Norme del programma per gli sviluppatori (in vigore dal 1 ottobre 2020)

Costruiamo insieme la fonte 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 consultare le nostre norme riportate di seguito.

Contenuti con limitazioni

Google Play viene utilizzato ogni giorno da persone di tutto il mondo per accedere ad app e giochi. Prima di inviare un'app, chiediti 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 incluse, a titolo esemplificativo ma non esaustivo, le app che promuovono la pedofilia o l'interazione inappropriata indirizzata a un minore (ad esempio palpeggiamenti o carezze).

Inoltre, sono vietate le app che attirano i bambini, ma contengono temi per adulti incluse, a titolo esemplificativo ma non esaustivo, app con eccessiva violenza, sangue e spargimento di sangue; app che rappresentano o incoraggiano attività dannose e pericolose. Non sono ammesse inoltre le app che promuovono una visione negativa del corpo o dell'immagine di sé, incluse app che rappresentano a scopo di intrattenimento chirurgia plastica, perdita di peso e altri interventi di carattere estetico relativi all'aspetto fisico di una persona.

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

Contenuti inappropriati

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 e linguaggio volgare

Sono vietate le app che contengono o promuovono contenuti di natura sessuale o linguaggio volgare, inclusa pornografia o qualsiasi contenuto o servizio inteso a essere sessualmente appagante. I contenuti che includono nudità possono essere consentiti se il loro scopo principale è educativo, documentaristico, scientifico o artistico e tale nudità non è fine a se stessa.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Rappresentazioni di nudo con connotazione sessuale o atteggiamenti sessualmente allusivi in cui il soggetto è nudo, sfocato o vestito in modo succinto e/o con un abbigliamento che non sarebbe accettabile in un contesto pubblico appropriato.
- Rappresentazioni, animazioni o illustrazioni di atti sessuali, atteggiamenti sessualmente allusivi o rappresentazione avente connotazione sessuale di parti del corpo.
- Contenuti raffiguranti o che rappresentano accessori sessuali, guide al sesso, temi sessuali illegali e fetish.
- Contenuti osceni o volgari inclusi, a titolo esemplificativo ma non esaustivo, contenuti che possono includere linguaggio volgare, insulti, testo esplicito, parole chiave per adulti/di natura sessuale nella scheda dello Store o nell'app.
- Contenuti che raffigurano, descrivono o promuovono la zoofilia.
- App che promuovono servizi di intrattenimento sessuale, di escort o di altro tipo che potrebbero essere interpretati come un'offerta di atti sessuali in cambio di un compenso.
- App che sviliscono o riducono le persone a oggetti.

Incitamento all'odio

Sono vietate 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, orientamento sessuale, genere, identità di genere o altre caratteristiche associate a discriminazione o emarginazione sistematica.

Le app con contenuti EDSA (aventi scopo didattico, documentaristico, scientifico o artistico) relative al nazismo potrebbero essere bloccate in determinati paesi, in conformità con le leggi e le normative locali.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Contenuti o affermazioni secondo i quali un gruppo protetto è inumano, inferiore o degno di odio.
- App che contengono insulti che incitano all'odio, stereotipi o teorie sulle caratteristiche negative che un gruppo protetto possiederebbe (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.
- Contenuti che promuovono simboli che incitano all'odio, ad esempio bandiere, simboli, segni di riconoscimento, oggetti correlati o comportamenti associati a gruppi che incitano all'odio.

Violenza

Non sono ammesse app che raffigurano o promuovono scene di violenza gratuita o altre attività pericolose. Sono generalmente ammesse le app che raffigurano scene di violenza fittizia nel contesto di un gioco, ad esempio cartoni animati, caccia o pesca.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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, il bullismo, le molestie, 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 app con contenuti di natura terroristica, ad esempio che promuovono atti terroristici, incitano alla violenza o esaltano attacchi terroristici. Per la pubblicazione di 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 che non manifestino la dovuta sensibilità nei confronti di calamità naturali, atrocità, conflitti, decessi o altri eventi tragici, oppure che sfruttino tali eventi. Le app con contenuti correlati a un evento sensibile sono generalmente consentite se tali contenuti hanno un valore ai fini EDSA o intendono informare o sensibilizzare le persone in merito all'evento.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Mancanza di sensibilità in relazione alla morte per suicidio, overdose, cause naturali e così via di una persona reale o di un gruppo di persone reali.
- Negazione di un evento tragico di rilievo.
- Apparente derivazione di profitto da un evento tragico senza vantaggi evidenti per le vittime.

Bullismo e molestie

Sono vietate le app che contengono o favoriscono minacce, molestie o atti di bullismo.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Bullismo nei confronti di vittime di conflitti internazionali o religiosi.
- Contenuti che configurano tentativi di sfruttamento di altri, inclusi estorsione, ricatto e così via.
- Pubblicazione di contenuti finalizzati alla pubblica umiliazione di un individuo.
- Molestie rivolte alle vittime di un evento tragico o ai loro amici e familiari.

Prodotti pericolosi

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

- Gli accessori soggetti a 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 proiettili.

Sono vietate le app che forniscono istruzioni per la produzione di esplosivi, armi da fuoco, munizioni, accessori per armi da fuoco soggetti a limitazioni o altre armi. Questo include 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, indipendentemente dalla loro legalità o meno.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 (tetraidrocannabinolo), inclusi prodotti come oli CBD contenenti THC.

Tabacco e alcol

Sono vietate le app che agevolano la vendita di tabacco (incluse le sigarette elettroniche e i vaporizzatori a penna) o che incoraggiano l'uso illegale o inappropriato di alcol o tabacco.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Raffigurare o incoraggiare l'uso o la vendita di alcol o tabacco a minori.
- Sottintendere che il consumo di tabacco possa migliorare le condizioni sociali, sessuali, professionali, intellettuali o atletiche.
- Raffigurare in una luce positiva l'eccessivo consumo di alcolici, inclusa la pratica del "binge drinking".

Servizi finanziari

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

Agli scopi 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 informative specifiche richieste dalla legge locale.

Opzioni binarie

Sono vietate le 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, da parte di una persona fisica, organizzazione o persona giuridica e a beneficio di un singolo consumatore, non destinato a finanziare l'istruzione personale o l'acquisto di immobilizzazioni. Per prendere decisioni informate in merito alla richiesta di un prestito personale, i consumatori interessati necessitano di informazioni su qualità, caratteristiche, commissioni, piano di rimborso, 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 sono inclusi: mutui immobiliari, prestiti per l'acquisto di un'auto, prestiti scolastici, linee di credito rotativo (ad esempio, carte di credito e linee di credito personale)

Le app che offrono prestiti personali incluse, a titolo esemplificativo ma non esaustivo, app che offrono prestiti direttamente, generatori di lead e app che mettono in comunicazione i consumatori con prestatori terzi, devono

specificare le seguenti informazioni nei 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
- Norme sulla privacy che informino in modo esauriente circa l'accesso, la raccolta, l'utilizzo e la condivisione dei dati utente personali e sensibili.

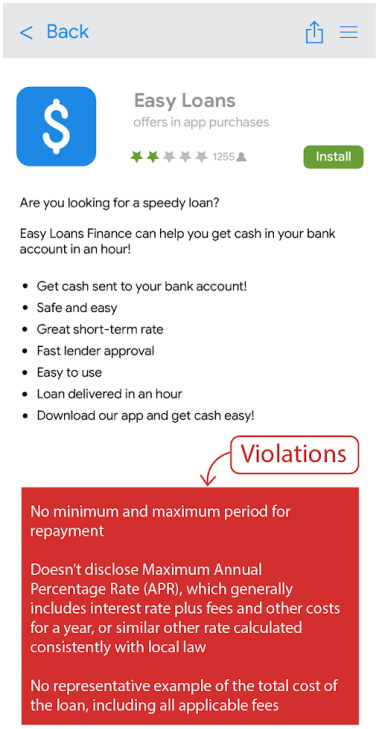
Sono vietate le app che promuovono prestiti personali che richiedono il rimborso completo entro al massimo 60 giorni dalla data di emissione (i cosiddetti "prestiti personali a breve termine").

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 prestatori terzi.

Di seguito è riportato un esempio di violazioni frequenti:



Giochi, concorsi e giochi e scommesse con vincite in denaro

Sono consentite app di giochi e scommesse con vincite in denaro, annunci correlati a giochi e scommesse con vincite in denaro e app di fantasport giornaliero che soddisfano determinati requisiti.

App di giochi e scommesse

Sono ammessi solo contenuti e servizi che agevolano giochi e scommesse online nei seguenti paesi:

- Regno Unito, Irlanda e Francia
- Brasile (limitato alle app approvate pubblicate dalla Caixa Economica Federal)

Queste app devono soddisfare i seguenti requisiti:

- Lo sviluppatore deve completare correttamente 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 per ogni paese in cui viene distribuita.
- Lo sviluppatore deve disporre di una licenza per giochi e scommesse valida per ogni paese in cui l'app viene distribuita.
- L'app deve impedire agli utenti minorenni di effettuare giochi e scommesse.

- L'app non deve poter essere utilizzata nei paesi non coperti dalla licenza per giochi e scommesse 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 classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC; e inoltre
- L'app e la relativa scheda devono visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse.

In tutti gli altri paesi non sono ammessi contenuti o servizi che favoriscono giochi e scommesse 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.

Altre app per concorsi, tornei e giochi e scommesse con vincite in denaro

Non sono ammessi contenuti o servizi che consentano o favoriscano la capacità degli utenti di puntare, rischiare o partecipare utilizzando denaro (inclusi gli articoli in-app acquistati con denaro) per aggiudicarsi un premio di valore monetario reale. Sono inclusi, a titolo esemplificativo ma non esaustivo, casinò online, scommesse sportive, lotterie che non soddisfano i requisiti per le app di giochi e scommesse sopra citati e giochi che offrono premi in denaro o altro valore reale.

Ecco alcuni esempi di violazioni:

- Giochi che accettano denaro a fronte dell'opportunità di aggiudicarsi un premio fisico o monetario
- Giochi con acquisizione di punti "fedeltà" (ad es. ottenuti tramite coinvolgimento o svolgimento di attività) che (1) avvenga o risulti accelerata tramite acquisti con denaro reale e che (2) possano essere scambiati con articoli o premi di valore monetario reale
- App che accettano o gestiscono puntate relative a scommesse, valute in-app richieste per la partecipazione, vincite o versamenti per ottenere o accelerare l'idoneità ad aggiudicarsi un premio fisico o monetario.
- App che offrono un "invito all'azione" per puntare, rischiare o partecipare a giochi, concorsi o tornei con vincite in denaro, ad esempio app con elementi di navigazione (voci di menu, schede, pulsanti ecc.) che invitano gli utenti, con frasi come "REGISTRATI" o "PARTECIPA ANCHE TU", a prendere parte a un torneo per vincere un premio in denaro.

Annunci di giochi e scommesse o di giochi, concorsi e tornei con vincite in denaro all'interno di app distribuite su Play

Sono ammesse le app che pubblicizzano giochi e scommesse o giochi, concorsi e tornei con vincite in denaro se soddisfano i seguenti requisiti:

- L'app e l'annuncio (inclusi gli inserzionisti) devono essere conformi a tutte le leggi vigenti e agli standard di settore per tutte le località in cui viene visualizzato l'annuncio.
- L'annuncio deve rispettare i requisiti di licenza locali per tutti i prodotti e servizi relativi a giochi e scommesse oggetto di promozione.
- L'app non deve mostrare annunci relativi a giochi e scommesse a individui di cui sia certa l'età 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.
- Se pubblicizza un'app di giochi e scommesse (come definita sopra), l'annuncio deve visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse nella pagina di destinazione, direttamente nella scheda dell'app pubblicizzata o all'interno dell'app;-
- L'app non deve fornire contenuti di giochi e scommesse simulati (ad es. app di casinò sui social; app con slot machine virtuali);
- L'app non deve fornire funzionalità di supporto per giochi e scommesse oppure giochi, lotterie e tornei con vincite in denaro (ad es. funzionalità che agevolano le scommesse, i pagamenti, il tracciamento di risultati/quote sportive o la gestione di fondi di partecipazione);
- Non devi essere titolare di quote di proprietà in servizi di giochi e scommesse o di giochi, lotterie o tornei con vincite in denaro pubblicizzati nell'app;
- I contenuti dell'app non devono promuovere o indirizzare gli utenti a servizi di giochi e scommesse o di giochi, lotterie o tornei con vincite in denaro

Solo le app di giochi e scommesse (come definite sopra) o le app che soddisfano tutti questi requisiti relativi agli annunci di giochi e scommesse possono includere annunci relativi a giochi e scommesse o a giochi, lotterie e tornei con vincite in denaro.

