Google Developer Policy - April 16, 2020

आइए, ऐप्लिकेशन और गेम के लिए दुनिया का सबसे सुरक्षित प्लैटफ़ॉर्म बनाएं

आपके नए तरह के बनाए गए ऐप्लिकेशन, आपकी और हमारी सफलता को आगे बढ़ाते हैं. हालांकि, इसके साथ नई ज़िम्मेदारियां भी आती हैं. डेवलपर कार्यक्रम की इन नीतियों और डेवलपर वितरण अनुबंध से यह पक्का होता है कि हम साथ मिलकर दुनिया के सबसे अनोखे और सुरक्षित ऐप्लिकेशन, Google Play की मदद से करोड़ों लोगों तक पहुंचाते रहें. हम चाहते हैं कि आप नीचे दी गई हमारी नीतियों के बारे में ज़्यादा जानें. आप नीतियों का प्रिंट व्यू भी देख सकते हैं.

People from all over the world use Google Play to access apps and games every day. Before submitting an app, ask yourself if your app is appropriate for Google Play and compliant with local laws.

बच्चों को खतरा

जिन ऐप्लिकेशन में नाबालिगों को यौन नज़रिए से दिखाने वाला कॉन्टेंट होता है उन्हें 'Play स्टोर' से तुरंत हटा दिया जाता है. उन ऐप्लिकेशन को अनुमति नहीं दी जाती जो बच्चों को पसंद आते हैं, लेकिन उनमें वयस्कों वाली थीम होती है.

अगर हमें बच्चों का यौन शोषण दिखाने वाले कॉन्टेंट के बारे में पता चलता है, तो हम उचित अधिकारियों से इसकी शिकायत करेंगे. साथ ही, इस तरह के ऐप्लिकेशन को उपयोगकर्ताओं तक पहुंचाने वाले लोगों के Google खाते भी मिटा देंगे.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

यौन सामग्री

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें पोर्नोग्राफ़ी जैसा सेक्शुअल कॉन्टेंट या कोई भी ऐसा कॉन्टेंट या सेवाएं होती हैं जिनका इरादा यौन रूप से खुश करना हो या ऐसे ऐप्लिकेशन जो इनका प्रचार करते हैं. नग्नता वाली सामग्री को अनुमति दी जा सकती है, लेकिन उसका मुख्य मकसद शैक्षणिक, डॉक्यूमेंट्री, वैज्ञानिक या कलात्मक होना चाहिए. इसके अलावा, यह कॉन्टेंट ऐप्लिकेशन में बेवजह शामिल नहीं होना चाहिए.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

> नग्नता को इस तरह से दिखाना जिसमें दिखाए जाने वाला व्यक्ति नग्न हो या उसने बहुत कम कपड़े पहने हों. साथ ही, किसी सार्वजनिक जगह के हिसाब से ऐसे कपड़े सही न हों.

यौन कृत्यों या यौन रूप से अश्लील मुद्राओं को दिखाना, ऐनिमेशन, या उदाहरण.
यौन विज्ञापन और कामोत्तेजक चीज़ें दिखाने वाली सामग्री.
ऐसा कॉन्टेंट जो कामुक है या धर्म का अपमान करता है.
पशुओं के साथ यौन गतिविधि दिखाने, इसके बारे में जानकारी देने या इसे बढ़ावा देने वाला कॉन्टेंट.
वे ऐप्लिकेशन जो सेक्स से जुड़े मनोरंजन, एस्कॉर्ट सेवाओं या ऐसी दूसरी सेवाओं का प्रचार करते हैं जिन्हें पैसे के बदले में यौन क्रियाएं देने वाली सेवा समझा जा सकता है.

अभद्र भाषा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी व्यक्ति या समूह के प्रति उनकी नस्ल या जातीय मूल, धर्म, दिव्यांगता, उम्र, राष्ट्रीयता, सैन्य सेवा के अनुभव, यौन रुझान, लिंग, लैंगिक पहचान, सामाजिक भेदभाव या अधिकार छीनने से जुड़ी दूसरी बातों की वजह से नफ़रत फैलाते हैं या उनके ख़िलाफ़ हिंसा को बढ़ावा देते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे दावों के संग्रह जिनका इरादा यह साबित करना है कि कोई संरक्षित समूह अमानवीय, सामाजिक तौर पर कमतर या नफ़रत के लायक है.
ऐसे ऐप्लिकेशन जिनमें किसी सुरक्षित समूह के बारे में नकारात्मक (जैसे कि नुकसान पहुंचाने वाला, भ्रष्ट, बुरा वगैरह) बातें कहीं गई हैं या फिर साफ़ तौर पर या किसी दूसरे तरीके से यह दावा किया गया है कि यह समूह एक खतरा है.
ऐसा कॉन्टेंट या भाषण जो दूसरों को यह मानने के लिए बढ़ावा देता है कि लोगों से नफ़रत या भेदभाव किया जाना चाहिए, क्योंकि वे किसी संरक्षित समूह के सदस्य हैं.

