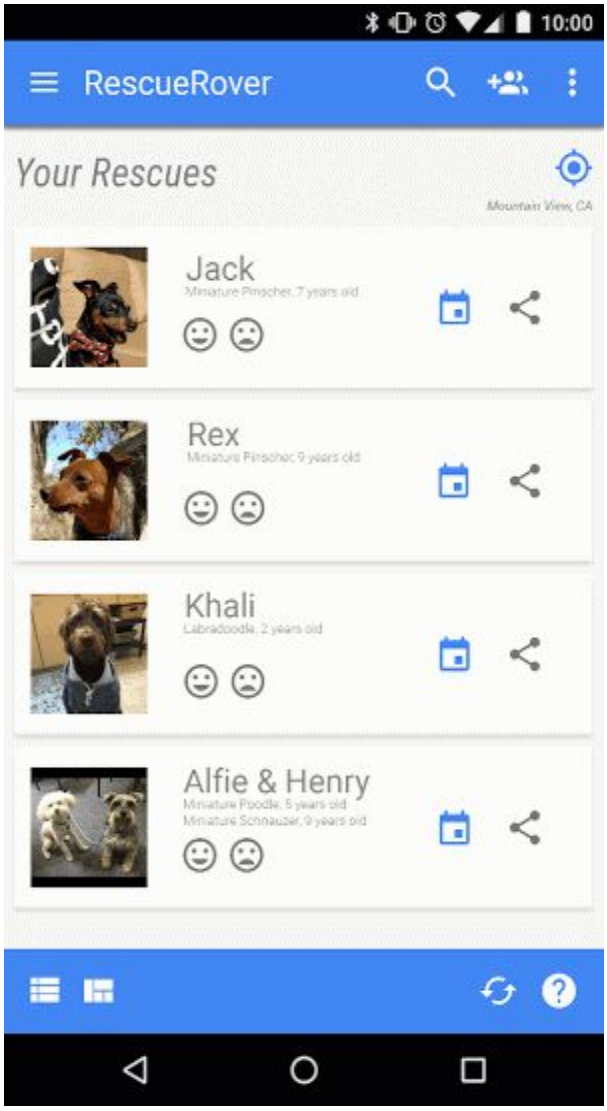
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Annunci che vengono mostrati all'esterno dell'app in cui sono pubblicati:



Descrizione. L'utente visita la schermata Home dell'app e compare all'improvviso un annuncio.

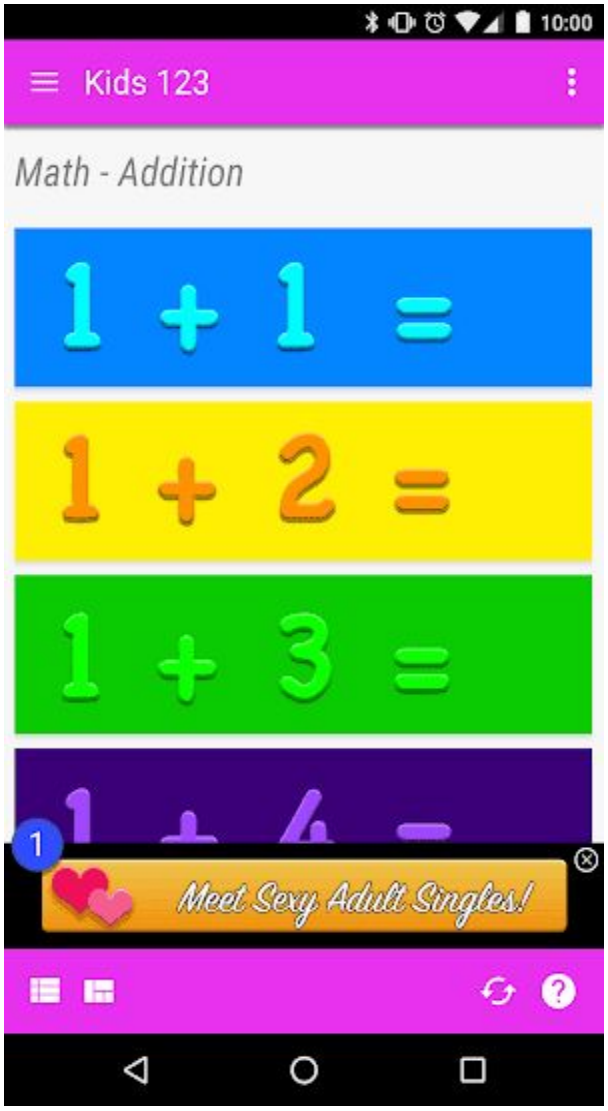
Annunci che vengono attivati dal pulsante Home o da altre funzioni ideate espressamente per uscire dall'app:



Descrizione: l'utente cerca di uscire dall'app e di accedere alla schermata Home, ma il flusso previsto viene interrotto da un annuncio.

Annunci inappropriati

Gli annunci mostrati nell'app devono essere adatti al pubblico previsto dell'app, a prescindere dalla conformità dei contenuti alle norme di Google.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.



① Questo annuncio non è adatto al pubblico previsto dell'app.

Utilizzo dell'ID pubblicità di Android

Nella versione 4.0 di Google Play Services sono state introdotte nuove API e un ID a disposizione dei fornitori di pubblicità e dati analitici. Di seguito sono riportati i termini per l'utilizzo dell'ID.

> Utilizzo. L'identificatore pubblicità di Android deve essere utilizzato soltanto per la pubblicità e l'analisi degli utenti. A ogni accesso dell'ID è necessario verificare lo stato dell'impostazione di disattivazione della pubblicità basata sugli interessi o della personalizzazione degli annunci.
> Associazione con informazioni personali o altri identificatori. L'identificatore pubblicità non deve essere collegato a informazioni che consentono l'identificazione personale o associato ad alcun identificatore del dispositivo persistente (ad esempio: SSAID, indirizzo MAC, IMEI e così via) senza l'esplicito consenso dell'utente.

Rispetto delle scelte degli utenti. In caso di reimpostazione, il nuovo identificatore pubblicità non deve essere collegato a un identificatore pubblicità precedente o a dati derivanti da un precedente identificatore pubblicità senza l'esplicito consenso dell'utente. È necessario inoltre rispettare l'impostazione di disattivazione della pubblicità basata sugli interessi o della personalizzazione degli annunci configurata dall'utente. Se un utente ha attivato questa impostazione, non è possibile utilizzare l'identificatore pubblicità per creare profili utente per scopi pubblicitari o per mostrare agli utenti pubblicità personalizzata. Sono ammesse, ad esempio, la pubblicità contestuale, l'impostazione di quote limite, il monitoraggio delle conversioni, i rapporti e il rilevamento di problemi di sicurezza e di attività fraudolente.
Trasparenza per gli utenti. La raccolta e l'utilizzo dell'identificatore pubblicità e l'impegno a rispettare i presenti termini devono essere comunicati agli utenti tramite un'Informativa sulla privacy legalmente adeguata. Per ulteriori informazioni sui nostri standard relativi alla privacy, leggere le norme relative ai Dati utente.
Rispetto dei termini e condizioni d'uso. L'identificatore pubblicità può essere utilizzato esclusivamente in conformità con i presenti termini, anche dalle eventuali parti con cui viene condiviso nel corso della propria attività. Per tutte le app caricate o pubblicate su Google Play è necessario utilizzare l'ID pubblicità (se disponibile sul dispositivo) anziché qualsiasi altro identificatore del dispositivo per qualunque finalità pubblicitaria.