Di seguito sono riportati alcuni esempi di violazioni comuni:

- Un'app concepita per utenti minorenni e che mostra un annuncio che promuove servizi di giochi e scommesse
- Un gioco di casinò simulato che promuove o indirizza gli utenti a casinò con denaro reale
- Un'app dedicata di tracciamento delle quote legate a eventi sportivi contenente annunci di giochi e scommesse integrati che rimandano a un sito di scommesse sportive
- Un'app di notizie che mostra annunci per un servizio di giochi e scommesse di proprietà o gestito dallo sviluppatore dell'app stessa
- App che contengono annunci di giochi e scommesse che violano le nostre norme sugli annunci ingannevoli, ad esempio gli annunci che vengono mostrati agli utenti sotto forma di pulsanti, icone o altri elementi in-app interattivi

App di fantasport giornaliero (DFS)

Sono consentite le app di fantasport giornaliero (DFS), come definito dalle leggi locali vigenti, se soddisfano i seguenti requisiti:

- L'app è 1)-distribuita solo negli Stati Uniti o 2) idonea in base ai requisiti delle app per giochi e scommesse sopra indicati;
- Lo sviluppatore deve completare correttamente 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 gli standard di settore per i paesi in cui è distribuita;
- L'app deve impedire agli utenti minorenni di effettuare scommesse o transazioni monetarie al suo interno.
- 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 classificazione AO (Adult Only - Solo adulti) o l'equivalente IARC; e inoltre
- L'app e la relativa scheda devono visualizzare chiaramente le informazioni sulla pratica responsabile di giochi e scommesse.

Se l'app è distribuita negli Stati Uniti, si applicano i seguenti requisiti aggiuntivi:

- L'app deve essere conforme a tutte le leggi vigenti e agli standard di settore per ogni 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 fantasport giornaliero;
- 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 fantasport giornaliero; e inoltre
- L'app non deve poter essere utilizzata negli stati o territori degli Stati Uniti in cui le app di fantasport giornaliero non sono legali.

Attività illegali

Sono vietate le app che agevolano o promuovono attività illegali.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

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

Contenuti generati dagli utenti

I contenuti generati dagli utenti (UGC) sono contenuti che gli utenti pubblicano in un'app e che sono visibili e accessibili ad almeno un sottoinsieme di utenti dell'app.

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 contenuti e comportamenti discutibili (in modo conforme alle Norme del programma per gli sviluppatori di Play) e vietarli nei termini e condizioni d'uso o nei criteri relativi agli utenti dell'app;
- Implementare una funzionalità di moderazione dei contenuti generati dagli utenti che sia continua, efficace e robusta, nonché ragionevole e coerente rispetto al tipo o ai tipi di contenuti generati dagli utenti ospitato o ospitati dall'app

    - Nel caso di app di live streaming, tutti i contenuti generati dagli utenti che siano discutibili devono essere rimossi idealmente in tempo reale e comunque non appena ragionevolmente possibile;
    - Nel caso di app in realtà aumentata (AR), la moderazione dei contenuti generati dagli utenti (incluso il sistema di segnalazione in-app) deve tenere conto sia di contenuti AR generati dagli utenti che siano discutibili (ad esempio, un'immagine AR sessualmente esplicita) sia della posizione di ancoraggio AR sensibile (ad esempio, contenuti AR ancorati a un'area geografica con restrizioni, come una base militare o una proprietà privata in cui l'ancoraggio AR potrebbe causare problemi al titolare della proprietà);
- Offrire un sistema in-app di facile utilizzo per la segnalazione di contenuti generati dagli utenti che siano discutibili e prendere provvedimenti nei confronti di tali contenuti, ove opportuno;
- Rimuovere o bloccare gli utenti molesti che violano i termini e condizioni d'uso dell'app e/o le norme relative agli utenti;
- Fornire misure di tutela per impedire che la monetizzazione in-app incoraggi comportamenti discutibili da parte degli utenti.

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

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Promozione di contenuti generati dagli utenti sessualmente espliciti, inclusa l'implementazione o l'autorizzazione 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 principalmente finalizzati a molestare o prendere di mira un'altra persona sottoponendola a maltrattamenti, attacchi crudeli o atti di derisione.
- App che omettono ripetutamente di adottare misure a seguito a 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 collegamento con la perdita di peso o il 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 non approvati da enti statali, commercializzati in modo da lasciarne intendere sicurezza o efficacia nel prevenire o curare una malattia o disturbo della 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.

Proprietà intellettuale

Quando gli sviluppatori copiano il lavoro altrui o lo utilizzano senza la dovuta autorizzazione, questo può arrecare danno al titolare. Evita qualsiasi uso illegittimo del lavoro di altre persone.

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 proprietari). Sono inoltre vietate le app che istigano o inducono alla violazione di diritti di proprietà intellettuale.

Risponderemo a chiare segnalazioni di presunta violazione del copyright. Per ulteriori informazioni o per presentare una richiesta ai sensi del DMCA (Digital Millennium Copyright Act), 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 disponi della documentazione scritta attestante la tua autorizzazione a utilizzare un contenuto di proprietà intellettuale di terze parti nella tua app o scheda dello Store (ad esempio nomi di brand, loghi e risorse grafiche), contatta il team di Google Play prima di inviare i contenuti per assicurarti che l'app non venga rifiutata per violazione di 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.

Presta attenzione quando utilizzi contenuti protetti da copyright per dimostrare la funzionalità della tua app. In genere l'approccio più sicuro consiste nel creare contenuti originali.

Di seguito sono riportati alcuni esempi di contenuti protetti da copyright che vengono spesso utilizzati senza autorizzazione o senza un motivo legittimo:

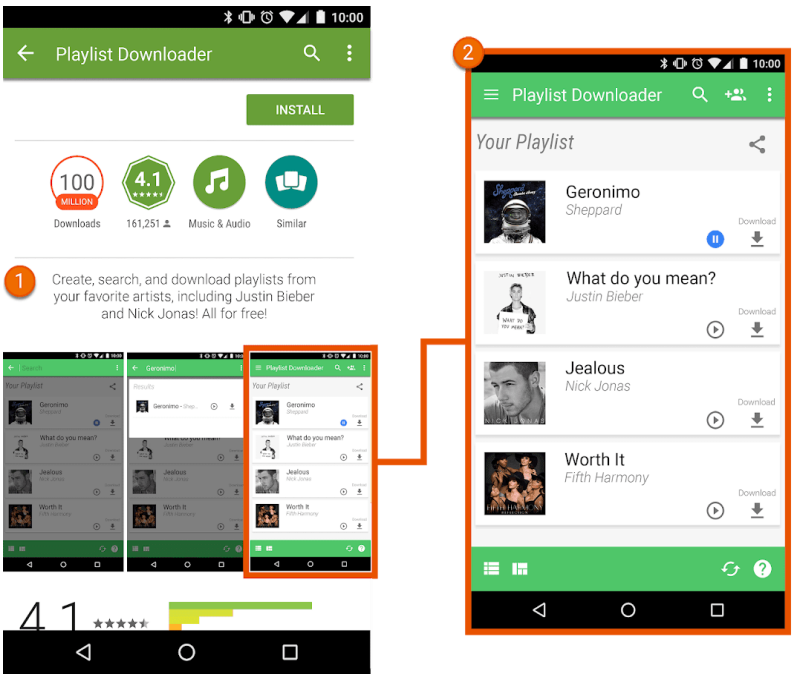
- Immagini di copertina di album musicali, videogiochi e libri.
- Immagini di marketing di film, programmi TV o videogiochi.
- Artwork o immagini da fumetti, cartoni animati, film, video musicali o programmi TV.
- Loghi di squadre sportive professionistiche o universitarie.
- Foto recuperate dall'account 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, devi verificare se potrebbe istigare alla violazione del copyright e, se necessario, rivolgerti a un consulente legale.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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, in violazione della 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 altri soggetti sono vietate. Un marchio è una parola, un simbolo o una combinazione di questi 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 potenzialmente confusione in merito all'origine del prodotto. Se la tua app utilizza marchi di un altro soggetto in un modo che rischia di creare confusione, 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 spacciarsi per il prodotto originale del proprietario del brand.

Privacy, comportamento ingannevole e abuso del dispositivo

Ci impegniamo a fornire un ambiente sicuro e protetto per i nostri utenti e a tutelare 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 assicurare la trasparenza in merito alla modalità di gestione dei dati utente (ovvero le informazioni fornite da un utente o raccolte in relazione 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, devi fare riferimento anche ai requisiti aggiuntivi nella sezione "Informazioni personali e sensibili" di seguito. I presenti 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 ma non esaustivo, 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 collegati a 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 promosse 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 eventualmente 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 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 (ad esempio, la raccolta dei dati avviene in background), dovrai soddisfare i seguenti requisiti:

Fornire un'informativa in-app circa l'accesso, la raccolta, l'utilizzo e la 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 visualizzata 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 dell'app deve essere associata e precedere immediatamente una richiesta di consenso dell'utente e, laddove possibile, un'autorizzazione di runtime associata. Non puoi 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 un intervento dell'utente (ad esempio tocco per accettazione, selezione una casella di controllo).
- **Non deve** considerare l'uscita dalla finestra contenente l'informativa (ad esempio, tocco fuori dalla finestra o pressione del pulsante Home o Indietro) come espressione del consenso; e inoltre
- **Non deve** utilizzare messaggi con scadenza o chiusura automatica per ottenere il consenso dell'utente.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Un'app che accede all'inventario di un utente delle app installate e non tratta questi dati come personali o sensibili e soggetti alle suddette norme sulla privacy e ai suddetti requisiti di gestione dei dati, informativa in posizione ben visibile e consenso.
- Un'app che accede ai dati del telefono o della rubrica di contatti e non considera questi dati come personali o sensibili e soggetti alle suddette norme sulla privacy e ai suddetti requisiti di gestione dei dati, informativa in posizione ben visibile e consenso.
- Un'app che registra la schermata dell'utente e non considera tali dati come personali o sensibili e soggetti alle norme sulla privacy.
- Un'app che rileva la posizione del dispositivo senza spiegarne in modo esauriente l'utilizzo e senza ottenere il consenso nel rispetto dei requisiti sopra indicati.
- Un'app che raccoglie autorizzazioni limitate in background, ad esempio a scopi di monitoraggio, ricerca o marketing, senza spiegarne in modo esauriente l'utilizzo e senza ottenere il consenso nel rispetto dei requisiti sopra indicati.

Restrizioni specifiche per l'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 codici di identificazione ufficiali	L'app non deve mai rendere pubblici eventuali dati utente personali o sensibili relativi ad attività finanziarie o di pagamento oppure codici di identificazione 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.
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)

Privacy Shield (scudo per la privacy)

Qualora tu acceda, utilizzi o elabori informazioni personali rese disponibili da Google che identificano un individuo in modo diretto o indiretto e provengono dall'Unione Europea o dalla Svizzera ("Informazioni personali dell'UE"), devi:

- Rispettare tutte le leggi, direttive, regolamenti e norme vigenti riguardanti la privacy, nonché la sicurezza e la protezione dei dati;
- Utilizzare, elaborare le Informazioni personali dell'UE o accedervi solo per scopi conformi al consenso rilasciato dalla persona cui tali informazioni fanno riferimento;

- Implementare le 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; e inoltre
- Fornire un livello di protezione pari a quello richiesto dai Principi del Privacy Shield (scudo per la privacy).

Devi monitorare regolarmente il rispetto di queste condizioni. Se in qualsiasi momento non potessi rispettare queste condizioni (o se esiste un rischio elevato che tu possa non rispettarle), devi informarci immediatamente inviando un'email all'indirizzo data-protection-office@google.com e 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. Puoi richiedere solo le autorizzazioni necessarie per implementare funzionalità o servizi esistenti della tua app che vengono promossi nella scheda del Play Store. Non puoi 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.

Devi richiedere le autorizzazioni di accesso ai dati all'interno del contesto (tramite auth incrementale), affinché gli utenti capiscano perché tali autorizzazioni sono necessarie. Devi utilizzare 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 fare richiesta agli utenti e accertarsi che prestino consenso esplicito agli usi aggiuntivi.

Autorizzazioni limitate

In aggiunta a quanto sopra, le autorizzazioni limitate sono autorizzazioni definite come Pericolosa, Speciale o Firma 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. Puoi 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, devi rispettare la loro decisione. Gli utenti non possono essere manipolati o forzati a concedere autorizzazioni non fondamentali. Devi 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 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 dati sensibili e alle seguenti restrizioni:

Autorizzazione limitata	Requisito
Il file manifest dell'app richiede il gruppo di autorizzazioni Registro chiamate (ad esempio READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	Deve essere registrato attivamente come gestore predefinito di telefono o assistente sul dispositivo.
Il file manifest dell'app richiede il gruppo di autorizzazioni SMS (ad esempio, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	Deve essere registrato attivamente 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 una o più tra 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 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

La posizione del dispositivo è considerata un dato utente personale e sensibile soggetto alle norme relative a Informazioni personali e dati 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.
- Non dovresti 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, potremo rifiutare eventuali app che richiedano la posizione in background o accedano a questa senza una giustificazione convincente.
- 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
- Viene terminato 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.

Autorizzazione Accesso a tutti i file

I file e gli attributi di directory sul dispositivo di un utente sono considerati dati utente personali e sensibili soggetti alle norme relative a Informazioni personali e sensibili e ai seguenti requisiti:

- Le app devono richiedere l'accesso solo allo spazio di archiviazione del dispositivo essenziale per il loro funzionamento e non possono richiedere l'accesso allo spazio di archiviazione per conto di terze parti per scopi non correlati alla funzionalità critica per gli utenti.
- I dispositivi Android su cui è installato R (Android 11, Livello API 30) o versioni successive richiedono l'autorizzazione MANAGE_EXTERNAL_STORAGE per gestire l'accesso nell'archivio condiviso. Tutte le app destinate a R e che richiedono accesso completo all'archivio condiviso ("Accesso a tutti i file") devono superare una revisione di accesso appropriata prima della pubblicazione. Le app autorizzate a utilizzare questa autorizzazione devono chiedere chiaramente agli utenti di abilitare "Accesso a tutti i file" nelle impostazioni "Accesso speciale per le app". Per ulteriori informazioni sui requisiti di R, consulta questo articolo del Centro assistenza.