हिंसा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें गैर-ज़रूरी हिंसा या दूसरी खतरनाक गतिविधियों को दिखाया जाता है या जो ऐसा करने को बढ़ावा देते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

किसी भी व्यक्ति या पशु के ख़िलाफ़ वास्तविक हिंसा या हिंसक धमकियों को ग्राफ़िक की मदद से दिखाना या उनके बारे में जानकारी देना.
ऐसे ऐप्लिकेशन जो खुद को नुकसान पहुंचाने, खुदकुशी करने, खाने से जुड़ी बीमारियां, चोकिंग गेम या ऐसी दूसरी गतिविधियों का प्रचार करते हैं जिनसे गंभीर चोट लग सकती है या किसी की जान भी जा सकती है.

आतंकवाद से जुड़ा कॉन्टेंट

हम आतंकवादी संगठनों को किसी भी काम के लिए Google Play पर ऐप्लिकेशन प्रकाशित नहीं करने देते, इसमें भर्ती करना भी शामिल है.

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें आतंकवाद से जुड़ी सामग्री होती है, जैसे कि आंतकी गतिविधियों को बढ़ावा देने, हिंसा करने के लिए उकसाने या आतंकी हमलों का जश्न मनाने की सामग्री. अगर आप शिक्षा, डॉक्यूमेंट्री, विज्ञान या कला को ध्यान में रखकर आतंकवाद से जुड़ा कॉन्टेंट पोस्ट कर रहे हैं, तो ध्यान रखें कि आप इतनी जानकारी ज़रूर दें कि इसका इस्तेमाल करने वाले यह समझ सकें कि किस बारे में बात हो रही है.

संवेदनशील ईवेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो प्राकृतिक आपदा, क्रूरता, झगड़ा, मौत या किसी दूसरी दुखद घटना को लेकर उचित संवेदनशीलता नहीं दिखाते या उसका फ़ायदा उठाने की कोशिश करते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- आत्महत्या, दवा की ज़्यादा मात्रा, प्राकृतिक कारणों वगैरह की वजह से किसी व्यक्ति या समूह में लोगों की मौत होने से जुड़ी संवेदनशीलता में कमी.
- किसी बड़ी दुखद घटना को नकारना.
- ऐसी दुखद घटना से फ़ायदा उठाते दिखना जिसमें पीड़ितों को कोई सीधा फ़ायदा न मिला हो.

धमकाना और उत्पीड़न करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें धमकी देने, उत्पीड़न करने या प्रताड़ित करने जैसी बातें शामिल होती हैं या जो ऐसी चीज़ों को बढ़ावा देते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- अंतरराष्ट्रीय या धार्मिक टकरावों से पीड़ित लोगों को धमकाना
- ऐसी सामग्री जो दूसरों का फ़ायदा उठाने की कोशिश करती है, जिसमें जबरन वसूली, ब्लैकमेल करना वगैरह शामिल है.
- किसी व्यक्ति को सार्वजनिक रूप से अपमानित करने के लिए सामग्री पोस्ट करना.
- किसी दुखद घटना के पीड़ितों या उनके दोस्तों और परिवार के लोगों का उत्पीड़न करना.

खतरनाक उत्पाद

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें विस्फोटकों, बंदूकों, गोला बारूद या बंदूकों से जुड़ी चीज़ों की बिक्री की जाती है.

- जिन चीज़ों पर रोक लगाई गई है उनमें मैगज़ीन या गोलियों के 30 राउंड से ज़्यादा गोलियों वाले बेल्ट और वें चीज़ें शामिल हैं जो किसी बंदूक को अपने आप चलने में मदद करती हैं या किसी बंदूक को अपने आप चलने वाला बना देती हैं (उदाहरण के लिए, बंप स्टॉक, गैटलिंग ट्रिगर, ड्रॉप-इन ऑटो सियर, बदलने वाले सामान).

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें विस्फोटक, बंदूक, गोला-बारूद, दूसरे हथियार या बंदूक से जुड़ी ऐसी चीज़ों को बनाने के निर्देश होते हैं जिनपर दरअसल रोक लगाई गई है. इसमें किसी बंदूक को अपने-आप चलने वाली बंदूक में बदलने या उसको अपने-आप चलने में मदद करने, उसकी गोलियां दागने की क्षमताओं को बढ़ाने या घटाने में मदद करने के बारे में निर्देश शामिल हैं.

गाँजा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो गांजा या इससे बने उत्पाद बेचने की सुविधा देते हैं, भले ही इसे कानूनी रूप से मंज़ूरी क्यों न मिली हो.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- इस्तेमाल करने वालों को ऐप्लिकेशन में मौजूद खरीदारी कार्ट की सुविधा की मदद से गांजा मंगवाने देना.
- गाँजे की डिलीवरी या पिक अप में इस्तेमाल करने वालों की मदद करना.