Programma relativo agli annunci per la famiglia

Se nell'app vengono visualizzati annunci e il pubblico di destinazione dell'app medesima include unicamente bambini e ragazzi come descritto nelle Norme per le famiglie, è necessario utilizzare SDK di annunci che dispongono dell'autocertificazione di conformità con le norme di Google Play, inclusi i requisiti di certificazione per gli SDK di annunci indicati di seguito. Se il pubblico di destinazione dell'app è costituito da bambini e ragazzi e da utenti di età più elevata, è necessario implementare misure di controllo dell'età e assicurarsi che gli annunci mostrati a bambini e ragazzi provengano esclusivamente da uno degli SDK di annunci autocertificati. Per le app del programma Per la famiglia è necessario utilizzare soltanto SDK di annunci autocertificati.

L'uso di SDK di annunci certificati Google Play è richiesto soltanto se gli SDK di annunci sono utilizzati per mostrare annunci a bambini e ragazzi. Quanto indicato di seguito è consentito senza obbligo di autocertificazione degli SDK di annunci con Google Play, ma lo sviluppatore rimane responsabile di garantire che i contenuti degli annunci e le procedure di raccolta dei dati siano conformi alle Norme relative ai dati utente di Play e alle Norme per le famiglie:

Annunci autopromozionali quando gli SDK vengano utilizzati per gestire la promozione incrociata delle app dello sviluppatore o per altri contenuti multimediali di proprietà e merchandising
Stipulazione di direct deal con gli inserzionisti quando lo sviluppatore utilizzi SDK per la gestione dell'inventario

Requisiti di certificazione degli SDK di annunci

- Definire i contenuti degli annunci e i comportamenti discutibili e vietarli nei termini o nelle norme dell'SDK di annunci. Le definizioni non devono essere in contrasto con le Norme del programma per gli sviluppatori di Google Play.
- Creare un metodo per classificare le creatività degli annunci dello sviluppatore in base alle fasce d'età appropriate, incluse almeno le fasce Per tutti e Per adulti. La metodologia di classificazione deve essere in linea con la metodologia che Google fornisce agli SDK una volta che hanno compilato il modulo di interesse riportato di seguito.
- Consentire ai publisher, in base a singole richieste o in relazione a singole app, di richiedere il trattamento per siti o servizi destinati ai minori per la pubblicazione di annunci. Tale trattamento deve essere conforme alle leggi e ai regolamenti vigenti, come la normativa statunitense Children's Online Privacy and Protection Act (COPPA) e il Regolamento generale sulla protezione dei dati (GDPR) dell'UE. Nel contesto del trattamento per siti o servizi destinati ai minori, Google Play richiede inoltre la disattivazione degli annunci personalizzati, della pubblicità basata sugli interessi e del remarketing.
- Assicurare che, quando le offerte in tempo reale vengono utilizzate per mostrare annunci a bambini e ragazzi, le creatività siano state esaminate e gli indicatori relativi alla privacy vengano propagati agli offerenti.
- Fornire a Google informazioni sufficienti per verificare la conformità dell'SDK di annunci a tutti i requisiti di certificazione e rispondere tempestivamente a eventuali richieste successive di informazioni.

Nota: gli SDK di annunci devono supportare la pubblicazione di annunci conformi a tutte le leggi e i regolamenti pertinenti relativi a bambini e ragazzi che possano applicarsi ai rispettivi publisher.

Requisiti di mediazione delle piattaforme di pubblicazione di annunci destinati ai minori:

- Utilizzare solo SDK di annunci certificati Google Play o implementare le misure di protezione necessarie per garantire che tutti gli annunci pubblicati dalle reti di mediazione siano conformi a tali requisiti; e inoltre
- Riportare i segnali necessari per indicare la classificazione dei contenuti degli annunci e l'eventuale trattamento applicabile per siti o servizi destinati ai minori.

Gli sviluppatori possono consultare un elenco di SDK di annunci autocertificati qui.

Inoltre, gli sviluppatori possono condividere questo modulo di interesse con gli SDK di annunci per cui vorrebbero ottenere l'autocertificazione.

Scheda dello Store e promozione

La promozione e la visibilità delle app incidono notevolmente sulla qualità dello store. Evita schede dello store contenenti spam, promozioni di scarsa qualità e tentativi di aumentare in modo artificiale la visibilità delle app su Google Play.

Promozione di app

Sono vietate le app che beneficiano di o adottano, direttamente o indirettamente, pratiche di promozione ingannevoli o dannose per gli utenti o per l'ecosistema degli sviluppatori. Sono incluse le app che adottano il seguente comportamento:

- Utilizzo di annunci ingannevoli su siti web, app o altre proprietà, incluse notifiche simili ad avvisi e notifiche di sistema.
- Promozione o utilizzo di stratagemmi per reindirizzare gli utenti a Google Play o scaricare app senza l'azione consapevole dell'utente.
- Promozione non richiesta tramite servizi SMS.

È tua responsabilità assicurarti che tutte le reti pubblicitarie o affiliate associate alla tua app siano conformi alle presenti norme e non adottino pratiche di promozione vietate.

Metadati

Non sono ammesse app contenenti metadati fuorvianti, non correttamente formattati, non descrittivi, irrilevanti, eccessivi o inappropriati, neanche nella descrizione, nel nome sviluppatore, nel titolo, nell'icona, negli screenshot e nelle immagini promozionali dell'app. Gli sviluppatori sono tenuti a fornire una descrizione chiara e ben scritta. Inoltre nella descrizione dell'app non sono consentite testimonianze degli utenti anonime o non attribuite.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

① Testimonianze degli utenti anonime o non attribuite

② Confronti di dati di app o brand

③ Blocchi di parole ed elenchi di parole verticali oppure orizzontali

Di seguito sono riportati alcuni esempi di testo, immagini o video inappropriati presenti nella tua scheda:

Immagini o video con contenuti a sfondo sessuale. Evita di utilizzare immagini allusive che mostrino seni, natiche, genitali o altri contenuti/parti anatomiche oggetto di feticismo, sia illustrati sia reali.

Linguaggio non adatto a tutti. Evita di utilizzare un linguaggio scurrile e volgare nella scheda della tua app. Se è un elemento fondamentale della tua app, devi censurare la presentazione all'interno della scheda dello Store.

- Violenza esplicita mostrata in primo piano nelle icone delle app, nelle immagini promozionali o nei video.
- Raffigurazioni dell'utilizzo illegale di droghe. Anche i contenuti a scopo didattico, documentaristico, scientifico o artistico devono essere adatti a tutti i tipi di pubblico all'interno della scheda dello Store.

Di seguito sono riportate alcune best practice:

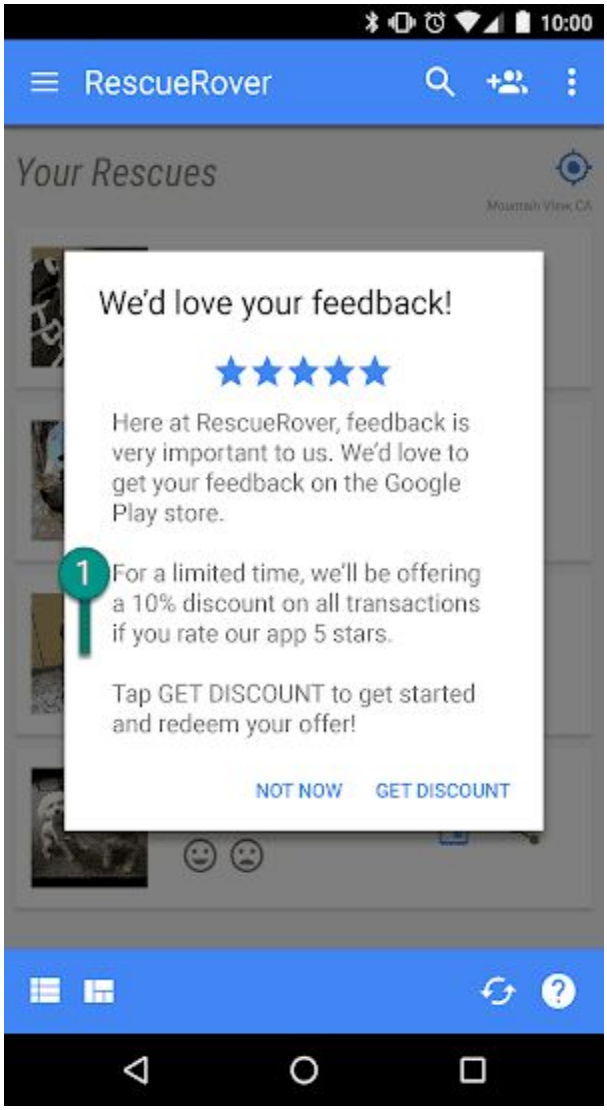
- Evidenzia gli aspetti migliori della tua app. Condividi con gli utenti fatti interessanti e coinvolgenti relativi alla tua app per aiutarli a capire che cosa la rende speciale.
- Assicurati che il titolo e la descrizione dell'app illustrino in modo accurato la funzionalità dell'app.
- Evita di utilizzare parole chiave o riferimenti ripetitivi o estranei al contesto.
- La descrizione dell'app deve essere breve e diretta. Le descrizioni brevi tendenzialmente offrono un'esperienza utente migliore, in particolare sui dispositivi con schermi piccoli. La ripetizione, la lunghezza, la formattazione non valida o i dettagli eccessivi potrebbero costituire una violazione di queste norme.
- Tieni presente che la tua scheda deve essere adatta a tutti. Evita di utilizzare testo, immagini o video inappropriati nella scheda e attieniti alle linee guida riportate in precedenza.

Valutazioni, recensioni e installazioni degli utenti

Gli sviluppatori non devono tentare di manipolare il posizionamento di qualsiasi app su Google Play. È vietato quindi, a titolo esemplificativo, gonfiare le valutazioni dei prodotti, le recensioni o il numero di installazioni con mezzi illeciti, ad esempio tramite installazioni, recensioni e valutazioni fraudolente o basate sull'offerta di incentivi.

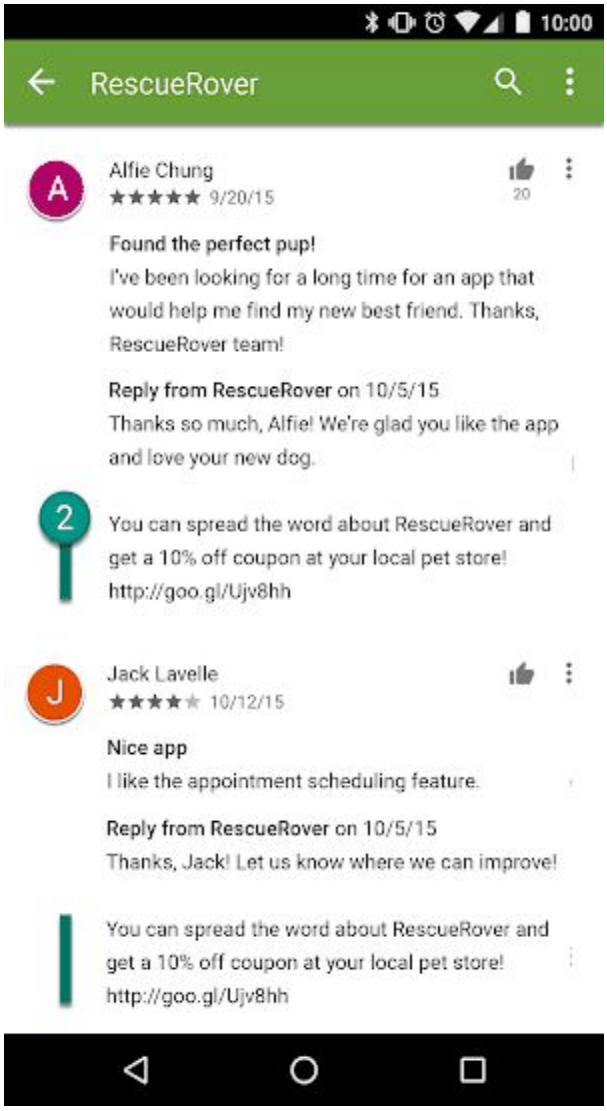
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Chiedere agli utenti di valutare l'app offrendo un incentivo:



① Questa notifica offre agli utenti uno sconto in cambio di una valutazione elevata.

Invio a ripetizione di valutazioni per influenzare il posizionamento dell'app su Google Play.
Invio di o esortazione degli utenti a inviare recensioni con contenuti inappropriati, inclusi coupon, affiliazioni, codici di gioco, indirizzi email o link che rimandano a siti web o altre app:



② Questa recensione esorta gli utenti a promuovere l'app RescueRover offrendo in cambio un coupon.

Le valutazioni e le recensioni sono parametri di qualità delle app, che gli utenti considerano autentici e pertinenti. Di seguito sono riportate alcune best practice da seguire per rispondere alle recensioni degli utenti:

Mantieni la risposta incentrata sui problemi sollevati nei commenti dell'utente e non richiedere una valutazione più alta.
Includi riferimenti a risorse utili, ad esempio un indirizzo di supporto o una pagina di domande frequenti.

Classificazioni dei contenuti

Il nostro sistema di classificazione dei contenuti include le classificazioni ufficiali dell'International Age Rating Coalition (IARC) ed è concepito per aiutare gli sviluppatori a comunicare agli utenti le classificazioni dei contenuti pertinenti a livello locale.

Modalità di utilizzo delle classificazioni dei contenuti

Le classificazioni dei contenuti vengono utilizzate per informare i consumatori, specialmente i genitori, riguardo ai contenuti potenzialmente discutibili presenti in un'app. Consentono inoltre di filtrare o bloccare i contenuti in determinati territori o per utenti specifici ove previsto dalla legge e determinare l'idoneità dell'app a programmi speciali per sviluppatori.

Modalità di assegnazione delle classificazioni dei contenuti

Per ricevere la classificazione dei contenuti, è necessario compilare un questionario per la classificazione in Play Console con domande sulla natura dei contenuti delle app. In base alle risposte al questionario, a ogni app verrà assegnata una classificazione dei contenuti da parte di più autorità di classificazione. La rappresentazione ingannevole dei contenuti delle app potrebbe comportarne la rimozione o la sospensione, perciò è importante dare risposte precise alle domande del questionario relativo alla classificazione dei contenuti.

Per evitare che un'app venga elencata come "Non classificata", è necessario compilare il questionario per la classificazione dei contenuti per ogni nuova app inviata alla Play Console e per tutte le app esistenti che sono attive su Google Play. Le app sprovviste di una classificazione dei contenuti verranno rimosse dal Play Store.

Se i contenuti o le funzionalità dell'app vengono modificati in modo tale da influire sulle risposte al questionario di classificazione, è necessario inviare un nuovo questionario relativo alla classificazione dei contenuti all'interno di Play Console.

Visita il Centro assistenza per ulteriori informazioni sulle varie autorità di classificazione e su come completare il questionario relativo alla classificazione dei contenuti.

Ricorsi contro le classificazioni

Se non sei d'accordo con la classificazione assegnata alla tua app, puoi presentare un ricorso direttamente all'autorità di classificazione dell'IARC utilizzando il link disponibile nel certificato inviato via email.

Spam e funzionalità minima

Le app devono fornire agli utenti almeno un livello di funzionalità di base e un'esperienza utente accettabile. Le app che si bloccano, presentano altri comportamenti non coerenti con un'esperienza utente funzionale o che servono solo per mandare spam agli utenti o a Google Play non sono considerate app che ampliano il catalogo in modo costruttivo.

Spam

Sono vietate le app che inviano spam agli utenti o inseriscono spam su Google Play, ad esempio le app che inviano messaggi indesiderati agli utenti oppure le app duplicate o di scarsa qualità.