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 (interfacce di programmazione di un'applicazione) o servizi inclusi, a titolo esemplificativo ma non esaustivo, 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.

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 vietato il codice che introduce o sfrutta vulnerabilità di sicurezza. Consulta il Programma App Security Improvement per scoprire i problemi di sicurezza più recenti segnalati agli sviluppatori.

Di seguito sono riportati alcuni esempi di violazioni comuni:

- 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.
- Agevolare servizi proxy verso terzi è consentito solo laddove sia lo scopo principale dell'app proposto all'utente.
- App o codice di terze parti (ad es. SDK) che scaricano codice eseguibile, ad esempio file dex o codice nativo, da una fonte diversa da Google Play.
- App che installano altre app su un dispositivo senza previo consenso dell'utente.
- App che agevolano o rimandano alla distribuzione o all'installazione di software dannoso.

Comportamento ingannevole

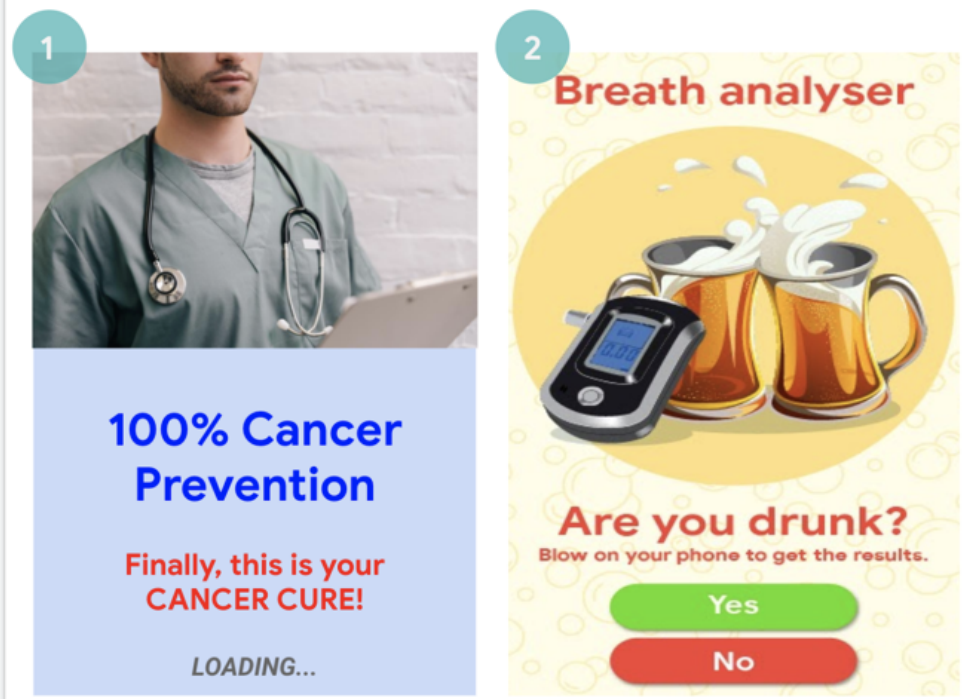
Sono vietate le app che cercano di ingannare gli utenti o di favorire comportamenti disonesti incluse, a titolo esemplificativo ma non esaustivo, tutte le app il cui funzionamento sia determinato essere impossibile. Le app devono contenere comunicazioni, descrizioni e immagini/video precisi relativi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

Affermazioni ingannevoli

Sono vietate le app contenenti affermazioni e informazioni false o fuorvianti, neanche nella descrizione, nel titolo, nell'icona e negli screenshot.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App contenenti rappresentazioni ingannevoli oppure descrizioni non precise e chiare in merito alla loro funzionalità:
  - Un'app contenente una descrizione e 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 testuale 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, dichiarando 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 (ad esempio, app repellenti per gli insetti), anche se sono rappresentate come scherzi, imitazioni, prese in giro e così via.
- App classificate in modo errato inclusa, a titolo esemplificativo, la classificazione o la categoria dell'app.
- 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 agevolare servizi governativi per i quali non sono autorizzate.
- App che dichiarano falsamente di essere le app ufficiali di un'entità riconosciuta. Titoli quali "App ufficiale di Justin Bieber" sono vietati senza le autorizzazioni o i diritti necessari.



(1) App che includono dichiarazioni mediche o relative alla salute (cura del cancro) ingannevoli
(2) App che dichiarano di avere funzionalità che in realtà non è possibile implementare (uso del telefono come etilometro)

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, preferiti, 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.

Agevolazione di 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 contenuti e funzionare secondo le ragionevoli e precise aspettative dell'utente.

È possibile scaricare risorse aggiuntive delle app (ad esempio, relative 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 indicate come "scherzo" o come create "per scopi di intrattenimento" (o altri sinonimi) non sono esenti dall'applicazione delle nostre norme.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App che imitano altre app o siti web per indurre con l'inganno gli utenti a comunicare informazioni personali o dati di autenticazione.
- App che mostrano o presentano numeri telefonici, contatti, indirizzi o informazioni che consentono l'identificazione personale, reali o non verificati, di individui o entità non consenzienti.

- App con funzionalità principali diverse in base all'area geografica dell'utente, ai parametri del dispositivo o ad altri dati dipendenti dall'utente in cui tali differenze non vengono pubblicizzate in modo evidente per l'utente nella scheda dello Store.
- App che cambiano in modo significativo da una versione all'altra senza avvisare l'utente (ad esempio, sezione "novità") né aggiornare la scheda dello Store.
- App che tentano di modificare oppure offuscare il comportamento durante la revisione.
- 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.

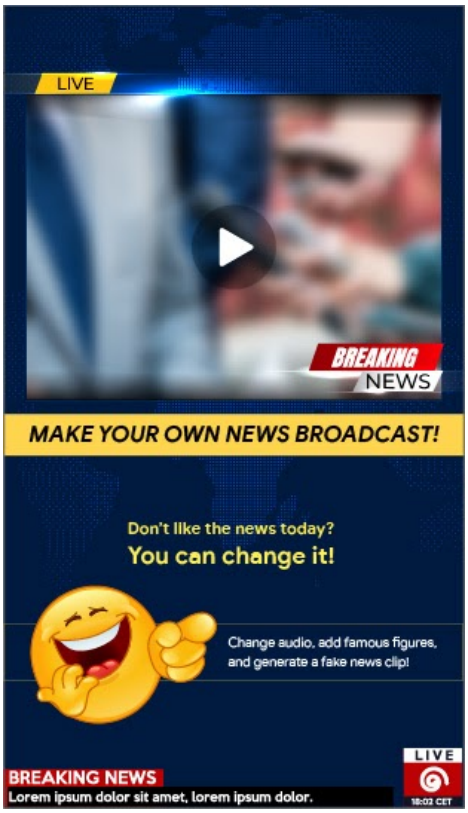
Contenuti multimediali manipolati

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 diffondere 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.

Di seguito sono riportati alcuni esempi di violazioni comuni:

- 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.



(1) Questa app fornisce funzionalità per alterare i clip multimediali per simulare un notiziario e aggiungere personaggi famosi o pubblici al clip senza watermark.

Rappresentazione ingannevole

Sono vietati gli account sviluppatore e le app che:

- Assumono l'identità di persone o organizzazioni oppure che occultano o rappresentano in maniera ingannevole informazioni sulla propria proprietà o sul proprio scopo principale.

- Intraprendono attività coordinate allo scopo di ingannare gli utenti. Sono inclusi, a titolo esemplificativo ma non esaustivo, gli account sviluppatore o le app che travisano o nascondono il proprio paese di origine e che indirizzano contenuti a utenti di un altro paese.
- Si coordinano con altri siti, sviluppatori, app o account per occultare o rappresentare in maniera ingannevole l'identità dell'app o dello sviluppatore o altri dati personali, se i contenuti proposti sono relativi a politica, problemi sociali o questioni di interesse pubblico.

Malware

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.

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.

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 fatturazione fraudolenta o spyware commerciale. Conseguentemente, un sottoinsieme di backdoor, in determinate circostanze, viene considerato da Google Play Protect come una vulnerabilità.

Fatturazione fraudolenta

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

La fatturazione fraudolenta su dispositivi mobili può essere costituita da: 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.

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 in modo condizionale 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 pagamento. 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.

Stalkerware

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

Le app stalkerware trasmettono dati a una parte diversa dal fornitore dell'app potenzialmente dannosa.

I genitori potrebbero usare forme ammissibili 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 a meno che non venga visualizzata una notifica persistente durante la trasmissione dei dati.

Solo le app conformi alle norme, progettate e commercializzate esclusivamente per il monitoraggio da parte di genitori (e famigliari) o per la gestione aziendale, possono essere distribuite nel Play Store con funzionalità di tracciamento e reporting, purché siano pienamente conformi ai requisiti descritti di seguito.

Le app non stalkerware distribuite sul Play Store che monitorano o tengono traccia del comportamento di un utente su un dispositivo devono soddisfare quanto meno 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.
- Le app devono 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.

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 funzioni principali 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 utilizzano funzionalità in modo illecito per evitare disinstallazione o arresto.
- 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 adeguata comunicazione o consenso.

Ad esempio, la trasmissione di una qualsiasi delle seguenti informazioni senza informativa 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 a pagamento 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 sia 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.

Software indesiderato per dispositivi mobili

Questa norma si basa sulle Norme relative al software indesiderato di Google definendo i principi per l'ecosistema Android e il Google Play Store. Adottiamo provvedimenti per tutelare gli utenti dal software che vìola tali princìpi, poiché quest'ultimo risulta potenzialmente negativo per la loro esperienza.

Software indesiderato per dispositivi mobili

Noi di Google riteniamo che se ci concentriamo sull'utente, tutto il resto viene da sé. Nei nostri Principi sul software e nelle Norme relative al software indesiderato, forniamo consigli generali per i software che offrono un'ottima esperienza utente. Questa norma si basa sulle Norme relative al software indesiderato di Google definendo i principi per l'ecosistema Android e il Google Play Store. Adottiamo provvedimenti per tutelare gli utenti dal software che vìola tali princìpi, poiché quest'ultimo risulta potenzialmente negativo per la loro esperienza.

Come indicato nelle Norme relative al software indesiderato, abbiamo riscontrato che la maggior parte dei software indesiderati presenta una o più delle stesse caratteristiche di base:

- È ingannevole in quanto promette un valore aggiunto che non offre.
- Cerca di indurre con l'inganno gli utenti a installarlo o si cela all'interno di un altro programma che l'utente sta installando.
- Non illustra all'utente le sue funzioni principali e distintive.
- Altera il sistema dell'utente in modi inaspettati.
- Raccoglie o trasmette informazioni private a insaputa degli utenti.
- Raccoglie o trasmette informazioni private senza una gestione sicura (ad esempio, trasmissione tramite HTTPS)
- Viene integrato in altro software senza comunicarne la presenza.

Sui dispositivi mobili, il software è codice sotto forma di app, programma binario, modifica del framework e così via. Per bloccare software dannosi per l'ecosistema informatico o che influenzano negativamente l'esperienza utente, prendiamo provvedimenti sul codice che vìola questi principi.

Di seguito, estendiamo l'applicabilità delle Norme relative al software indesiderato anche al software per dispositivi mobili. Come per quelle norme, continueremo a perfezionare queste Norme relative al software indesiderato per dispositivi mobili in modo da affrontare nuovi tipi di violazioni.

Comportamento trasparente e divulgazione chiara

Tutto il codice deve rispettare le promesse fatte all'utente. Le app devono fornire tutte le funzionalità comunicate. Le app non devono confondere gli utenti.

- Le app devono indicare chiaramente la propria funzionalità e obiettivi.
- Spiega in modo chiaro ed esplicito le modifiche che verranno apportate dall'app al sistema e consenti agli utenti di esaminare e approvare tutte le modifiche e le opzioni di installazione significative.
- Il software non deve rappresentare in modo ingannevole lo stato del dispositivo dell'utente, ad esempio dichiarando che il sistema è in uno stato di sicurezza critico o infettato da virus.
- Non utilizzare attività non valide concepite per aumentare il traffico dagli annunci pubblicitari e/o le conversioni.
- Sono vietate le app che ingannano gli utenti assumendo l'identità di un altro soggetto (ad esempio, altri sviluppatori, aziende, persone giuridiche) o di un'altra app. Evita di lasciare falsamente intendere che l'app sia collegata o autorizzata da qualcuno.

Esempi di violazioni:

- Frode pubblicitaria
- Furto d'identità

Proteggere i dati utente

Sii chiaro e trasparente in merito all'accesso, all'utilizzo, alla raccolta e alla condivisione di dati utente personali e sensibili. L'utilizzo dei dati utente deve rispettare tutte le Norme pertinenti relative ai dati utente, ove applicabili, e adottare tutte le misure necessarie per proteggere tali dati.