ऐसे उत्पादों की बिक्री की सुविधा देना जिनमें टीएचसी है.

तंबाकू और शराब

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो तंबाकू (इसमें ई-सिगरेट भी शामिल है) बेचने की सुविधा देते हैं या शराब या तंबाकू के गैर-ज़िम्मेदाराना इस्तेमाल को बढ़ावा देते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- शराब या तंबाकू के इस्तेमाल को दिखाना या बढ़ावा देना. साथ ही, ये चीज़ें नाबालिगों को बेचते हुए दिखाना या इसे बढ़ावा देना.
- यह मानना कि तंबाकू खाने से सामाजिक, यौन, पेशेवर, बौद्धिक या एथलेटिक स्थिति में सुधार आ सकता है.
- किसी की मंज़ूरी के साथ बहुत ज़्यादा शराब पीते हुए दिखाना, जिसमें बहुत ज़्यादा शराब पीना, शराब पीने का उत्सव या शराब पीने की प्रतियोगिता को दिखाना शामिल है.

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो लोगों को धोखा देने वाले या नुकसान पहुंचाने वाले वित्तीय उत्पाद और सेवाएं मुहैया कराते हैं.

इस नीति के तहत, हम पैसों और आभासी मुद्राओं के प्रबंधन या निवेश के काम को वित्तीय उत्पाद और सेवा मानते हैं. इसमें इस्तेमाल करने वाले व्यक्ति की ज़रूरतों के हिसाब से सुझाव देना भी शामिल है.

अगर आपके ऐप्लिकेशन में वित्तीय उत्पाद या सेवाएं शामिल हैं या वह इनका प्रचार करता है, तो आप जिस इलाके या देश के लोगों को टारगेट कर रहे हैं आपको उस राज्य के और स्थानीय नियमों का पालन करना होगा. उदाहरण के लिए, आपको स्थानीय कानून के मुताबिक ज़रूरी जानकारी सार्वजनिक करनी होगी.

बाइनरी ऑप्शन

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो लोगों को बाइनरी ऑप्शन का कारोबार करने की सुविधा देते हैं.

आभासी मुद्राएं

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो डिवाइस पर आभासी मुद्रा बनाते हैं. वहीं, हम उन ऐप्लिकेशन को मंज़ूरी देते हैं जो कहीं और से आभासी मुद्रा बनाए जाने का प्रबंधन करते हैं.

निजी कर्ज़

हमारे हिसाब से निजी क़र्ज़ वह रकम होती है जो एक व्यक्ति किसी दूसरे व्यक्ति, संगठन या इकाई से सिर्फ़ एक बार में लेता है. यह क़र्ज़ कोई संपत्ति खरीदने या पढ़ाई के लिए नहीं लिया जाता. इसे लेने वाले लोगों को इसकी क्वालिटी, सुविधाओं, शुल्क, जोखिमों, और इससे होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे क़र्ज़ के बारे में सोच-समझकर फ़ैसला ले सकें.

- उदाहरण के लिए: निजी क़र्ज़, दिन के हिसाब से मिलने वाले क़र्ज़ (पेडे क़र्ज़), खास लोगों और संगठन वाली वेबसाइटों से मिलने वाले क़र्ज़ (पीयर-टू-पीयर क़र्ज़), गाड़ी को गिरवी रखकर मिलने वाले क़र्ज़ (टाइटल क़र्ज़)

इसमें ये शामिल नहीं हैं: संपत्ति या घर गिरवी रखकर लिया जाने वाला क़र्ज़, कार के लिए लिया जाने वाला क़र्ज़, पढ़ाई के लिए लिया जाने वाला क़र्ज़, और तय की गई किसी उपलब्ध रकम के लिए पेशकश करना (जैसे कि क्रेडिट कार्ड या ज़रूरत पड़ने पर अनिश्चित ब्याज दर पर लिया जाने वाला क़र्ज़)

निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन को अपने मेटाडेटा में नीचे दी गई जानकारी देना ज़रूरी है:

पैसे लौटाने के लिए तय किए गए, कम से कम और ज़्यादा से ज़्यादा दिनों की संख्या
सालाना ब्याज की ज़्यादा से ज़्यादा दर (APR), जिसमें आम तौर पर साल भर की ब्याज की दर, शुल्क, और अन्य लागतें शामिल होती हैं या फिर जिसमें स्थानीय कानून के हिसाब से लगने वाली इसी तरह की दूसरे दर शामिल होती है
सभी तरह के लागू शुल्क को जोड़कर क़र्ज़ की कुल कीमत का एक उदाहरण

हम निजी क़र्ज़ का प्रचार करने वाले उन ऐप्लिकेशन को मंज़ूरी नहीं देते जो क़र्ज़ की पूरी रकम लौटाने के लिए 60 दिन या उससे कम समय की शर्त रखते हैं (इन्हें हम "कम अवधि वाले निजी क़र्ज़" कहते हैं). यह नीति उन ऐप्लिकेशन पर लागू होती है जो सीधे तौर पर क़र्ज़ की सुविधा देते हैं, लीड बनाते हैं, और जो ग्राहकों को क़र्ज़ देने वाले तीसरे पक्ष के लोगों से मिलाते हैं.