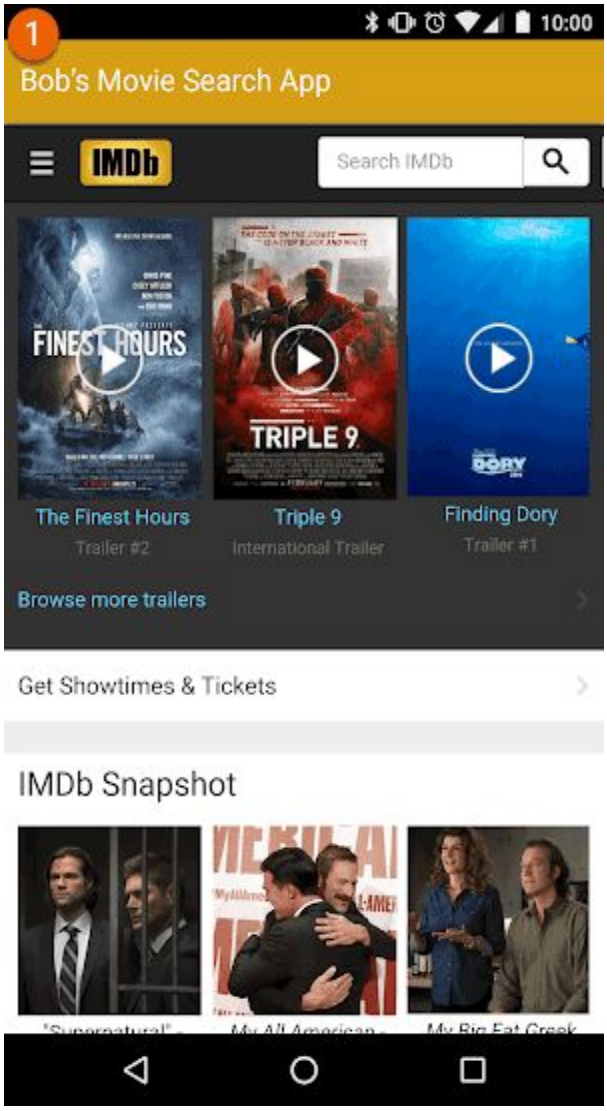
Spam nei messaggi

Sono vietate le app che inviano SMS, email o altri messaggi per conto dell'utente senza offrire a quest'ultimo la possibilità di verificare i contenuti e i destinatari previsti.

Spam legato alle visualizzazioni web e per promuovere traffico affiliato

Sono vietate le app il cui scopo principale è indirizzare traffico affiliato verso un sito web o fornire una visualizzazione web di un sito senza l'autorizzazione del proprietario o dell'amministratore del sito stesso.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

> Un'app il cui scopo principale è indirizzare il traffico dai referral verso un sito web al fine di ricevere crediti per le registrazioni o gli acquisti degli utenti sul sito in questione.
> App il cui scopo principale è fornire una visualizzazione web di un sito web senza autorizzazione:



① Questa app è denominata "Bob's Movie Search App" e fornisce semplicemente una visualizzazione web di IMDb.

Contenuti ripetitivi

Sono vietate le app che forniscono semplicemente la stessa esperienza di altre app già presenti su Google Play. Le app dovrebbero essere utili per gli utenti e quindi fornire servizi o contenuti unici.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

La copia di contenuti di altre app senza aggiungere alcun contenuto originale o alcuna utilità.

La creazione di diverse app con funzionalità, contenuti ed esperienze utente molto simili. Se il volume di contenuti di ogni singola app è ridotto, gli sviluppatori potrebbero creare un'unica app che raccolga tutti i contenuti.

Sono vietate le app create tramite uno strumento automatizzato o un servizio di procedure guidate oppure basate su modelli e inviate a Google Play dall'operatore di tale servizio per conto di altre persone. Tali app sono ammesse soltanto se vengono pubblicate da un account sviluppatore registrato individualmente e appartenente all'utente dello strumento automatizzato, non all'operatore del servizio.

App realizzate appositamente per gli annunci

Sono vietate le app il cui scopo principale è pubblicare annunci.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

Le app in cui vengono inseriti annunci interstitial dopo ogni azione dell'utente inclusi, a titolo esemplificativo, clic, scorrimenti e così via.

Funzionalità minima

Assicurati che la tua app fornisca un'esperienza utente stabile, coinvolgente e reattiva.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App progettate per non fare nulla o per non avere alcuna funzione

Funzioni inaccessibili

Sono vietate le app che si arrestano in modo anomalo, chiedono di forzare la chiusura, si bloccano o funzionano in maniera anomala.
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App che non si installano
App che si installano, ma non si caricano
App che si caricano, ma non sono reattive

Altri programmi

Oltre a dover essere conformi alle norme relative ai contenuti stabilite altrove nel presente Centro norme, le app ideate per altre esperienze Android e distribuite tramite Google Play potrebbero anche essere soggette a requisiti relativi alle norme specifici del programma. Assicurati di leggere l'elenco che segue per stabilire se ci sono delle norme che si applicano alla tua app.

App istantanee Android

Abbiamo realizzato le app istantanee Android con lo scopo di offrire agli utenti esperienze piacevoli e semplicissime rispettando allo stesso tempo gli standard più elevati di privacy e sicurezza. Le nostre norme sono state pensate a sostegno di tale scopo.

Gli sviluppatori che scelgono di distribuire app istantanee Android tramite Google Play devono rispettare le norme che seguono, oltre a tutte le altre Norme del programma di Google Play per gli sviluppatori.

Identità

Gli sviluppatori di app istantanee con funzionalità di accesso devono integrare la funzione Smart Lock per password.

Supporto dei link

Gli sviluppatori di app istantanee Android sono tenuti a supportare correttamente i link relativi ad altre app. Se le app installate o le app istantanee dello sviluppatore contengono link che potrebbero rimandare a un'app istantanea, lo sviluppatore deve indirizzare gli utenti a tale app anziché, ad esempio, mostrare i link in un componente WebView.

Specifiche tecniche

Gli sviluppatori devono rispettare le specifiche tecniche e i requisiti relativi alle app istantanee Android (che potrebbero essere occasionalmente modificati) indicati da Google, inclusi quelli riportati nella nostra documentazione pubblica.

Offerta dell'installazione di app

L'app istantanea potrebbe offrire all'utente l'app installabile, ma questo non deve essere lo scopo principale dell'app istantanea. Se offre l'installazione, gli sviluppatori sono tenuti a:

- Usare l'icona "get app" (scarica l'app) di Material Design e l'etichetta "Installa" per il pulsante di installazione.
- Non avere più di due o tre richieste di installazione implicite nell'app istantanea.

Non usare un banner o un'altra tecnica in stile pubblicitario per presentare una richiesta di installazione agli utenti.

Ulteriori dettagli sulle app istantanee e linee guida relative all'esperienza utente sono disponibili nella pagina contenente le best practice per l'esperienza utente.

Modifica dello stato del dispositivo

Le app istantanee non devono apportare al dispositivo dell'utente modifiche che permangano più a lungo della sessione con l'app istantanea. Ad esempio, le app istantanee non possono cambiare lo sfondo dell'utente o creare un widget nella schermata Home.

Visibilità delle app

Gli sviluppatori devono assicurarsi che le app istantanee siano visibili all'utente in modo che quest'ultimo sia sempre a conoscenza dell'esecuzione dell'app sul proprio dispositivo.

Identificatori dei dispositivi

Le app istantanee non sono autorizzate ad accedere agli identificatori dei dispositivi che (1) persistono dopo l'interruzione dell'esecuzione dell'app istantanea e (2) non sono reimpostabili dall'utente. Di seguito sono riportati alcuni esempi:

Numero di serie della build
Indirizzi MAC di chip di rete
IMEI, IMSI

Le app istantanee potrebbero accedere al numero di telefono se ottenuto usando l'autorizzazione relativa al tempo di esecuzione. Lo sviluppatore non deve cercare di identificare l'utente usando questi identificatori o qualsiasi altro mezzo.