- Devi fornire agli utenti l'opportunità di accettare la raccolta dei loro dati prima di iniziare a raccoglierli e inviarli dal dispositivo, inclusi dati relativi ad account di terze parti, email, numero di telefono, app installate, file, posizione e qualsiasi altro dato personale e sensibile del quale l'utente non si aspetterebbe la raccolta.
- I dati utente personali e sensibili che vengono raccolti devono essere gestiti in modo sicuro, inclusa la trasmissione mediante metodi moderni di crittografia (ad esempio, tramite HTTPS).
- Il software, incluse le app per dispositivi mobili, deve trasmettere ai server solo dati utente personali e sensibili, in quanto correlati alla funzionalità dell'app.

Esempi di violazioni:

- Raccolta dei dati (vedi Spyware)
- Utilizzo illecito di autorizzazioni limitate

Esempi di Norme sui dati utente:

- *Norme sui dati utente di Google Play*
- *Norme sui dati utente dei requisiti GMS*
- *Norme sui dati utente del servizio API di Google*

Non compromettere l'esperienza su dispositivi mobili

L'esperienza utente deve essere semplice, facile da capire e basata su scelte chiare effettuate dall'utente. Deve presentare all'utente una proposta di valore chiara e non interrompere l'esperienza utente pubblicizzata o desiderata.

- Non mostrare annunci che vengono presentati agli utenti in modi imprevisti, ad esempio compromettendo o interferendo con l'usabilità delle funzionalità del dispositivo o visualizzandoli al di fuori dell'app senza che sia possibile

chiuderli facilmente e senza consenso e attribuzione adeguati.
- Le app non devono interferire con altre app o con l'usabilità del dispositivo.
- La possibilità di procedere alla disinstallazione, se applicabile, deve essere chiara.
- Il software per dispositivi mobili non deve imitare le richieste del sistema operativo del dispositivo o di altre app. Non eliminare gli avvisi all'utente da altre app o dal sistema operativo, in particolare quelli che lo informano delle modifiche al sistema operativo.

Esempi di violazioni:

- Annunci improvvisi
- Utilizzo non autorizzato o imitazione di funzionalità di sistema

Frode pubblicitaria

La frode pubblicitaria è severamente vietata. Le interazioni con gli annunci generate allo scopo di indurre una rete pubblicitaria a ritenere che il traffico provenga da un autentico interesse dell'utente è considerata frode pubblicitaria, una forma di traffico non valido. Le frodi pubblicitarie possono essere il sottoprodotto dell'implementazione di annunci in modi non consentiti da parte degli sviluppatori, ad esempio visualizzazione di annunci nascosti, clic automatico sugli annunci, alterazione o modifica di informazioni e altre modalità di utilizzo di azioni non umane (spider, bot e così via) o di attività umane concepite per generare traffico dagli annunci pubblicitari non valido. Il traffico non valido e le frodi pubblicitarie sono dannosi per inserzionisti, sviluppatori e utenti e comportano una perdita di fiducia a lungo termine nell'ecosistema degli annunci per dispositivi mobili.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

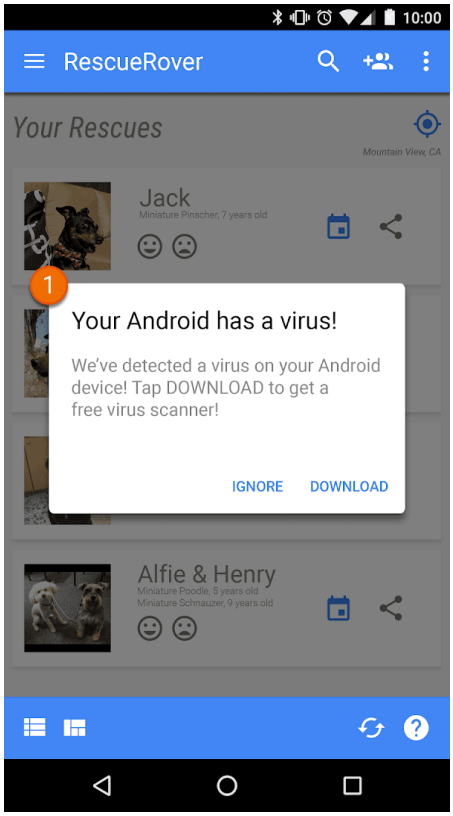
- App che mostra annunci che non sono visibili all'utente.
- App che genera automaticamente clic sugli annunci senza l'intenzione dell'utente o che genera traffico di rete equivalente per assegnare in modo fraudolento i crediti relativi ai clic.
- App che invia clic di attribuzione di installazione non veritieri per ricevere pagamenti per installazioni che non provengono dalla rete del mittente.
- App che mostra annunci quando l'utente non si trova nella sua interfaccia.
- False dichiarazioni dell'inventario pubblicitario da parte di un'app, ad esempio un'app che comunica alle reti pubblicitarie che è in esecuzione su un dispositivo iOS quando in realtà è installata su Android o un'app che rappresenta in modo ingannevole il nome del pacchetto che viene monetizzato.

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.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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, leggi le Norme relative agli annunci.

Furto d'identità

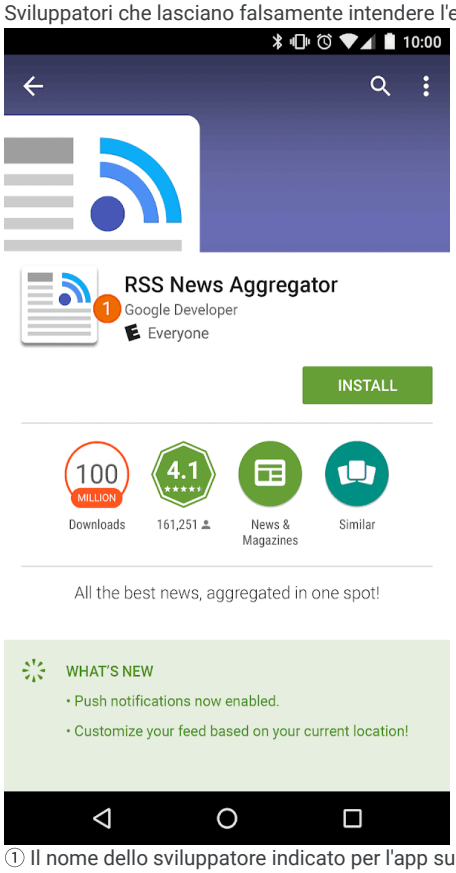
Quando gli sviluppatori assumono l'identità di altri soggetti o delle loro app, ingannano gli utenti e arrecano danno alla community degli sviluppatori. Sono vietate le app che ingannano gli utenti assumendo l'identità di altri soggetti.

Furto d'identità

Sono vietate le app che ingannano gli utenti assumendo l'identità di altri soggetti (ad esempio, altri sviluppatori, aziende, persone giuridiche) o di un'altra app. Evita di lasciar falsamente intendere che l'app sia collegata o autorizzata da qualcuno. Fai attenzione a non utilizzare icone dell'app, descrizioni, titoli o elementi in-app che potrebbero fuorviare gli utenti in merito alla relazione della tua app con un altro soggetto o con un'altra app.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Sviluppatori che lasciano falsamente intendere l'esistenza di una relazione con un'altra azienda o sviluppatore:



① Il nome dello sviluppatore indicato per l'app suggerisce una relazione ufficiale con Google, che in realtà non sussiste.

- Titoli e icone di app talmente simili a quelli di prodotti o servizi esistenti da poter trarre in inganno gli utenti:

Monetizzazione e annunci

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, sei tenuto 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.

Di seguito sono riportati alcuni esempi di prodotti supportati dalla Fatturazione in-app di Google Play:

- **Giochi virtuali**, inclusi tesori, monete, vite o turni extra, elementi o strumenti speciali, personaggi o avatar, tempo di gioco o livelli aggiuntivi.
- **Funzionalità o contenuti di app**, ad esempio versioni senza annunci delle app o nuove funzionalità non disponibili nelle versioni gratuite.
- **Servizi ad abbonamento**, ad esempio servizi di musica in streaming, video, libri o altri servizi multimediali; pubblicazioni digitali, anche se offerte in combinazione con un'edizione cartacea, e servizi di social network.
- **Prodotti software nel cloud**, inclusi servizi di archiviazione dati, software per la produttività aziendale e software di gestione finanziaria.

Di seguito sono riportati alcuni esempi di prodotti attualmente non supportati dalla Fatturazione in-app di Google Play:

- **Prodotti al dettaglio**, ad esempio alimentari, abbigliamento, articoli per la casa ed elettronica.
- **Commissioni di servizio**, ad esempio servizi di taxi e trasporto, di pulizia, consegna di cibo a domicilio, prezzi di biglietti aerei e biglietti di eventi.
- **Quote di iscrizione una tantum o quote periodiche**, ad esempio iscrizioni in palestra, programmi fedeltà o circoli che offrono accessori, abbigliamento o altri prodotti fisici.
- **Pagamenti una tantum**, inclusi pagamenti peer-to-peer, aste online e donazioni.
- **Pagamento elettronico di fatture**, ad esempio conti di carte di credito, bollette e servizi di telecomunicazione o via cavo.

Tieni presente che l'API Google Pay è a disposizione per le app che vendono servizi e prodotti fisici. Per ulteriori informazioni, visita la nostra pagina per sviluppatori Google Pay.

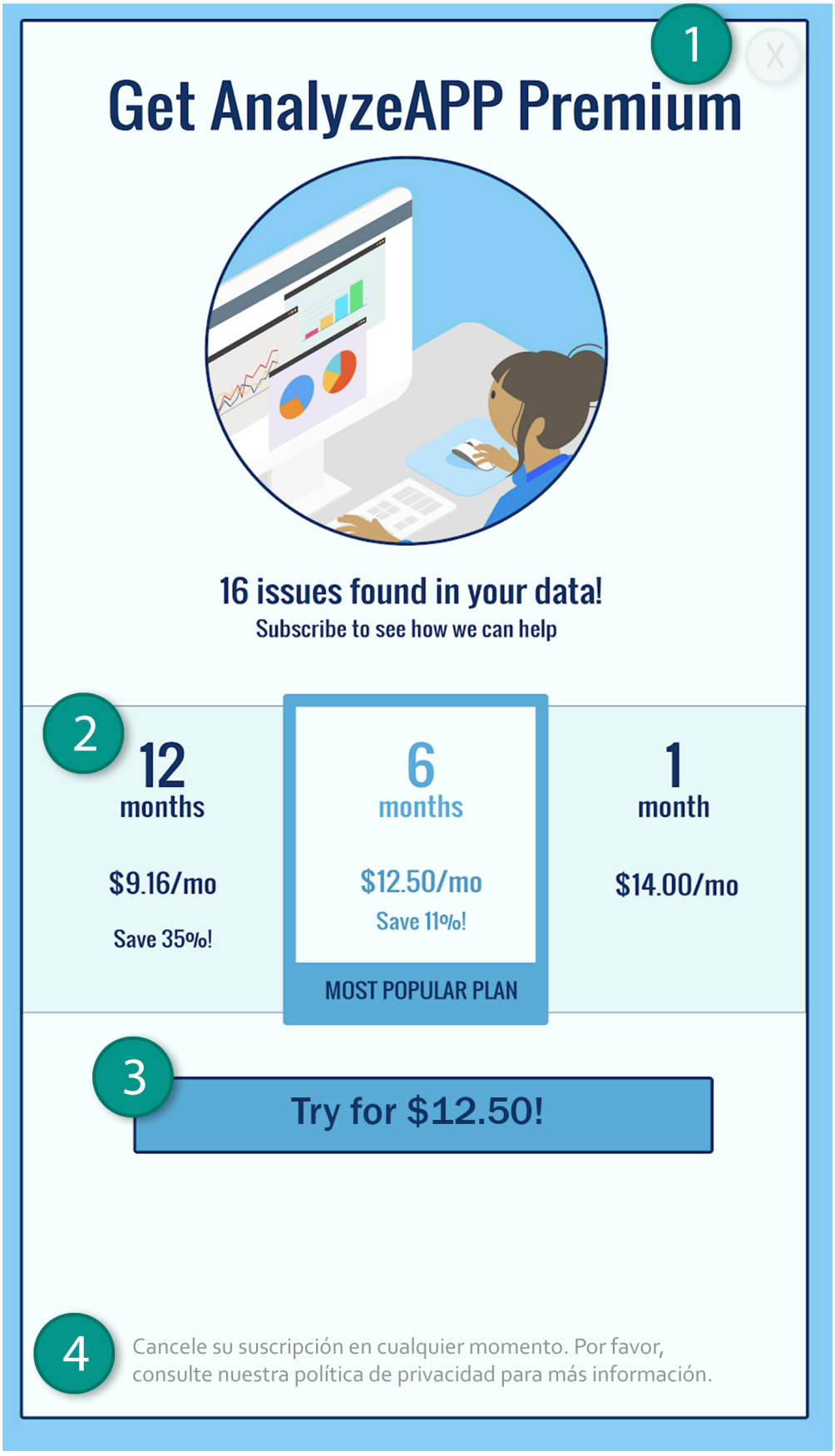
Abbonamenti

In qualità di sviluppatore, devi evitare di 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: devi essere trasparente in merito alla tua 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.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 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.