ज़्यादा APR वाले निजी क़र्ज़

हम अमेरिका में ऐसे ऐप्लिकेशन को निजी क़र्ज़ देने की मंज़ूरी नहीं देते जिनके सालाना ब्याज की दर (APR) 36% या उससे ज़्यादा होती है. अमेरिका में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के लिए, ट्रुथ इन लेंडिंग ऐक्ट (TILA) के तहत उनका ज़्यादा से ज़्यादा लिया जाने वाला APR दिखाना ज़रूरी है.

यह नीति उन ऐप्लिकेशन पर लागू होती है जो सीधे तौर पर क़र्ज़ की सुविधा देते हैं, लीड बनाते हैं, और जो ग्राहकों को क़र्ज़ देने वाले तीसरे पक्ष के लोगों से मिलाते हैं.

जुआ

हम ऑनलाइन जुआ खेलने की सुविधा देने वाले सिर्फ़ ऐसे कॉन्टेंट, सेवाओं, और विज्ञापनों को तब तक मंज़ूरी देते हैं, जब तक वे कुछ खास शर्तों को पूरा करते हैं. हम रोज़ के फ़ैंटसी स्पोर्ट वाले उन ऐप्लिकेशन को भी मंज़ूरी देते हैं जो कुछ खास शर्तों को पूरा करते हैं.

जुए वाले ऐप्लिकेशन

(इस समय सिर्फ़ यूके, आयरलैंड, और फ़्रांस में मंज़ूरी दी गई है)

हम ऑनलाइन जुआ खेलने की सुविधा देने वाले कॉन्टेंट और सेवाओं को तब तक ही मंज़ूरी देते हैं, जब तक कि वे नीचे दी गई शर्तों को पूरा करते हैं:

Play में अपने ऐप्लिकेशन को वितरित करने के लिए, डेवलपर को ऐप्लिकेशन प्रोसेस सही तरीके से पूरा करना होगा;
ऐप्लिकेशन को उस राज्य या इलाके में लागू सभी कानूनों और औद्योगिक मानकों का पालन करना चाहिए, जहाँ इस ऐप्लिकेशन को वितरित जा रहा है;
डेवलपर के पास हर उस देश के लिए जुए का एक मान्य लाइसेंस होना चाहिए जिसमें ऐप्लिकेशन वितरित होता है;
ऐप्लिकेशन को कम आयु के उपयोगकर्ताओं को ऐप्लिकेशन में जुआ खेलने से रोकना चाहिए;

ऐप्लिकेशन के इस्तेमाल को उन देशों में रोक देना चाहिए जो डेवलपर के दिए हुए जुए के लाइसेंस में शामिल नहीं हैं;
ऐप्लिकेशन को Google Play में सशुल्क ऐप्लिकेशन के तौर पर नहीं खरीदा जाना चाहिए और न ही उन्हें खरीदने के लिए, Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल किया जाना चाहिए;
ऐप्लिकेशन को 'play स्टोर' से मुफ़्त में डाउनलोड और इंस्टॉल किया जाना चाहिए;
ऐप्लिकेशन को AO (सिर्फ़ वयस्क) या IARC के रूप में रेट किया जाना चाहिए; और
ऐप्लिकेशन और इसके ऐप्लिकेशन लिस्टिंग में, ज़िम्मेदारी से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

दूसरी सभी जगहों के लिए, हम ऐसे कॉन्टेंट या सेवाओं को मंज़ूरी नहीं देते हैं जो ऑनलाइन जुए को बढ़ावा देती हैं. इनमें ऑनलाइन कसीनो, खेलों पर सट्टा लगाना और लॉटरी, और कौशल वाले ऐसे गेम जो नकद या असल दुनिया के दूसरे मूल्य के इनाम ऑफ़र करते हैं, शामिल हैं, हालांकि ये यहीं तक सीमित नहीं हैं.