Traffico di rete

Il traffico di rete dall'interno dell'app istantanea deve essere criptato usando un protocollo TLS come HTTPS.

Famiglie

Google Play offre agli sviluppatori una piattaforma completa per mostrare contenuti di alta qualità, adatti alle specifiche fasce d'età e idonei per tutta la famiglia. Prima di inviare un'app per il programma Per la famiglia o presentare un'app destinata ai bambini sul Google Play Store,

hai la responsabilità di assicurarti che l'app sia adatta ai bambini e conforme a tutte le leggi vigenti.

Leggi informazioni sui requisiti del programma e delle Norme per le famiglie e consulta l'elenco di controllo interattivo sul portale Academy for App Success.

Progettare app per bambini e famiglie

L'uso della tecnologia come strumento per arricchire la vita delle famiglie continua a crescere e i genitori sono sempre alla ricerca di contenuti sicuri e di alta qualità da condividere con i propri figli. Le tue app possono essere progettate appositamente per i bambini oppure potrebbero comunque attirare la loro attenzione. Google Play ti aiuterà a garantire che la tua app sia sicura per tutti gli utenti, comprese le famiglie.

Il termine "bambino" può assumere significati diversi a seconda dei paesi e dei contesti. È importante rivolgersi a un consulente legale che aiuti a determinare gli eventuali obblighi e/o le restrizioni in base alle fasce d'età applicabili alla tua app. Dato che tu sai meglio di chiunque come funziona la tua app, ci affidiamo a te per garantire che le app disponibili su Google Play siano sicure per le famiglie.

Le app progettate specificatamente per i bambini devono partecipare al programma Per la famiglia. Tuttavia, se la tua app si rivolge sia ai bambini sia ad altri segmenti di pubblico, partecipare al programma Per la famiglia è comunque un ottimo modo per farla conoscere agli utenti appropriati. Se decidi di non partecipare al programma Per la famiglia, devi comunque rispettare i requisiti delle Norme per le famiglie di Google Play riportati di seguito, così come tutte le altre Norme del programma per gli sviluppatori di Google Play e il Contratto di distribuzione per gli sviluppatori.

Requisiti di Play Console

Pubblico di destinazione e contenuti

Nella sezione Pubblico di destinazione e contenuti di Google Play Console, devi indicare il pubblico di destinazione della tua app, prima della pubblicazione, selezionandolo dall'elenco delle fasce d'età fornite. Indipendentemente dalla tua selezione in Google Play Console, qualora tu scelga di includere nella tua app immagini e termini che potrebbero essere considerati come destinati ai bambini, ciò potrà influire sulla valutazione di Google Play in merito al pubblico di destinazione dichiarato. Google Play si riserva il diritto di rivedere le informazioni sull'app fornite per determinare se il pubblico di destinazione indicato sia corretto.

Nel caso in cui selezioni un pubblico di destinazione che include solo gli adulti, ma Google ritenga tale indicazione non corretta perché l'app ha come target anche i bambini, avrai la possibilità di chiarire agli utenti che la tua app non è destinata ai bambini accettando di mostrare un'etichetta di avviso.

Ti invitiamo a selezionare più fasce di età per il pubblico di destinazione della tua app soltanto se l'hai progettata, e sei certo che sia idonea, per gli utenti inclusi nelle fasce di età selezionate. Ad esempio, per le app progettate per i bambini di età compresa fra 1 e 5 anni e di età inferiore è necessario selezionare "Fino a 5 anni". Se la tua app è progettata per uno specifico livello di istruzione, scegli la fascia d'età che lo definisce meglio. Seleziona le fasce d'età che includono sia adulti che bambini soltanto se hai ideato la tua app per utenti di tutte le età.

Aggiornamenti alla sezione Pubblico di destinazione e contenuti

Puoi sempre aggiornare le informazioni relative alla tua app nella sezione Pubblico di destinazione e contenuti di Google Play Console. È necessario un aggiornamento dell'app prima che tali informazioni siano riportate nel Google Play Store. Tuttavia, eventuali modifiche apportate in questa sezione di Google Play Console potranno essere esaminate per verificarne la conformità alle norme anche prima di inviare un aggiornamento dell'app.

Ti consigliamo vivamente di comunicare ai tuoi utenti eventuali modifiche della fascia d'età scelta come target per la tua app o l'inserimento di annunci o acquisti in-app, utilizzando la sezione "Novità" della pagina relativa alla scheda dello Store della tua app o tramite notifiche in-app.

Rappresentazioni ingannevoli in Play Console

La rappresentazione ingannevole di qualsiasi informazione inerente la tua app in Play Console, inclusa la sezione Pubblico di destinazione e contenuti, potrebbe comportare la rimozione o la sospensione dell'app, perciò è importante fornire informazioni precise.

Requisiti delle Norme per le famiglie

Se il pubblico di destinazione della tua app include i bambini, devi soddisfare i requisiti seguenti. Il mancato rispetto di tali requisiti può comportare la rimozione o sospensione dell'app.

1. Contenuti delle app: i contenuti delle app accessibili ai bambini devono essere adeguati per questi ultimi.
2. Risposte di Google Play Console: lo sviluppatore è tenuto a rispondere con precisione alle domande contenute in Google Play Console relative alla sua app e ad aggiornare tali risposte per riflettere con precisione qualsiasi modifica apportata all'app.
3. Annunci: se la tua app visualizza annunci per bambini o utenti di età sconosciuta, devi:
   utilizzare solo SDK di annunci certificati Google Play per mostrare annunci a tali utenti;
   assicurarti che gli annunci mostrati a tali utenti non prevedano pubblicità basata sugli interessi o remarketing;
   garantire che gli annunci mostrati a tali utenti presentino contenuti appropriati per i bambini;
   garantire che gli annunci mostrati a tali utenti rispettino i requisiti relativi al formato degli annunci per le famiglie; infine

assicurare la conformità a tutte le normative legali e gli standard di settore applicabili in materia di pubblicità destinata ai bambini.

4. Raccolta dati: lo sviluppatore è tenuto a divulgare la raccolta di eventuali dati personali e sensibili relativi a bambini e ragazzi nell'app, compresa la raccolta tramite API e SDK richiamati o utilizzati nell'app medesima. I dati sensibili relativi a bambini e ragazzi includono, a titolo esemplificativo ma non esaustivo, le informazioni di autenticazione, i dati dei sensori della videocamera e del microfono, i dati del dispositivo, l'ID Android, i dati sull'utilizzo degli annunci e l'ID pubblicità.
5. API e SDK: lo sviluppatore deve assicurare che l'app implementi correttamente eventuali API e SDK.
    Le app destinate esclusivamente ai bambini non devono contenere API o SDK non approvati per l'utilizzo in servizi rivolti ai minori. Ciò include il servizio Accedi con Google (o qualsiasi altro servizio API di Google che acceda ai dati associati a un Account Google), i servizi per i giochi di Google Play e qualsiasi altro servizio API che utilizzi la tecnologia OAuth per l'autenticazione e l'autorizzazione.
    Le app destinate sia a bambini e ragazzi sia a un pubblico di età più elevata non devono implementare API o SDK non approvati per l'utilizzo nei servizi rivolti ai minori, a meno che non vengano utilizzati dietro un filtro di controllo dell'età o implementati in un modo che non comporti la raccolta di dati da bambini e ragazzi (ad esempio, fornendo il servizio Accedi con Google come funzionalità facoltativa). Ricorda che tutti gli utenti devono poter accedere alla tua app e a una ragionevole gamma delle sue funzionalità.
6. Norme sulla privacy: lo sviluppatore deve fornire un link alle norme sulla privacy dell'app nella pagina della scheda dello Store dell'app medesima. Questo link deve essere mantenuto sempre attivo nel periodo di disponibilità dell'app sullo Store e deve reindirizzare a norme sulla privacy che, tra le altre cose, descrivano accuratamente la raccolta e l'utilizzo dei dati da parte dell'app.
7. Limitazioni speciali:
    Se la tua app utilizza la realtà aumentata, dovrai includere un avviso di sicurezza che venga visualizzato immediatamente all'avvio della sezione AR. L'avviso dovrà contenere quanto segue:
        Un messaggio appropriato relativo all'importanza della supervisione dei genitori.
        Un promemoria che ricordi i rischi fisici nella realtà (ad esempio indicando all'utente di prestare attenzione a ciò che lo circonda).
    La tua app non deve richiedere l'utilizzo di dispositivi sconsigliati per l'uso da parte dei bambini (ad esempio Daydream, Oculus).
8. Conformità legale: lo sviluppatore deve assicurare che l'app, compresi API o SDK richiamati o utilizzati, sia conforme alla normativa statunitense Children's Online Privacy and Protection Act (COPPA), al Regolamento generale sulla protezione dei dati (GDPR) dell'UE e a eventuali altre leggi o regolamenti vigenti.

Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

App che promuovono giochi per bambini nella scheda dello Store, ma il cui contenuto è appropriato solo per un pubblico adulto.
App che implementano API con termini di servizio che ne vietano l'utilizzo in app rivolte ai minori.
App che promuovono un'immagine positiva dell'uso di alcol, tabacco o sostanze controllate.
App che includono giochi e scommesse reali o simulati.
App con violenza, spargimenti di sangue e contenuti scioccanti non adatti ai bambini.
App che offrono servizi di incontri oppure consulenza sessuale o matrimoniale.
App che mostrano ai bambini annunci destinati a un pubblico adulto.

Programma Per la famiglia

Le app progettate specificatamente per i bambini devono partecipare al programma Per la famiglia. Se la tua app è progettata per tutti, compresi bambini e famiglie, anche tu puoi presentare domanda per partecipare al programma.

Per poter essere accettata nel programma, l'app deve essere conforme a tutti i requisiti delle Norme per le famiglie e a tutti i requisiti di idoneità del programma Per la famiglia, oltre a quelli indicati nelle Norme del programma per gli sviluppatori di Google Play e nel Contratto di distribuzione per gli sviluppatori.

Per ulteriori informazioni sulla procedura per l'invio dell'app per l'inclusione nel programma, fai clic qui.

Idoneità al programma

I contenuti delle app che partecipano al programma Per la famiglia, compresi i contenuti degli annunci, devono essere pertinenti e adatti ai bambini e soddisfare tutti i requisiti riportati di seguito. Le app accettate per la partecipazione al programma Per la famiglia devono garantire la conformità costante a tutti i requisiti del programma. Google Play si riserva il diritto di rifiutare o rimuovere, a sua discrezione esclusiva, le app ritenute non appropriate al programma Per la famiglia.

Requisiti del programma Per la famiglia

1. Le app devono avere la classificazione ESRB Per tutti, Per tutti 10+ o altra classificazione equivalente.
2. È necessario divulgare accuratamente gli elementi interattivi dell'app nel questionario di classificazione dei contenuti in Google Play Console, incluso quanto segue:
    se gli utenti possono interagire o scambiarsi informazioni;
    se le informazioni personali fornite dagli utenti vengono condivise con terze parti; e inoltre

se la posizione fisica dell'utente viene condivisa con altri utenti.

3. Se l'app utilizza l'API Android Speech, il parametro RecognizerIntent.EXTRA_CALLING_PACKAGE dell'app deve essere impostato sul relativo PackageName.
4. Le app devono utilizzare soltanto SDK di annunci certificati Google Play.
5. Le app progettate specificamente per i bambini non possono richiedere autorizzazioni di accesso alla posizione.
6. Le app devono utilizzare la Gestione dispositivi companion (CDM) quando richiedono il Bluetooth, a meno che l'app non sia destinata solo a versioni di sistema operativo dei dispositivi non compatibili con CDM.

Di seguito sono riportati alcuni esempi di app comuni non idonee per il programma:

App con classificazione ESRB Per tutti, ma con annunci relativi a contenuti di giochi e scommesse
App per genitori o tutori (ad esempio tracker per l'allattamento al seno o guide allo sviluppo)
Guide per i genitori o app di gestione dei dispositivi destinate esclusivamente a genitori o tutori

Categorie

Se lo sviluppatore viene ammesso a partecipare al programma Per la famiglia potrà scegliere una seconda categoria specifica per il programma che descriva l'app. Di seguito vengono indicate le categorie disponibili per le app che partecipano al programma Per la famiglia:

Azione e avventura: app/giochi orientati all'azione che comprendono una grande varietà di contenuti, dai giochi di gare automobilistiche ad avventure fantastiche, ad altre app e giochi progettati per coinvolgere l'utente.

Giochi di logica: giochi che stimolano la riflessione, tra cui rompicapo, abbinamenti, quiz e altri giochi che mettono alla prova la memoria, l'intelligenza o la logica.

Creatività: app e giochi che stimolano la creatività, tra cui app di disegno o pittura, app di codifica e altre app e giochi di tipo creativo.

Istruzione: app e giochi progettati con il contributo di esperti dell'apprendimento (ad esempio, educatori, specialisti dell'apprendimento, ricercatori) per promuovere l'apprendimento, ad esempio accademico, socio-emotivo, fisico e creativo, così come relativo a capacità di base, al pensiero critico e al problem solving.

Musica e video: app e giochi con una componente musicale o video, dalle app di simulazione di strumenti a quelle che offrono contenuti video e audio musicali.

Giochi di ruolo: app e giochi in cui l'utente può interpretare un ruolo, ad esempio fingendo di essere un cuoco o cuoca, un infermiere o infermiera, un principe o principessa, un vigile o vigilessa del fuoco, un poliziotto o poliziotta o un personaggio immaginario.

Annunci e monetizzazione

Le norme riportate di seguito si applicano a qualsiasi annuncio (incluso per le tue app e per le app di terze parti), qualsiasi offerta di acquisto in-app o qualsiasi altro contenuto commerciale (come il posizionamento di prodotti a pagamento) offerto agli utenti di app soggette alle norme sulle famiglie e/o agli obblighi del programma Per la famiglia. Tutti gli annunci, le offerte di acquisto in-app e i contenuti commerciali presenti in queste app devono essere conformi alle leggi e normative applicabili (incluse eventuali indicazioni del settore o di autoregolamentazione pertinenti).

Google Play si riserva il diritto di agire in merito alle app in caso di tattiche commerciali eccessivamente aggressive.