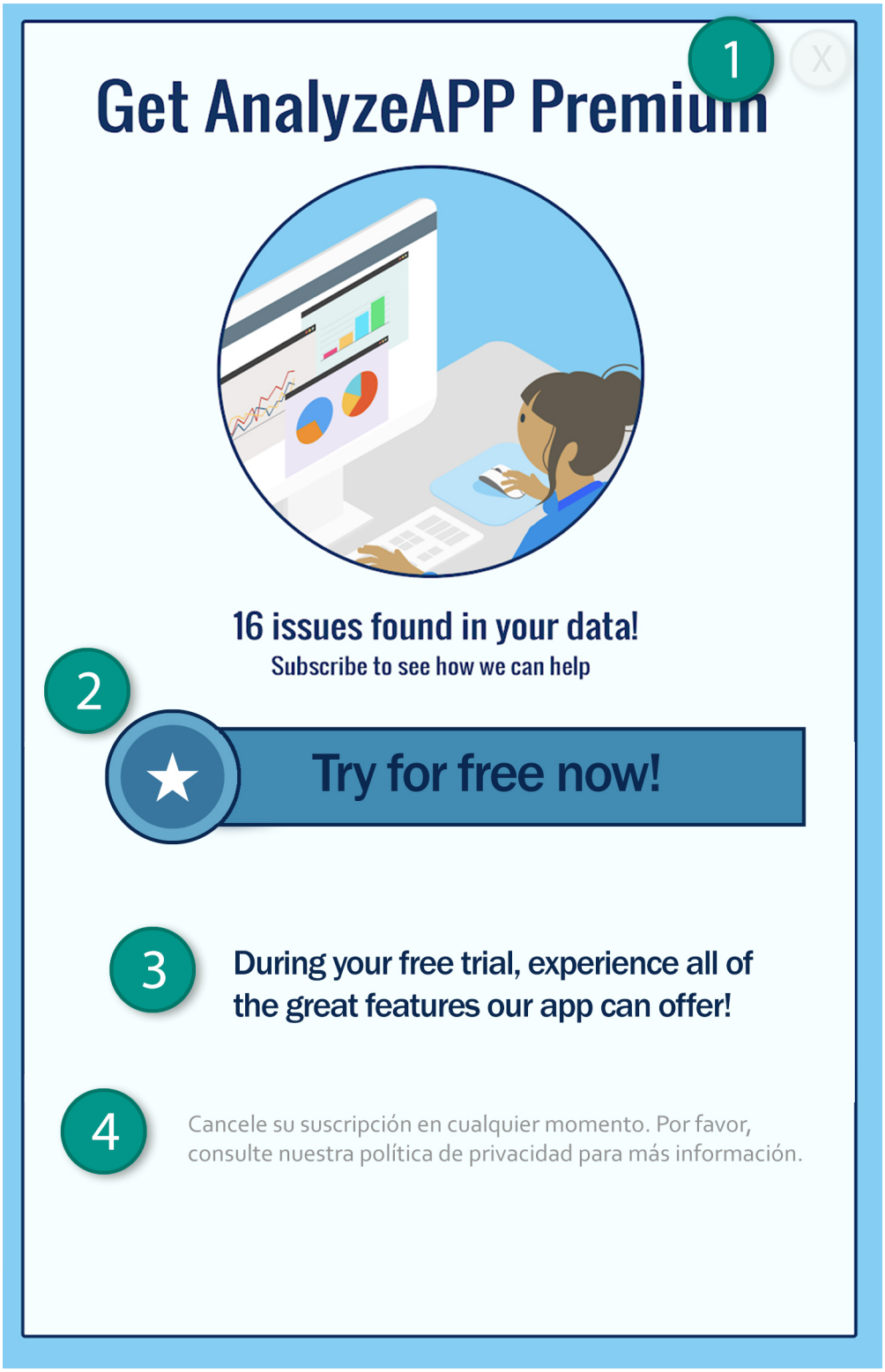
④ L'offerta deve essere localizzata nella stessa lingua dei termini e condizioni, in modo tale che gli utenti possano comprendere l'offerta completa.

Prove gratuite e offerte di lancio

Prima che un utente attivi l'abbonamento offerto dall'app: devi 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. Devi assicurarti 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.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 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 cancellazione degli abbonamenti

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

È tua responsabilità informare gli utenti in merito a eventuali modifiche apportate alle norme su abbonamento, cancellazione e rimborsi e assicurarti che tali norme siano conformi alla legge vigente.

Annunci

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 consultare 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 su autorizzazione per la pubblicazione di annunci sono soggette alle norme relative alle Informazioni personali e dati sensibili e devono inoltre soddisfare i seguenti requisiti:

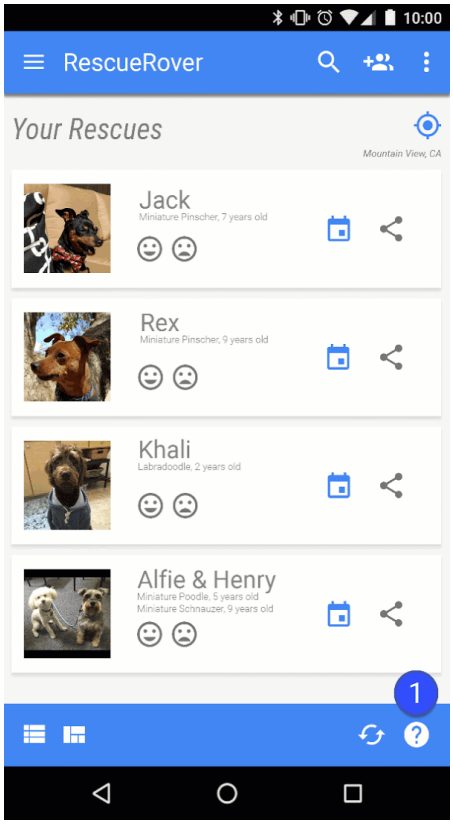
- L'utilizzo o la raccolta per scopi pubblicitari di dati sulla posizione del dispositivo basati su autorizzazione devono essere chiari all'utente e documentati nelle norme sulla privacy obbligatorie dell'app, incluso il collegamento a eventuali norme sulla privacy di reti pubblicitarie pertinenti, relative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

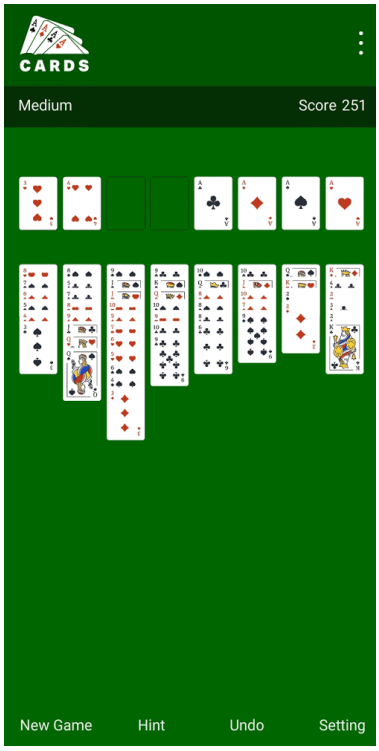
Di seguito sono riportati alcuni esempi di violazioni frequenti:

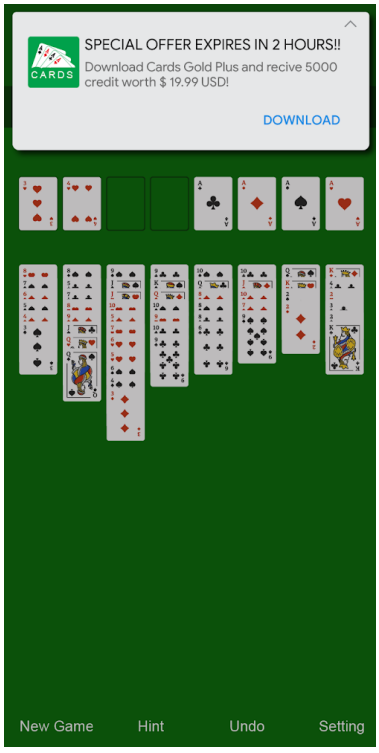
- Annunci che imitano l'interfaccia utente di un'app:



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:



- 

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 essere presenti annunci o funzionalità che monetizzano la schermata di blocco di un dispositivo.

Annunci improvvisi

Gli annunci improvvisi sono annunci che vengono mostrati agli utenti in modi imprevisti, che potrebbero generare clic involontari o compromettere o interferire con l'usabilità delle funzionalità del dispositivo.

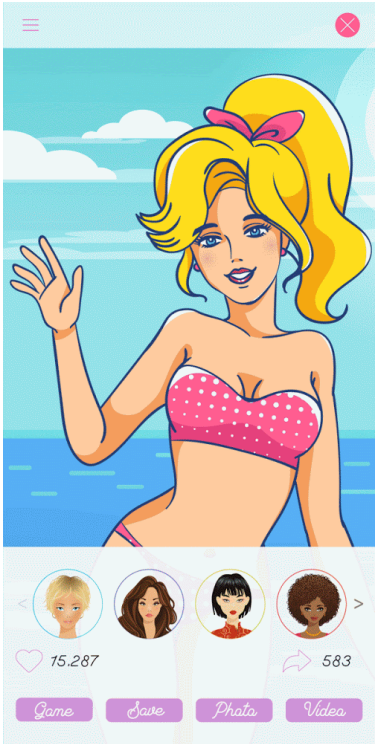
L'app non può obbligare un utente a fare clic su un annuncio o a inviare informazioni personali a scopi pubblicitari come condizione per poter utilizzare la funzionalità completa di un'app. Gli annunci interstitial possono essere mostrati solo all'interno dell'app che li pubblica. Se nell'app vengono mostrati annunci interstitial o altri annunci che interferiscono con il normale utilizzo, gli utenti devono poter ignorare facilmente gli annunci senza essere penalizzati.

Di seguito sono riportati alcuni esempi di violazioni comuni:

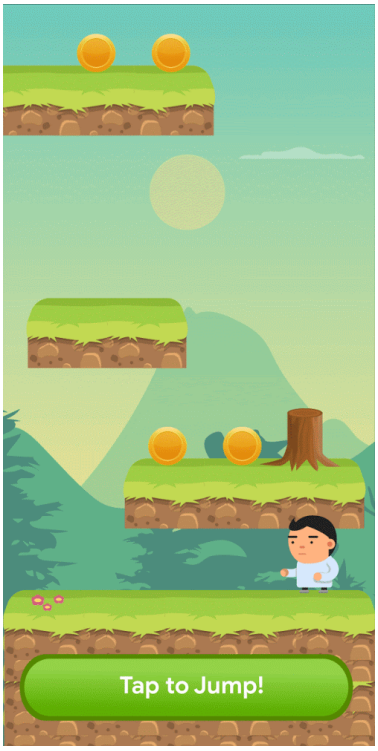
- Annunci che occupano tutto lo schermo o che interferiscono con il normale utilizzo, che non è chiaro come poter ignorare:

① Non è disponibile un pulsante per ignorare questo annuncio.

- Annunci che obbligano l'utente a eseguire il click-through usando un falso pulsante Ignora o facendo apparire improvvisamente gli annunci in aree dell'app che in genere l'utente tocca per accedere a un'altra funzionalità.



Un annuncio che utilizza un falso pulsante Ignora



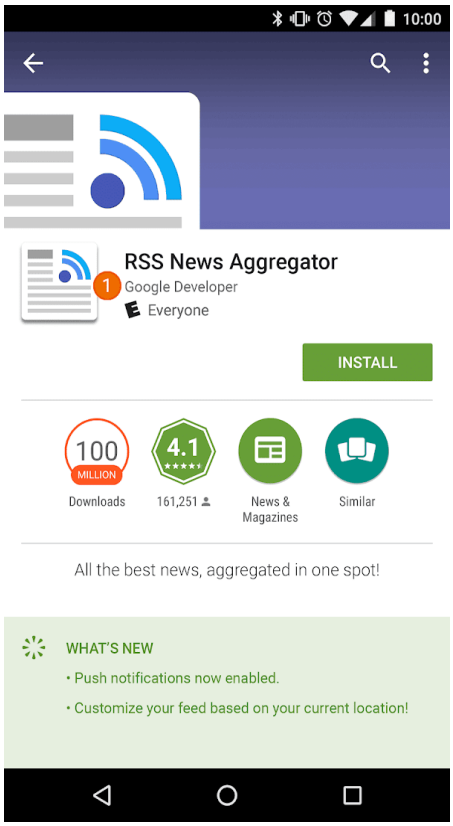
Un annuncio che appare all'improvviso in un'area che l'utente è abituato a toccare per accedere alle funzionalità in-app

Interferenze 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.