Play में शामिल ऐसे ऐप्लिकेशन जो जुए का विज्ञापन देते हैं

हम ऑनलाइन जुए को बढ़ावा देने वाले विज्ञापनों को तब तक ही मंज़ूरी देते हैं, जब तक कि वे नीचे दी गई शर्तों को पूरा करते हैं:

किसी भी इलाके में जुए से जुड़े विज्ञापन दिखाए जाने के लिए, ऐप्लिकेशन और विज्ञापन (जुए से जुड़े विज्ञापन देने वाले लोगों सहित) को उस इलाके में लागू सभी कानूनों और उद्योग के मानकों का पालन करना होगा;
विज्ञापन को, प्रचार किए जा रहे जुए से जुड़े सभी उत्पादों और सेवाओं की स्थानीय लाइसेंस ज़रूरतों को पूरा करना चाहिए;
ऐप्लिकेशन को, 18 से कम उम्र के लोगों के लिए जुए से जुड़ा कोई विज्ञापन प्रदर्शित नहीं करना चाहिए;
ऐप्लिकेशन को परिवार के लिए बनाए गए कार्यक्रम में नामांकित नहीं कराया जाना चाहिए;
ऐप्लिकेशन को 18 से कम उम्र के लोगों को लक्षित नहीं करना चाहिए;
विज्ञापन को लैंडिंग पेज पर, विज्ञापन की गई ऐप्लिकेशन सूची पर या ऐप्लिकेशन के अंदर, ज़िम्मेदारी से खेले जाने वाले जुए के बारे में स्पष्ट तरीके से जानकारी प्रदर्शित करनी चाहिए; और
जुए का विज्ञापन देने वाला ऐप्लिकेशन, जुए की नकल करने वाला ऐप्लिकेशन (ऐसा मनोरंजक गेम जिसमें असली पैसे के बिना जुआ खेला जाता है) नहीं होना चाहिए.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

'KIDS 123' ऐप्लिकेशन में जुए की सेवाओं का प्रचार करने वाला एक विज्ञापन शामिल होता है

रोज़ाना के फ़ैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन

हम रोज़ के फ़ैंटसी स्पोर्ट (DFS) को तब तक ही मंज़ूरी देते हैं, जब तक कि वे नीचे दी गई शर्तों को पूरा करते हैं:

ऐप्लिकेशन को सिर्फ़ संयुक्त राज्य में ही ऐक्सेस की मंज़ूरी देनी चाहिए या वितरित किया जाना चाहिए;
DFS ऐप्लिकेशन को यूएस के अधिकार क्षेत्र से बाहर के इलाकों में पंहुचाने के अपने टारगेट के लिए, रीयल मनी गैंबलिंग (असली धन दांव पर लगाकर जुआ खेलने वाले ऐप्लिकेशन) ऐप्लिकेशन प्रोसेस की मंज़ूरी मिलनी चाहिए;
Play में ऐप्लिकेशन को वितरित करने के लिए, डेवलपर को DFS ऐप्लिकेशन प्रोसेस सही तरीके से पूरा करना होगा;

ऐप्लिकेशन को यूएस के उस राज्य या इलाके में लागू सभी कानूनों और औद्योगिक मानकों का पालन करना होगा, जहां उस ऐप्लिकेशन को वितरित जा रहा है;
डेवलपर के पास यूएस के हर उस राज्य या क्षेत्र के लिए मान्य लाइसेंस होना चाहिए जिसमें रोज़ के फ़ैंटसी खेल वाले ऐप्लिकेशन के लिए लाइसेंस की ज़रूरत होती है;
ऐप्लिकेशन को कम उम्र के उपयोगकर्ताओं को ऐप्लिकेशन में जुआ खेलने या पैसे का लेन-देन करने से रोकना चाहिए;
ऐप्लिकेशन को यूएस के उन राज्यों या क्षेत्रों में इस्तेमाल को रोकना चाहिए जिनमें डेवलपर के पास रोज़ के फ़ैंटसी खेल वाले ऐप्लिकेशन के लिए ज़रूरी लाइसेंस नहीं है;
ऐप्लिकेशन के इस्तेमाल को यूएस के उन राज्यों या इलाकों में रोक देना चाहिए जिनमें रोज़ के फ़ैंटसी स्पोर्ट वाले ऐप्लिकेशन का इस्तेमाल गैर-कानूनी रूप से किया जाता है;
ऐप्लिकेशन को Google Play में सशुल्क ऐप्लिकेशन के तौर पर नहीं खरीदा जाना चाहिए और न ही उन्हें खरीदने के लिए, Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल किया जाना चाहिए;
ऐप्लिकेशन को 'play स्टोर' से मुफ़्त में डाउनलोड और इंस्टॉल किया जाना चाहिए;
ऐप्लिकेशन को AO (सिर्फ़ वयस्क) या IARC के रूप में रेट किया जाना चाहिए; और
ऐप्लिकेशन और इसके ऐप्लिकेशन लिस्टिंग में, ज़िम्मेदारी से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो गैरकानूनी गतिविधियों की सुविधा देते हैं या उनका प्रचार करते हैं. यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

गैरकानूनी दवाएं या डॉक्टर की सलाह के बिना दवाएं खरीदने या बेचने की सुविधा देना.
नाबालिगों को किसी नशीली दवा, शराब या तंबाकू का इस्तेमाल करते हुए या बेचते हुए दिखाना या बढ़ावा देना.
गैरकानूनी दवाएं उगाने या बनाने के निर्देश.