Requisiti relativi al formato degli annunci

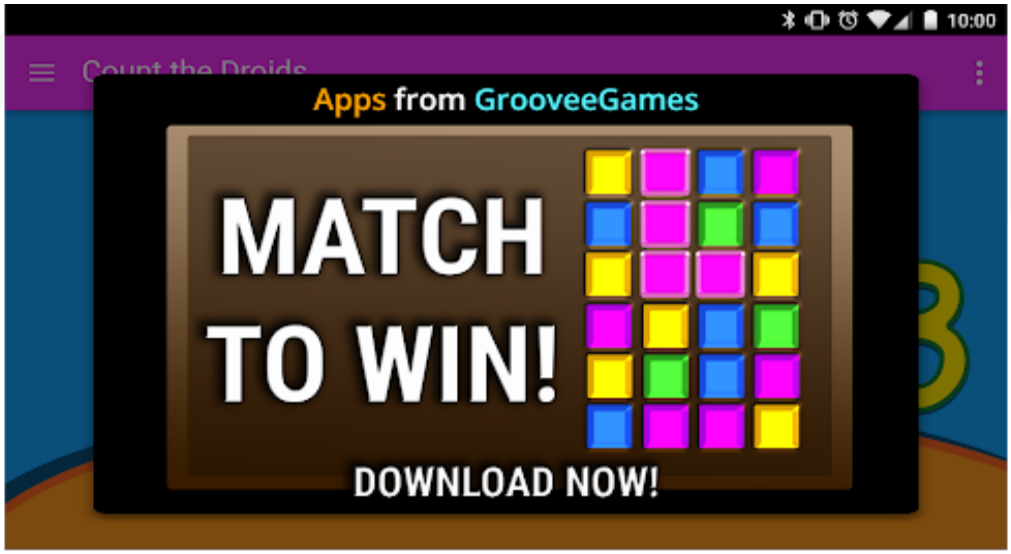
Gli annunci e le offerte di acquisto in-app non devono avere contenuti ingannevoli o essere strutturati in modo da determinare clic involontari da parte di utenti che sono bambini o ragazzi. Sono vietati:

- Uso di Barriere di annunci
- Annunci che interferiscono con il normale utilizzo dell'app e che non possono essere chiusi dopo 5 secondi
- Offerte o annunci interstitial per l'acquisto in-app visualizzati immediatamente all'avvio dell'app
- Posizionamenti di annunci multipli sulla stessa pagina
- Annunci e offerte per acquisti in-app che non siano chiaramente distinguibili dal contenuto dell'app
- Uso di tattiche emotivamente manipolative o scioccanti per incoraggiare la visualizzazione di annunci o gli acquisti in-app
- La mancata distinzione tra l'uso di monete di giochi virtuali rispetto a soldi reali per fare acquisti in-app

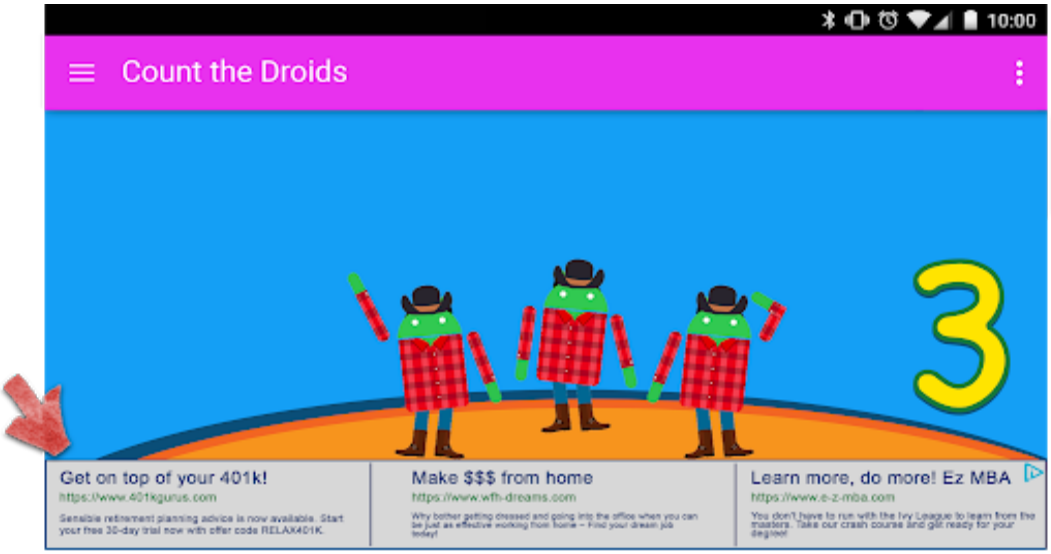
Per garantire che Google Play rimanga una piattaforma sicura e rispettosa, abbiamo creato degli standard che definiscono e proibiscono i contenuti dannosi o inappropriati per i nostri utenti.

- Annunci che si allontanano dal dito dell'utente mentre questi tenta di chiuderli

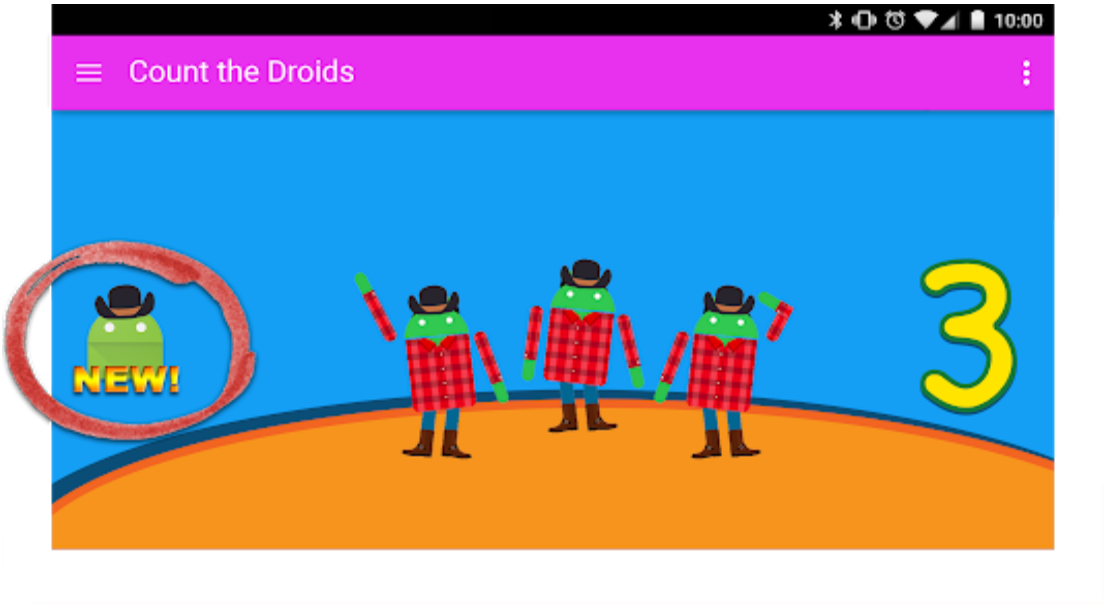
Annunci che occupano quasi tutto lo schermo del dispositivo senza fornire all'utente un modo chiaro per chiuderli, come illustrato nell'esempio seguente:



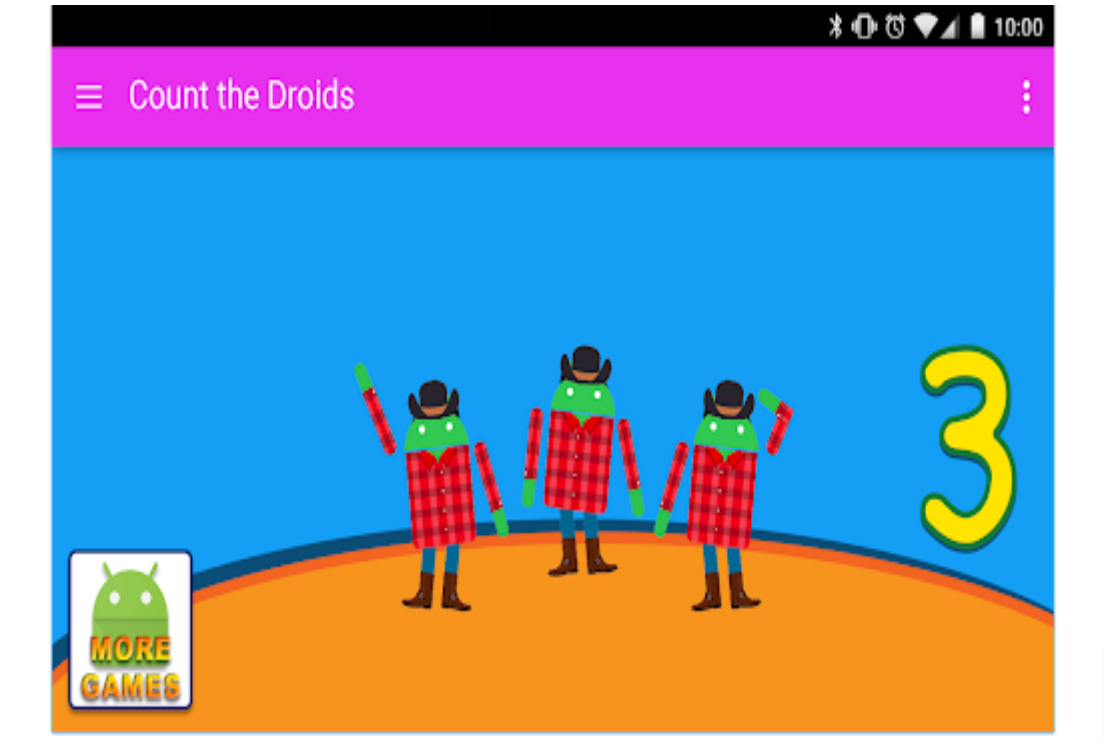
Annunci banner che mostrano più offerte, come illustrato nell'esempio seguente:



Annunci che l'utente potrebbe scambiare per contenuti dell'app, come illustrato nell'esempio seguente:



Pulsanti o annunci che promuovono le altre schede dello Store dello sviluppatore in Google Play Store, ma che non sono distinguibili dai contenuti delle app, come illustrato nell'esempio seguente:



Di seguito sono riportati alcuni esempi di contenuti pubblicitari inappropriati che non dovrebbero essere mostrati ai bambini.

- Contenuti multimediali inappropriati: annunci relativi a programmi TV, film, album musicali o altri mezzi di informazione non adatti a bambini e ragazzi.
- Videogiochi e software scaricabile inappropriati: annunci relativi a software scaricabile e videogiochi non adatti a bambini e ragazzi.
- Sostanze controllate o nocive: annunci relativi ad alcol, tabacco, sostanze controllate o altre sostanze nocive.
- Giochi e scommesse: annunci relativi a simulazioni di giochi e scommesse, promozioni di concorsi e lotterie (anche se la partecipazione è gratuita).
- Contenuti per adulti e a sfondo sessuale: annunci con contenuti sessuali, sessualmente allusivi e inappropriati per i minori.
- Incontri o relazioni: annunci relativi a siti di incontri o relazioni per adulti.
- Contenuti violenti: annunci con contenuti violenti ed espliciti non adatti a bambini e ragazzi.

SDK di annunci

Per pubblicare annunci per bambini e ragazzi possono essere utilizzati soltanto SDK di annunci certificati Google Play. Per le app del programma Per la famiglia è necessario utilizzare soltanto SDK di annunci certificati Google Play. Per le app destinate anche a utenti adulti, è possibile utilizzare SDK di annunci non certificati se nell'app è presente un filtro di controllo dell'età ed eventuali SDK di annunci non certificati vengono utilizzati solo per mostrare annunci a utenti sicuramente adulti.

Consultare la pagina Norme del Programma relativo agli annunci per la famiglia per maggiori dettagli su questi requisiti e per consultare l'elenco aggiornato degli SDK di annunci approvati.

Se si utilizza AdMob, fare riferimento al Centro assistenza AdMob per ulteriori informazioni sui prodotti.

È tua responsabilità garantire che la tua app soddisfi tutti i requisiti relativi a pubblicità, acquisti in-app e contenuti commerciali. Contattare il fornitore o i fornitori degli SDK di annunci per ulteriori informazioni sulle norme relative ai contenuti e sulle prassi pubblicitarie da loro applicate.

Acquisti in-app

Per le app che partecipano al programma Per la famiglia, Google Play esegue nuovamente l'autenticazione di tutti gli utenti prima di qualsiasi acquisto in-app. Questa misura serve ad assicurare che gli acquisti vengano effettuati dalla parte finanziariamente responsabile e non da bambini.

Applicazione

Evitare le violazioni delle norme è sempre meglio che doverle gestire ma, qualora si verifichino, ci impegniamo ad assicurare che gli sviluppatori sappiano come rendere conformi le loro app. Ti invitiamo a comunicarci eventuali violazioni riscontrate o a porci eventuali domande sulla gestione delle violazioni.

Copertura delle norme

Le nostre norme si applicano a qualsiasi contenuto mostrato o reso disponibile dall'app tramite link, compresi eventuali annunci mostrati agli utenti ed eventuali contenuti generati dagli utenti che siano ospitati o resi disponibili dall'app tramite link. Si applicano, inoltre, a qualsiasi contenuto dell'account sviluppatore mostrato pubblicamente su Google Play, inclusi il nome dello sviluppatore e la pagina di destinazione del sito web dello sviluppatore indicato.

Sono vietate le app che consentono agli utenti di installare altre app sui propri dispositivi. Le app che forniscono accesso ad altre app, giochi o software senza installazione, incluse le funzionalità e le esperienze offerte da terze parti, devono garantire che tutti i contenuti a cui forniscono l'accesso ottemperino a tutte le norme di Google Play e che possano anche essere soggette a ulteriori revisioni secondo le norme.

I termini definiti utilizzati in queste norme hanno lo stesso significato che hanno nel Contratto di distribuzione per gli sviluppatori (DDA, attribuzione basata sui dati). Oltre a rispettare queste norme e il Contratto di distribuzione per gli sviluppatori, i contenuti della tua app devono essere classificati in conformità con le nostre Linee guida per la classificazione dei contenuti.

Le app che potrebbero non essere appropriate per un vasto pubblico o comportare un'esperienza di bassa qualità per i nostri utenti finali non sono idonee alla promozione su Google Play. Rimangono, tuttavia, disponibili su Google Play fintanto che continuano a essere conformi con queste norme e con il Contratto di distribuzione per gli sviluppatori.

Google si riserva la facoltà di includere o rimuovere app da Google Play a sua discrezione. Potremmo agire in base a una serie di fattori, tra cui, a titolo esemplificativo, un modello di comportamento dannoso o un alto rischio di abuso. Identifichiamo il rischio di abuso utilizzando vari elementi come la cronologia delle violazioni precedenti, il feedback degli utenti e l'uso di brand, personaggi e altre risorse popolari.

Procedura di applicazione

Se l'app vìola le nostre norme, verrà rimossa da Google Play e tu riceverai un'email di notifica contenente il motivo preciso della rimozione. Violazioni gravi o ripetute (quali malware, frodi e

app che potrebbero arrecare danno all'utente o al dispositivo) di queste norme o del Contratto di distribuzione per gli sviluppatori comporteranno la chiusura di account singoli o correlati.

Tieni presente che le comunicazioni amministrative o relative a rimozioni potrebbero non indicare ogni singola violazione delle norme riscontrata nell'app o nel più ampio catalogo di app. È responsabilità degli sviluppatori risolvere eventuali problemi segnalati relativi alle norme e verificare con la dovuta attenzione che le altre parti dell'app siano completamente conformi alle norme. La mancata risoluzione delle violazioni potrebbe comportare ulteriori provvedimenti, ad esempio la rimozione definitiva dell'app o la chiusura dell'account.

Gestione e segnalazione di violazioni delle norme

In caso di domande o dubbi riguardanti una rimozione o una valutazione/un commento di un utente, puoi consultare le risorse riportate di seguito o contattarci tramite il Centro assistenza Google Play. Non siamo, tuttavia, in grado di fornirti consulenza legale, che puoi richiedere a un consulente.

Verifica delle app e ricorsi
Segnalazione di una violazione delle norme
Contatta Google Play in merito alla chiusura dell'account o alla rimozione di app
Avvisi imparziali
Segnalazione di app e commenti inappropriati
La mia app è stata rimossa da Google Play
Informazioni sulla chiusura degli account sviluppatore Google Play

Developer Distribution Agreement