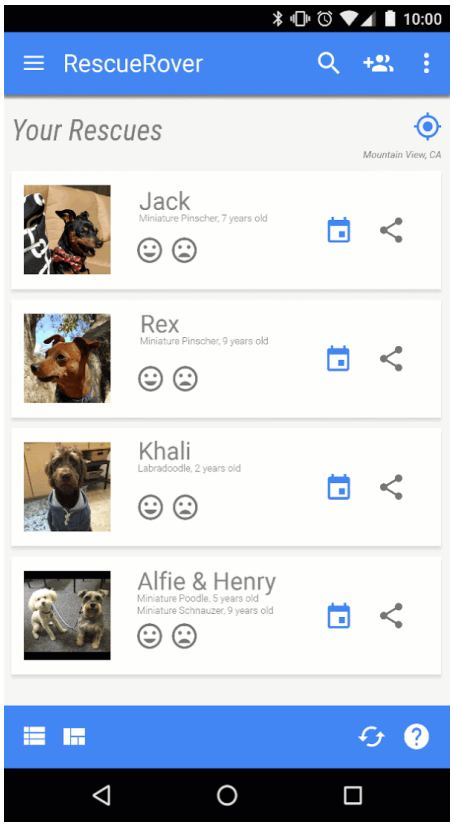
Di seguito sono riportati alcuni esempi di violazioni comuni:

- 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:

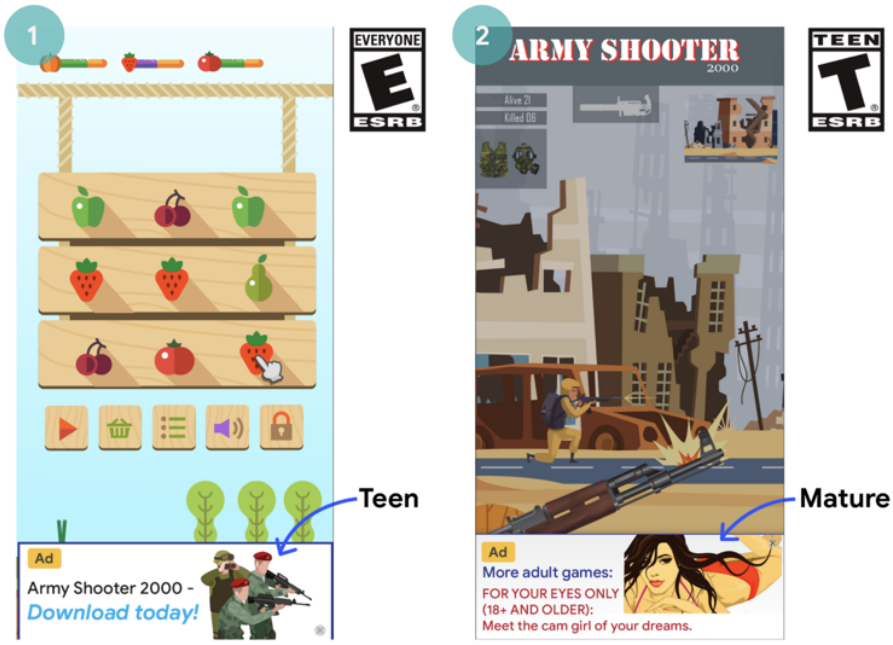


Descrizione: l'utente cerca di uscire dall'app e di accedere alla schermata Home, ma il flusso previsto viene interrotto da un annuncio.

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.

Di seguito è riportato un esempio di violazione frequente:



① Questo annuncio non è appropriato (adolescenti) per il pubblico previsto dell'app (7+)
② Questo annuncio non è appropriato (adulti) per il pubblico previsto dell'app (12+)

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'ID 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 che consentono l'identificazione personale o altri identificatori**
  - Utilizzo pubblicitario: l'ID pubblicità non può essere collegato a identificatori del dispositivo persistenti (ad esempio, SSAID, indirizzo MAC, IMEI e così via) per scopi pubblicitari. L'ID pubblicità può essere collegato a informazioni personali solo con il consenso esplicito dell'utente.
  - Utilizzo per scopi di analisi: l'ID pubblicità può essere collegato solo a informazioni che consentono l'identificazione personale o associato a un identificatore del dispositivo persistente (ad esempio, SSAID, indirizzo MAC, IMEI e così via) con il consenso esplicito dell'utente.
- **Rispetto delle scelte degli utenti**. In caso di reimpostazione, il nuovo ID pubblicità non deve essere collegato a un ID pubblicità precedente o a dati derivanti da un precedente ID pubblicità senza l'esplicito consenso dell'utente. Devi 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 puoi utilizzare l'ID 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'ID 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, consulta le norme relative ai Dati utente.
- **Rispetto dei termini e condizioni d'uso**. L'ID pubblicità può essere utilizzato esclusivamente in conformità con i presenti termini, anche dalle parti con cui tu lo condivida eventualmente nel corso della tua 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, devi 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 sia da bambini e ragazzi sia da utenti di età più elevata, devi implementare misure di controllo dell'età e assicurarti 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 rimani 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:

- Pubblicità autopromozionale qualora tu utilizzi SDK per gestire la promozione incrociata delle tue app o per altri contenuti multimediali di proprietà e merchandising
- Stipulazione di direct deal con gli inserzionisti qualora tu utilizzi SDK per la gestione dell'inventario

Requisiti di certificazione degli SDK di annunci

- Definire il contenuto dell'annuncio e i comportamenti discutibili e vietarli nei termini o nelle norme dell'SDK di annunci. Le definizioni devono essere conformi alle Norme del programma per gli sviluppatori di Google Play.
- Creare un metodo per classificare le creatività degli annunci in base alle fasce d'età appropriate. Queste ultime devono includere 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 gli sviluppatori abbiano compilato il modulo di interesse riportato di seguito.
- Consenti ai publisher, in base alle singole richieste o per app, di richiedere un 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. Google Play richiede agli SDK di annunci di disattivare annunci personalizzati, pubblicità basata sugli interessi e remarketing nell'ambito del trattamento per siti o servizi destinati ai minori.
- Consenti ai publisher di selezionare formati degli annunci conformi alle Norme relative agli Annunci per le famiglie e alla monetizzazione di Play e che soddisfano i requisiti del programma App approvate dagli insegnanti.
- Assicurati 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.
- Fornisci a Google informazioni sufficienti, come quelle indicate nel modulo di interesse riportato di seguito, 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 conforme a tutte le leggi e i regolamenti pertinenti relativi a bambini e ragazzi che possano applicarsi ai rispettivi publisher.

Requisiti di mediazione per le piattaforme di pubblicazione in caso di pubblicazione di annunci destinati ai minori:

- Utilizza solo SDK di annunci certificati Google Play o implementa le misure di protezione necessarie per garantire che tutti gli annunci pubblicati dalle reti di mediazione siano conformi a tali requisiti; e inoltre
- Trasmetti le informazioni necessarie alle piattaforme di mediazione 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 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.
- Tecniche di promozione o installazione che reindirizzano gli utenti a Google Play o al download di app senza un'azione informata da parte dell'utente.
- Promozione non richiesta tramite servizi SMS.

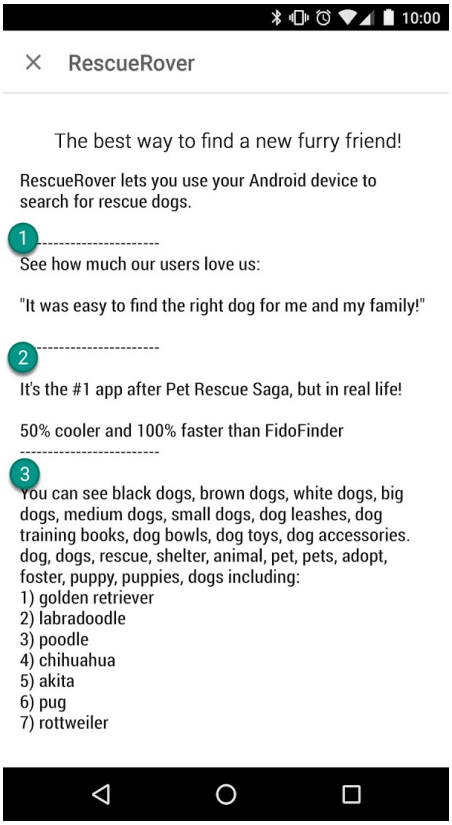
Devi assicurarti che tutte le reti pubblicitarie o gli affiliati associati alla tua app si adeguino alle presenti norme e non adottino pratiche di promozione vietate.

Metadati

Sono vietate le app contenenti metadati fuorvianti, non correttamente formattati, non descrittivi, irrilevanti, eccessivi o inappropriati che siano contenuti, a titolo esemplificativo ma non esaustivo, 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 della loro app. Inoltre nella descrizione dell'app non sono consentite testimonianze degli utenti prive di attribuzione o anonime.

Oltre ai requisiti qui indicati, norme per gli sviluppatori di Play specifiche potrebbero richiedere di fornire ulteriori informazioni sui metadati.

Di seguito sono riportati alcuni esempi di violazioni frequenti:



① Testimonianze degli utenti anonime o prive di attribuzione
② Confronti relativi a dati tra 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 sessualmente allusivi. Evita di utilizzare immagini allusive che mostrino seni, natiche, genitali o altri contenuti/parti anatomiche oggetto di feticismo, sia illustrati sia reali.
- Utilizzo di linguaggio volgare o comunque non appropriato per un pubblico generico nella scheda dello Store dell'app.
- Violenza esplicita mostrata in evidenza nelle icone delle app, nelle immagini promozionali o nei video.
- Raffigurazioni dell'utilizzo illegale di droghe. Anche i contenuti EDSA (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:

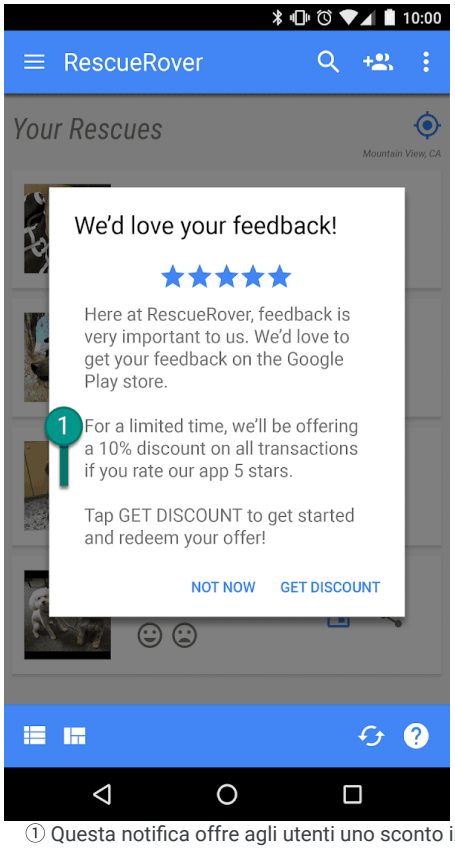
- Evidenzia gli aspetti migliori dell'app. Condividi con gli utenti fatti interessanti e coinvolgenti relativi all'app per aiutarli a capire che cosa la rende speciale.
- Assicurati che il titolo e la descrizione dell'app ne illustrino in modo accurato la funzionalità.
- Evita di utilizzare parole chiave 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. Lunghezza o dettagli eccessivi o formattazione non valida potrebbero costituire una violazione di queste norme.
- Tieni presente che la scheda deve essere adatta a un pubblico generico. Evita di utilizzare testo, immagini o video inappropriati nella scheda e attieniti alle linee guida riportate in precedenza.

Valutazioni degli utenti, recensioni e installazioni

Gli sviluppatori non devono tentare di manipolare il posizionamento di qualsiasi app su Google Play. È vietato quindi, a titolo esemplificativo ma non esaustivo, incrementare artificialmente 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.

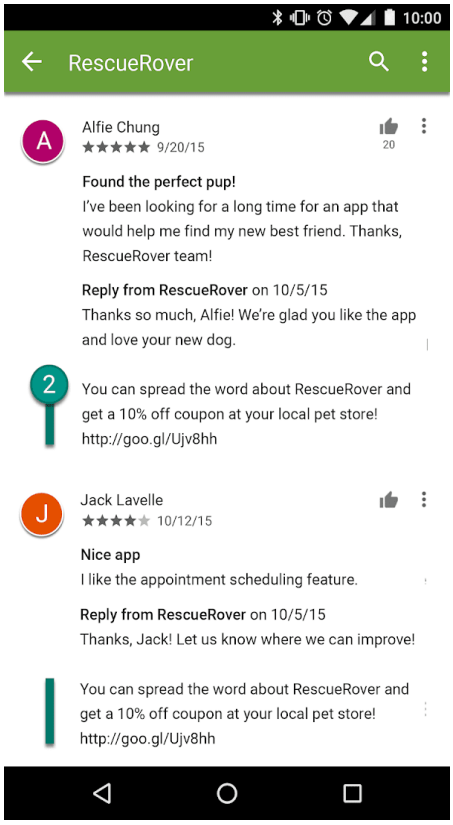
Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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

Le classificazioni dei contenuti su Google Play sono fornite dall'IARC (International Age Rating Coalition) e sono concepite per aiutare gli sviluppatori a comunicare agli utenti le classificazioni dei contenuti pertinenti a livello locale. Le autorità IARC regionali definiscono linee guida utilizzate per determinare il livello di maturità dei contenuti in un'app. Su Google Play non sono consentite app senza classificazione dei contenuti.

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 una classificazione dei contenuti devi compilare un questionario per la classificazione dell'app in Play Console che chiede informazioni sulla natura dei contenuti delle tue 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 dell'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 indicata come "Non classificata", devi compilare il questionario per la classificazione dei contenuti per ogni nuova app inviata a Play Console e per tutte le app esistenti che sono attive su Google Play.