यूज़र जनरेटेड कॉन्टेंट

यूज़र जनरेटेड कॉन्टेंट (यूजीसी) ऐसा कॉन्टेंट है जिसे इस्तेमाल करने वाले लोग किसी ऐप्लिकेशन में जोड़ते हैं. साथ ही, जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों के कम से कम एक सबसेट को दिखता है या वे उसे ऐक्सेस कर सकते हैं. आपत्तिजनक सामग्री ऐसी सामग्री है जो हमारी नीतियों का उल्लंघन करती है.

ऐसे ऐप्लिकेशन जिनमें UGC है या जो इसकी सुविधा देते हैं, उन्हें:

उपयोगकर्ताओं के लिए यह बात ज़रूरी बनाना चाहिए कि वे UGC सामग्री बनाने या अपलोड करने से पहले ऐप्लिकेशन की इस्तेमाल की शर्तें और/या उपयोगकर्ता नीति को स्वीकार करें;
Google Play की डेवलपर कार्यक्रम नीतियों से संगत तरीके और उसकी भावना के हिसाब से ऐसी UGC तय करनी चाहिए जो आपत्तिजनक है और ऐसी UGC को ऐप्लिकेशन के इस्तेमाल की शर्तों और/या उपयोगकर्ता नीति के ज़रिए प्रतिबंधित करना चाहिए;
बेहतरीन, असरदार, और लगातार होने वाला यूजीसी (लोगों का बनाया कॉन्टेंट) मॉडरेशन लागू करना चाहिए. ऐप्लिकेशन पर होस्ट किया गया इस तरह का यूजीसी (लोगों का बनाया कॉन्टेंट) उचित और अनुकूल होता है;
ऐप्लिकेशन को एक ऐसा इन-ऐप्लिकेशन सिस्टम उपलब्ध कराना चाहिए जो उपयोगकर्ता के लिए आसान हो. साथ ही, जिससे आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) को हटाया जा सके और उसकी शिकायत की जा सके;

लाइव स्ट्रीमिंग ऐप्लिकेशन में ऐसा यूजीसी (लोगों का बनाया कॉन्टेंट) जिनमें समस्या हो उसे जितना रीयल-टाइम में हो सके उतना जल्दी हटा दिया जाना चाहिए; और

बुरा बर्ताव करने वाले ऐसे उपयोगकर्ता जो ऐप्लिकेशन की इस्तेमाल की शर्तों और/या उपयोगकर्ता नीति का उल्लंघन करते हैं उन्हें हटा देना चाहिए या ब्लॉक कर देना चाहिए;

ऐप्लिकेशन के अंदर कमाई करने की सुविधा की सुरक्षा के लिए उपयोगकर्ताओं के आपत्तिजनक बर्ताव पर रोक लगानी चाहिए.

ऐसे ऐप्लिकेशन जिनका मुख्य मकसद आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) को शामिल करना है उन्हें Google Play से हटा दिया जाएगा. इसी तरह, जिन ऐप्लिकेशन का इस्तेमाल मुख्य रूप से आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) को होस्ट करने के लिए किया जाता है या जिनकी छवी उपयोगकर्ताओं के बीच खराब हो चुकी है, उन्हें भी Google Play से हटा दिया जाएगा.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

अश्लील यौन कॉन्टेंट का प्रचार करना जिनमें मुख्य रूप से पैसे लेकर आपत्तिजनक कॉन्टेंट को बढ़ावा देने वाली सुविधाएं शामिल हैं.

यूज़र जनरेटेड कॉन्टेंट (यूजीसी) वाले ऐसे ऐप्लिकेशन जिनमें डराना, उत्पीड़न या धमकियों के ख़िलाफ़ ज़रूरी सुरक्षा उपायों की कमी हो खासकर नाबालिगों को लेकर.

किसी ऐप्लिकेशन में शामिल ऐसी पोस्ट, टिप्पणियां या फ़ोटो जिनका मुख्य मकसद किसी दूसरे व्यक्ति से बुरा बर्ताव करना, नुकसान पहुंचाने वाला हमला करना या मज़ाक़ उड़ाने के लिए उसे प्रताड़ित करना या अकेला छोड़ देना हो.

ऐसे ऐप्लिकेशन, जो आपत्तिजनक कॉन्टेंट के बारे में उपयोगकर्ता की शिकायतों का हल करने में लगातार नाकामयाब हो रहे हों.