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

Visita il Centro assistenza per ulteriori informazioni sulle diverse autorità di classificazione e su come completare il questionario per la classificazione dei contenuti.

Ricorsi contro le classificazioni

Qualora tu non sia d'accordo con la classificazione assegnata all'app, puoi presentare un ricorso direttamente all'autorità di classificazione IARC utilizzando il link disponibile nel certificato inviato via email.

Notizie

Un'app per cui viene dichiarato che si tratta di un'app di "notizie" su Google Play deve rispettare tutti i requisiti che seguono.

Le app di notizie che richiedono agli utenti di acquistare un abbonamento devono fornire un'anteprima dei contenuti prima dell'acquisto.

Le app di notizie DEVONO:

- Dare informazioni sulla proprietà relative all'editore giornalistico e ai suoi collaboratori inclusi, a titolo esemplificativo, il sito web ufficiale delle notizie pubblicate nell'app, informazioni di contatto valide e verificabili e l'editore originale di ogni articolo; e
- Avere un sito web o una pagina in-app che fornisca informazioni di contatto valide per l'editore giornalistico.

Le app di notizie NON DEVONO:

- Contenere errori ortografici o grammaticali significativi;
- Avere soltanto contenuti statici (ad esempio contenuti risalenti a diversi mesi prima della data corrente); e
- Avere come finalità principale l'affiliate marketing o le entrate pubblicitarie.

Le app di notizie che raccolgono contenuti di diverse fonti di pubblicazione devono essere trasparenti in merito alla fonte di pubblicazione dei contenuti nell'app; ogni fonte deve rispettare i requisiti delle norme relative alle notizie.

Spam e funzionalità minima

Come minimo, le app devono fornire agli utenti un livello di funzionalità di base e un'esperienza utente accettabile. Le app che presentano arresti anomali, altri comportamenti non coerenti con un'esperienza utente funzionale o che hanno il solo scopo di inviare spam agli utenti o a Google Play non sono considerate app che contribuiscono al catalogo in modo costruttivo.

Spam

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

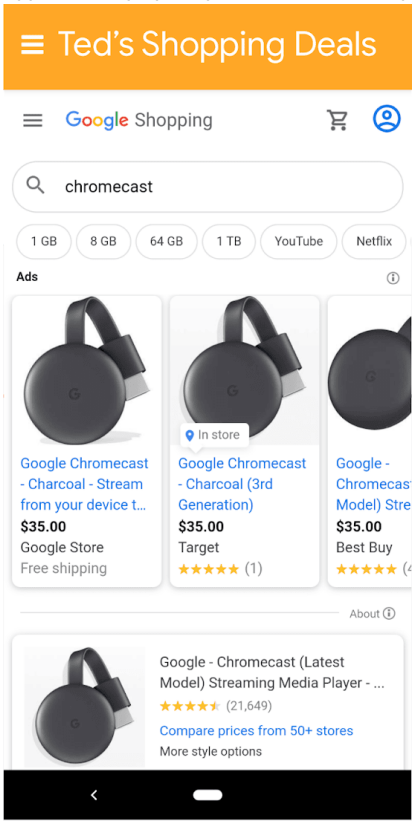
Spam legato alle visualizzazioni web e alle affiliazioni

Sono vietate le app il cui scopo principale è indirizzare traffico affiliato verso un sito web o fornire un componente WebView di un sito senza l'autorizzazione del proprietario o dell'amministratore del sito stesso.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 un componente WebView di un sito web senza autorizzazione:



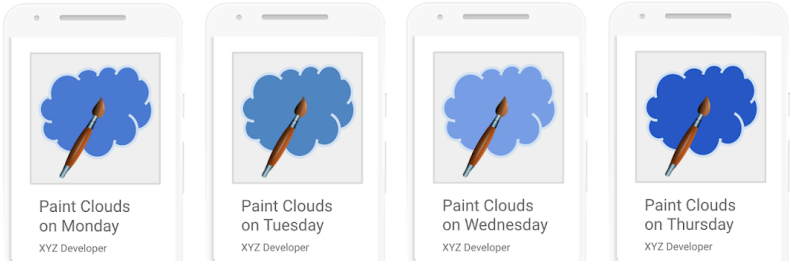
Questa app è denominata "Ted's Shopping Deal" e fornisce semplicemente una visualizzazione web di Google Shopping.

Contenuti ripetitivi

Sono vietate le app che si limitano a fornire la stessa esperienza di altre app già presenti su Google Play. Le app dovrebbero offrire valore agli utenti fornendo loro servizi o contenuti unici.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- Copia di contenuti di altre app senza aggiungere valore o contenuti originali.
- Creazione di più app con funzionalità, contenuti ed esperienze utente molto simili. Se il volume di contenuti di ogni singola app è ridotto, gli sviluppatori dovrebbero valutare la creazione di un'app unica che raccolga tutti i contenuti.



App realizzate appositamente per gli annunci

Sono vietate le app il cui scopo principale è pubblicare annunci.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- App in cui vengono inseriti annunci interstitial dopo ogni azione dell'utente inclusi, a titolo esemplificativo ma non esaustivo, clic, scorrimenti ecc.

Funzionalità minima

Assicurati che la tua app fornisca un'esperienza utente stabile, coinvolgente e reattiva.

Di seguito sono riportati alcuni esempi di violazioni comuni:

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

Funzioni inaccessibili

Sono vietate le app che si arrestano in modo anomalo, richiedono la chiusura forzata, si bloccano o comunque funzionano in maniera anomala.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 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 essere soggette anche a requisiti previsti da norme relative a programmi specifici. Assicurati di leggere l'elenco che segue per stabilire se una o più norme indicate si applicano alla tua app.

App istantanee Android

Abbiamo realizzato le app istantanee Android con lo scopo di offrire agli utenti esperienze piacevoli e senza attrito 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 per gli sviluppatori di Google Play.

Identità

Gli sviluppatori di app istantanee con funzionalità di accesso devono integrare la funzionalità 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 l'app installata o l'app istantanea dello sviluppatore contiene link che potrebbero rimandare a un'app istantanea, lo sviluppatore deve indirizzare gli utenti a tale app anziché, ad esempio, integrare i link in un componente WebView.

Specifiche tecniche

Gli sviluppatori devono rispettare le specifiche tecniche e i requisiti relativi alle app istantanee Android (come di tanto in tanto 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 il suo scopo principale. In caso di offerta di installazione, gli sviluppatori sono tenuti a quanto segue:

- Usare l'icona "get app" (scarica l'app) di Material Design e l'etichetta "Install" (installa) per il pulsante di installazione.
- Non includere 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'UX 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 la cui durata vada oltre quella della sessione dell'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 del fatto che l'app è in esecuzione sul proprio dispositivo.

Identificatori dei dispositivi

Le app istantanee non sono autorizzate ad accedere a 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 possono accedere al numero di telefono se ottenuto usando l'autorizzazione di runtime. 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, idonei per le fasce di età di destinazione e adatti a tutta la famiglia. Prima di inviare un'app per il programma Per la famiglia o 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.

Devi consultare le informazioni sul processo relativo al programma Per la famiglia e 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 attirare semplicemente la loro attenzione. Google Play aiuterà a garantire che siano sicure 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 ti aiuti a determinare gli eventuali obblighi e/o le restrizioni in base alle fasce d'età applicabili alla propria 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. Se la tua app si rivolge sia ai bambini sia a segmenti di pubblico di età superiore, puoi comunque partecipare al programma Per la famiglia. Tutte le app che partecipano al programma Per la famiglia saranno idonee a essere classificate per il programma App approvate dagli insegnanti, ma non possiamo garantire che verranno incluse nel programma. Se opti per 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 indicate. Indipendentemente dalla selezione effettuata in Google Play Console, qualora tu scelga di includere nell'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 tu selezioni un pubblico di destinazione che include solo gli adulti, ma Google ritenga tale indicazione non corretta perché l'app è destinata sia a bambini sia ad adulti, avrai la possibilità di chiarire agli utenti che l'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 dell'app soltanto se è stata 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 inferiore è necessario selezionare "Fino a 5 anni". Se l'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 l'app è stata pensata per utenti di tutte le età.

Aggiornamento della sezione Pubblico di destinazione e contenuti

Puoi sempre aggiornare le informazioni relative all'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 che venga presentato un aggiornamento dell'app.

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

Rappresentazione ingannevole in Play Console

La rappresentazione ingannevole di qualsiasi informazione inerente l'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 relativi alle norme sulle famiglie

Se i bambini sono inclusi nel pubblico di destinazione dell'app, devi rispettare gli obblighi seguenti. Il mancato rispetto di tali obblighi 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:** devi rispondere con precisione alle domande relative alla tua app contenute in Google Play Console e ad aggiornare tali risposte per riflettere con precisione qualsiasi modifica apportata all'app.
3. **Annunci:** se l'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;
   - Garantire che gli annunci mostrati a tali utenti non prevedano pubblicità basata sugli interessi (pubblicità indirizzata a singoli utenti che hanno determinate caratteristiche sulla base del loro comportamento di navigazione online) o remarketing (pubblicità indirizzata a singoli utenti sulla base di interazioni precedenti con un'app o un sito web);
   - 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; e infine
   - Garantire la conformità a tutte le normative e gli standard di settore applicabili in materia di pubblicità destinata ai bambini.
4. **Raccolta dati:** devi divulgare la raccolta di eventuali informazioni personali e sensibili relative a bambini e ragazzi nell'app, compresa la raccolta tramite API e SDK richiamati o utilizzati nell'app medesima. Le informazioni sensibili relative 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:** devi assicurarti 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 minori 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 dai bambini (ad esempio, fornendo il servizio Accedi con Google come funzionalità facoltativa). Le app destinate sia a minori sia a un pubblico di età più elevata non devono richiedere agli utenti di eseguire l'accesso o accedere ai contenuti tramite un'API o un SDK non approvato per l'utilizzo nei servizi rivolti ai minori.
6. **Norme sulla privacy:** devi 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 l'app utilizza la realtà aumentata, dovrai includere un avviso di sicurezza che venga visualizzato contestualmente 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).

- L'app non deve richiedere l'utilizzo di dispositivi sconsigliati per l'uso da parte dei bambini (ad esempio Daydream, Oculus).

8. **Conformità legale:** devi 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.

Di seguito sono riportati alcuni esempi di violazioni frequenti:

- 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 i cui termini di servizio 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 contengono link a siti web che presentano contenuti che violano le Norme del programma per gli sviluppatori di Google Play.
- App che mostrano ai bambini annunci destinati a un pubblico adulto (ad esempio, contenuti violenti, di natura sessuale o collegati a giochi e scommesse). Per ulteriori informazioni sulle Norme di Google Play relative alla pubblicità, agli acquisti in-app e ai contenuti commerciali destinati ai minori, consulta le Norme relative agli Annunci per le famiglie e alla monetizzazione.

Programma Per la famiglia

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

Per poter essere accettata nel programma, l'app deve essere conforme a tutti i requisiti di cui alle 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 può rifiutare, rimuovere o sospendere qualsiasi app ritenuta non appropriata 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. Devi specificare 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 Companion Device Manager (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
- App che utilizzano un'icona dell'app o un'icona in Avvio applicazioni non appropriata per i minori

Categorie

Se vieni ammesso a partecipare al programma Per la famiglia potrai scegliere una seconda categoria specifica del 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, giochi di 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 presente nell'app, inclusi annunci per le app tue e di terze parti, offerte di acquisti in-app o qualsiasi altro contenuto commerciale (come il posizionamento di prodotti a pagamento), offerto agli utenti di app soggette ai requisiti delle Norme per le famiglie e/o ai requisiti del programma Per la famiglia. Tutti gli annunci, le offerte di acquisti in-app e i contenuti commerciali presenti in queste app devono essere conformi alle leggi e normative vigenti (incluse eventuali indicazioni di settore o di autoregolamentazione pertinenti).

Google Play si riserva il diritto di rifiutare, rimuovere o sospendere le app in caso di tattiche commerciali eccessivamente aggressive.