Google Play ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देता है जो किसी कानूनी दावे के बावजूद भी, बिना मंज़ूरी वाली चीज़ों को बेचते हैं या उनका प्रचार करते हैं. उदाहरण:

प्रतिबंधित दवाओं और उत्पादोंकी इस कम जानकारी वाली सूची के सभी आइटम

ऐसे उत्पाद जिनमें इफ़ेड्रा है

वज़न घटाने या वज़न नियंत्रण से जुड़े या एनाबॉलिक स्टेरॉइड के साथ प्रचार किए गए ह्यूमन कोरियोनिक गॉनाडोट्रॉपिन (एचसीजी) वाले उत्पाद

एक्टिव फ़ार्मास्यूटिकल या खतरनाक सामग्री वाले हर्बल और सप्लीमेंट

झूठे या गुमराह करने वाले स्वास्थ्य से जुड़े दावे, जिनमें यह दावा किया गया है कि उत्पाद डॉक्टर से सुझाई गई दवाओं या नियंत्रित पदार्थों की तरह काम करता है

किसी खास बीमारी या रोग को रोकने, उसकी चिकित्सा या इलाज करने के लिए सुरक्षित या प्रभावी होने के दावे के साथ बेचे जाने वाले ऐसे उत्पाद, जिनकी सरकार ने मंज़ूरी न दी हो

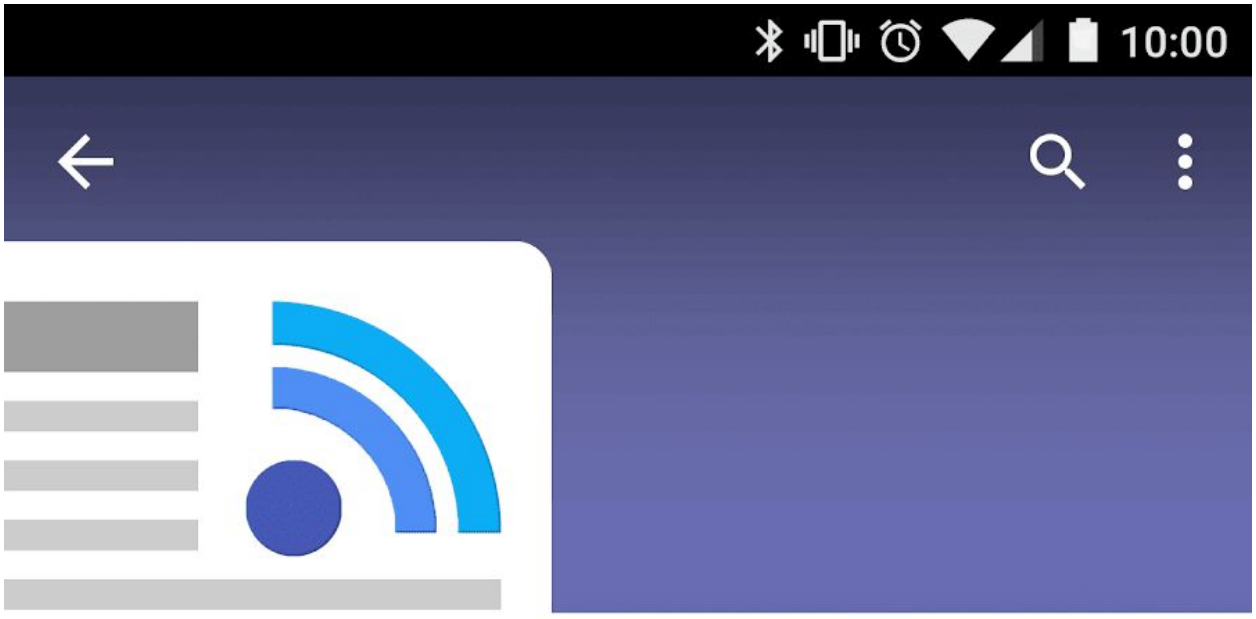
किसी भी सरकारी या कानूनी कार्रवाई या चेतावनी के तहत आने वाले उत्पाद

ऐसे उत्पाद जिनका नाम बिना मंज़ूरी वाली ऐसी दवाओं या सप्लीमेंट या कंट्रोल की जाने वाली ऐसी चीज़ों से मिलता है, जो भटका देती हैं

हम जिन दवाओं और उत्पादों को अस्वीकार करते हैं या जिन पर गुमराह करने वाले के तौर पर नज़र रखते है, उनके बारे में ज़्यादा जानकारी के लिए, कृपया www.legitscript.com पर जाएं.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो किसी अन्य इकाई के ब्रैंड, शीर्षक, लोगो या नाम का इस्तेमाल इस तरीके से करते हैं, जिसकी वजह से इस्तेमाल करने वाले लोग गुमराह हो सकते हैं. अगर आपको किसी अन्य इकाई का समर्थन नहीं है या आपका उससे संबंध नहीं है, तो ऐसा दिखाने की कोशिश न करें. किसी को नुकसान न पहुंचाने के इरादे से भी पहचान चुराई जा सकती है, इसलिए कृपया ऐसे किसी ब्रैंड का इस्तेमाल करते हुए सावधानी बरतें जिनकी आपको जानकारी न हो. यह उस ब्रैंड पर भी लागू होता है जो फ़िलहाल Google Play पर मौजूद नहीं है.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे डेवलपर जो किसी अन्य इकाई के साथ जुड़े होने की गलत जानकारी देते हैं:



RSS News Aggregator

Google Developer

Everyone

INSTALL

100 MILLION
Downloads

4.1
161,251

News & Magazines

Similar

All the best news, aggregated in one spot!