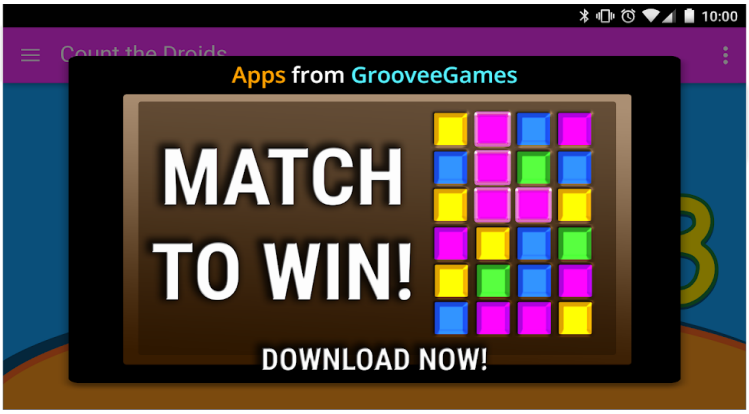
Requisiti relativi al formato degli annunci

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

- Annunci improvvisi, inclusi gli annunci che occupano l'intero schermo o che interferiscono con il normale utilizzo e non forniscono un modo chiaro per ignorarli (ad esempio, Barriere di annunci)
- Annunci che interferiscono con il normale gameplay o utilizzo dell'app e che non possono essere chiusi dopo 5 secondi. Gli annunci che non interferiscono con il normale gameplay o utilizzo dell'app possono rimanere visualizzati per più di 5 secondi (ad esempio, contenuti video con annunci integrati).
- Offerte o annunci interstitial per l'acquisto in-app visualizzati contestualmente all'avvio dell'app
- Più posizionamenti dell'annuncio in una pagina (ad esempio, sono vietati annunci banner che mostrano più offerte nello stesso posizionamento o più banner o annunci video).
- 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
- Mancata distinzione tra l'uso di monete di giochi virtuali rispetto a soldi reali per effettuare acquisti in-app

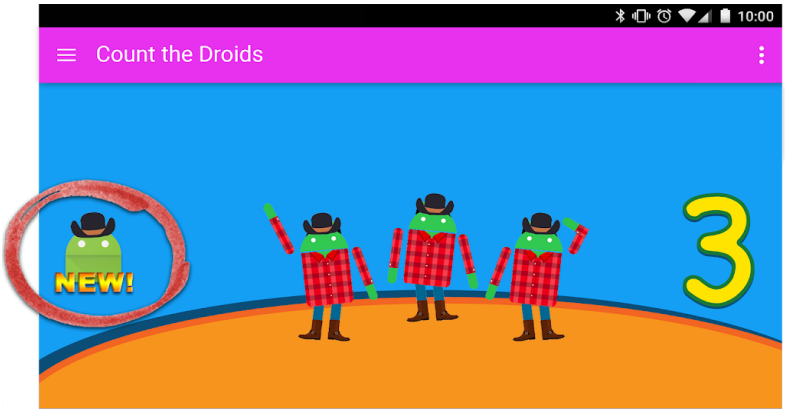
Di seguito sono riportati alcuni esempi di violazioni comuni relative ai formati degli annunci

- 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:

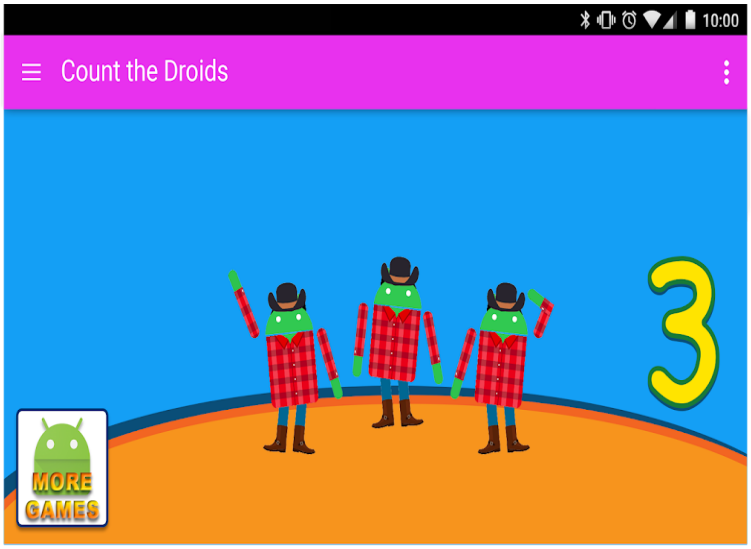


- Annunci banner che mostrano più offerte, come illustrato nell'esempio seguente:

- 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

Se pubblichi annunci nella tua app e questa è destinata soltanto un pubblico di minori, devi utilizzare SDK degli annunci certificati di Google Play. Se il pubblico di destinazione dell'app è costituito da bambini e ragazzi e da utenti di età più elevata, devi implementare misure di controllo dell'età, come un filtro di controllo dell'età e assicurarti che gli annunci mostrati ai bambini provengano esclusivamente dagli SDK di annunci certificati di Google Play. Per le app del programma Per la famiglia è necessario utilizzare soltanto SDK di annunci autocertificati.

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

Se utilizzi AdMob, dovrai fare riferimento al Centro assistenza AdMob per ulteriori informazioni sui prodotti.

È tua responsabilità garantire che l'app soddisfi tutti i requisiti relativi a pubblicità, acquisti in-app e contenuti commerciali. Contatta il fornitore 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 a posteriori ma, qualora si verifichino, ci impegniamo ad assicurare che gli sviluppatori sappiano come rendere conformi le loro app dopo una violazione. 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 del tuo account sviluppatore mostrato pubblicamente su Google Play, inclusi il tuo nome sviluppatore e la pagina di destinazione del tuo sito web dello sviluppatore specificato.

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 funzionalità ed esperienze offerte da terze parti, devono garantire che tutti i contenuti a cui forniscono l'accesso siano conformi a tutte le norme di Google Play; possono inoltre 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). Oltre a rispettare queste norme e il Contratto di distribuzione per gli sviluppatori, i contenuti dell'app devono essere classificati in conformità con le nostre Linee guida per la classificazione dei contenuti.

Nel valutare se includere o rimuovere un'app da Google Play, prendiamo in considerazione una serie di fattori tra cui, a titolo esemplificativo ma non esaustivo, un comportamento dannoso ricorrente o un rischio elevato di comportamento illecito. Identifichiamo il rischio di comportamento illecito utilizzando elementi quali, a titolo esemplificativo ma non esaustivo, la cronologia delle violazioni precedenti, il feedback degli utenti, l'uso di brand e personaggi noti e altre risorse.

Funzionamento di Google Play Protect

Google Play Protect controlla le app al momento dell'installazione. Inoltre esegue periodicamente la scansione del dispositivo. Se rileva un'app potenzialmente dannosa, potrebbe:

- Inviare una notifica. Per rimuovere l'app, tocca la notifica, quindi tocca Disinstalla.
- Disattivare l'app fino a quando non viene disinstallata.
- Rimuovere automaticamente l'app: nella maggior parte dei casi, quando viene rilevata un'app dannosa, ricevi una notifica che comunica che l'app è stata rimossa.

Funzionamento della protezione antimalware

Per proteggerti da URL e software dannosi di terze parti e da altri problemi di sicurezza, Google potrebbe ricevere informazioni su:

- Connessioni di rete del dispositivo
- URL potenzialmente dannosi
- Sistema operativo e app installate sul dispositivo tramite Google Play o altre origini

Potresti ricevere un avviso da Google che segnala un'app o un URL potenzialmente non sicuri. Google potrebbe rimuovere l'URL o l'app oppure bloccarne l'installazione, qualora sia noto che l'app o l'URL sono dannosi per dispositivi, dati o utenti.

Puoi scegliere di disattivare alcune di queste protezioni nelle impostazioni del dispositivo. Tuttavia Google potrebbe continuare a ricevere informazioni sulle app installate tramite Google Play e le app installate sul dispositivo da altre fonti potrebbero continuare a essere controllate per individuare problemi di sicurezza, senza l'invio di informazioni a Google.

Funzionamento degli avvisi sulla privacy

Google Play Protect ti avvisa se un'app viene rimossa dal Google Play Store perché potrebbe accedere alle tue informazioni personali; avrai la possibilità di disinstallare l'app.

Procedura di applicazione

Se la tua app viola una delle nostre norme, prenderemo le misure opportune, come descritto di seguito. Inoltre, ti forniremo via email informazioni pertinenti sull'azione che abbiamo intrapreso, insieme alle istruzioni su come presentare ricorso se ritieni che ci sia stato un errore.

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 delle norme in tutte le tue app potrebbe comportare ulteriori provvedimenti.

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 (DDA) comporteranno la chiusura di account sviluppatore Google Play singoli o correlati.

Provvedimenti

I diversi provvedimenti possono influire sulla tua app in modi altrettanto differenti. La seguente sezione descrive le varie azioni che Google Play potrebbe intraprendere e il relativo impatto sull'app e/o sul tuo account sviluppatore Google Play. Queste informazioni sono spiegate anche in questo video.

Rifiuto

- Su Google Play non verranno resi disponibili le nuove app o gli aggiornamenti dell'app inviati per la revisione.
- Se un aggiornamento di un'app esistente viene rifiutato, la versione dell'app pubblicata prima di tale aggiornamento rimane disponibile su Google Play.
- I rifiuti non influiscono sul tuo accesso alle installazioni, alle statistiche e alle valutazioni esistenti degli utenti relative all'app rifiutata.
- I rifiuti non influiscono sulla reputazione del tuo account sviluppatore Google Play.

Ti ricordiamo di non inviare nuovamente un'app rifiutata prima di aver risolto tutte le violazioni delle norme.

Rimozione

- L'app e le eventuali versioni precedenti vengono rimosse da Google Play e non saranno più disponibili per il download.
- Poiché l'app viene rimossa, gli utenti non potranno visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app. Queste informazioni verranno ripristinate una volta che avrai inviato un aggiornamento conforme alle norme per l'app rimossa.
- Gli utenti potrebbero non essere in grado di effettuare acquisti in-app o utilizzare funzionalità di fatturazione in-app finché una versione conforme alle norme non verrà approvata da Google Play.
- Le rimozioni non influiscono immediatamente sulla reputazione del tuo account sviluppatore Google Play, ma rimozioni multiple potrebbero comportare la sospensione dell'account.

Nota: non tentare di ripubblicare un'app rimossa fino a quando tutte le violazioni delle norme non saranno state risolte.

Sospensione

- L'app e le eventuali versioni precedenti vengono rimosse da Google Play e non saranno più disponibili per il download.
- La sospensione può verificarsi a causa di violazioni delle norme gravi o ripetute, nonché di rimozioni o rifiuti ripetuti di app.
- Poiché l'app è sospesa, gli utenti non potranno visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni esistenti dell'app. Queste informazioni verranno ripristinate una volta che avrai inviato un aggiornamento conforme alle norme.
- Non potrai più utilizzare l'APK o l'app bundle di un'app sospesa.
- Gli utenti non saranno in grado di effettuare acquisti in-app o utilizzare funzionalità di fatturazione in-app finché una versione conforme alle norme non verrà approvata da Google Play.
- Le sospensioni incidono, in qualità di avvertimenti, sulla buona reputazione del tuo account sviluppatore Google Play. Più avvertimenti possono comportare la chiusura degli account sviluppatore Google Play individuali e correlati.

Nota: non tentare di ripubblicare un'app sospesa a meno che Google Play non ti abbia indicato che puoi farlo.

Visibilità limitata

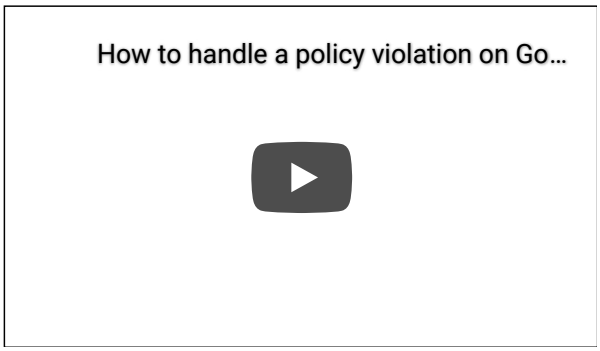
- La rilevabilità dell'app su Google Play è limitata. L'app rimarrà disponibile su Google Play e sarà accessibile agli utenti con un link diretto alla scheda del Play Store dell'app.
- Lo stato di Visibilità limitata dell'app non influisce sulla buona reputazione del tuo account sviluppatore Google Play.
- Lo stato di Visibilità limitata non incide sulla capacità degli utenti di visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app esistenti.

Chiusura dell'account

- Quando il tuo account sviluppatore viene chiuso, tutte le app nel tuo catalogo verranno rimosse da Google Play e non potrai più pubblicare nuove app. Ciò significa anche che qualsiasi account sviluppatore Google Play correlato verrà sospeso definitivamente.
- Sospensioni ripetute o relative a violazioni gravi delle norme potrebbero comportare la chiusura del tuo account Play Console.
- Poiché le app all'interno dell'account chiuso vengono rimosse, gli utenti non saranno in grado di visualizzare la scheda dello Store, le installazioni, le statistiche e le valutazioni dell'app esistenti.

Nota: anche tutti i nuovi account che tenterai di aprire verranno chiusi (senza rimborso della quota di registrazione sviluppatore) quindi, se sei titolare di un account chiuso, non tentare di registrare un nuovo account Play Console.

Gestione e segnalazione di violazioni delle norme



Ricorso contro un provvedimento

Ripristineremo le applicazioni se è stato commesso un errore ed emerge che la tua applicazione non vìola le norme del programma di Google Play e il Contratto di distribuzione per gli sviluppatori. Se, dopo aver esaminato attentamente le norme, ritieni che la nostra decisione possa essere stata presa erroneamente, dovrai seguire le istruzioni fornite nell'email di notifica dell'applicazione per presentare ricorso.

Altre risorse

Per ulteriori informazioni riguardanti un provvedimento o una valutazione/un commento di un utente, puoi consultare alcune delle risorse riportate di seguito o contattarci tramite il Centro assistenza Google Play. Non siamo, tuttavia, in grado di fornire consulenza legale, per la quale dovrai rivolgerti a un consulente legale di fiducia.

- Verifica delle app e ricorsi
- Come segnalare la violazione di una norma
- Contattare Google Play in merito alla chiusura dell'account o alla rimozione di app
- Avvisi imparziali
- Segnalare app e commenti inappropriati
- La mia app è stata rimossa da Google Play
- Informazioni sulla chiusura degli account sviluppatore Google Play