WHAT'S NEW

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

① इस ऐप्लिकेशन के डेवलपर के नाम से इसके Google के साथ जुड़े होने का पता चलता है, जबकि दोनों के बीच ऐसा कोई संबंध है ही नहीं.
ऐसे ऐप्लिकेशन जिनके शीर्षक और आइकॉन मौजूदा उत्पादों या सेवाओं से मिलते-जुलते हैं जिससे इस्तेमाल करने वाले लोग गुमराह हो सकते हैं:

✓	 Google Maps	 Google+	 YouTube	 Twitter
✗	 Google Maps Navigator	 Google+ Sharify	 YouTube Aggregator	 TwitterPro

ऐसे ऐप्लिकेशन जो पहले से मौजूद किसी जानी-मानी इकाई का आधिकारिक ऐप्लिकेशन होने का गलत दावा करते हैं. ज़रूरी अनुमतियों या अधिकारों के बिना "जस्टिन बीबर ऑफ़िशियल" जैसे शीर्षकों का इस्तेमाल करने की अनुमति नहीं है.
ऐसे ऐप्लिकेशन जो Android ब्रैंड दिशानिर्देशों का उल्लंघन करते हैं.

बौद्धिक संपत्ति

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते हैं जो दूसरे लोगों के बौद्धिक संपत्ति के अधिकारों का उल्लंघन करते हैं. इनमें ट्रेडमार्क, कॉपीराइट, पेटेंट, और कारोबार से जुड़ी गोपनीय जानकारी के साथ मालिकाना अधिकार शामिल हैं. हम ऐसे ऐप्लिकेशन को भी अनुमति नहीं देते हैं जो बौद्धिक संपत्ति के अधिकारों के उल्लंघन को बढ़ावा देते हैं या ऐसा करने के लिए प्रोत्साहित करते हैं.

हम कॉपीराइट के कथित उल्लंघन के आरोपों वाली, साफ़ तौर पर दी गई सूचनाओं का जवाब देंगे. ज़्यादा जानकारी पाने के लिए या DMCA अनुरोध दर्ज करने के लिए, हमारी कॉपीराइट से जुड़ी प्रक्रियाओं पर जाएं.

किसी ऐप्लिकेशन में हो रही नकली उत्पादों की बिक्री या बिक्री के लिए प्रचार के बारे में शिकायत करने के लिए, कृपया नकली सामान की सूचना सबमिट करें.

अगर आप ट्रेडमार्क के मालिक हैं और आपको लगता है कि Google Play पर मौजूद कोई ऐप्लिकेशन आपके ट्रेडमार्क अधिकारों का उल्लंघन करता है, तो अपनी समस्या हल करने के लिए, आप सीधे डेवलपर से भी संपर्क कर सकते हैं. अगर आपकी समस्या फिर भी हल नहीं होती है, तो कृपया इस फ़ॉर्म को भर के ट्रेडमार्क के बारे में शिकायत दर्ज करें.

अगर आपके पास यह बताने वाला लिखित दस्तावेज़ है कि आपको अपने ऐप्लिकेशन या स्टोर पेज (जैसे ब्रांड का नाम, लोगो, और ग्राफ़िक रचनाएं) में किसी तीसरे पक्ष की बौद्धिक संपत्ति का इस्तेमाल करने की अनुमति है, तो

आप सबमिशन से पहले ही, Google Play टीम से संपर्क करें इससे आप यह पक्का कर सकते हैं कि आपका ऐप्लिकेशन, बौद्धिक संपत्ति के उल्लंघन के लिए अस्वीकार न हो जाए.

कॉपीराइट वाले कॉन्टेंट का बिना मंज़ूरी इस्तेमाल करना

हम उन ऐप्लिकेशन को अनुमति नहीं देते हैं जो कॉपीराइट का उल्लंघन करते हैं. कॉपीराइट कॉन्टेंट में बदलाव करने से भी उल्लंघन हो सकता है. ऐसा हो सकता है कि डेवलपर को, कॉपीराइट वाले कॉन्टेंट को इस्तेमाल करने के अधिकारों का सबूत देने को कहा जाए.

जब आप अपने ऐप्लिकेशन की सुविधा दिखा रहे हों, तो उसमें कॉपीराइट वाले कॉन्टेंट का इस्तेमाल करते समय कृपया ध्यान रखें. आम तौर पर, सुरक्षित तरीका यह है कि कुछ ऐसा बनाएं जो पूरी तरह से आपका ही हो.

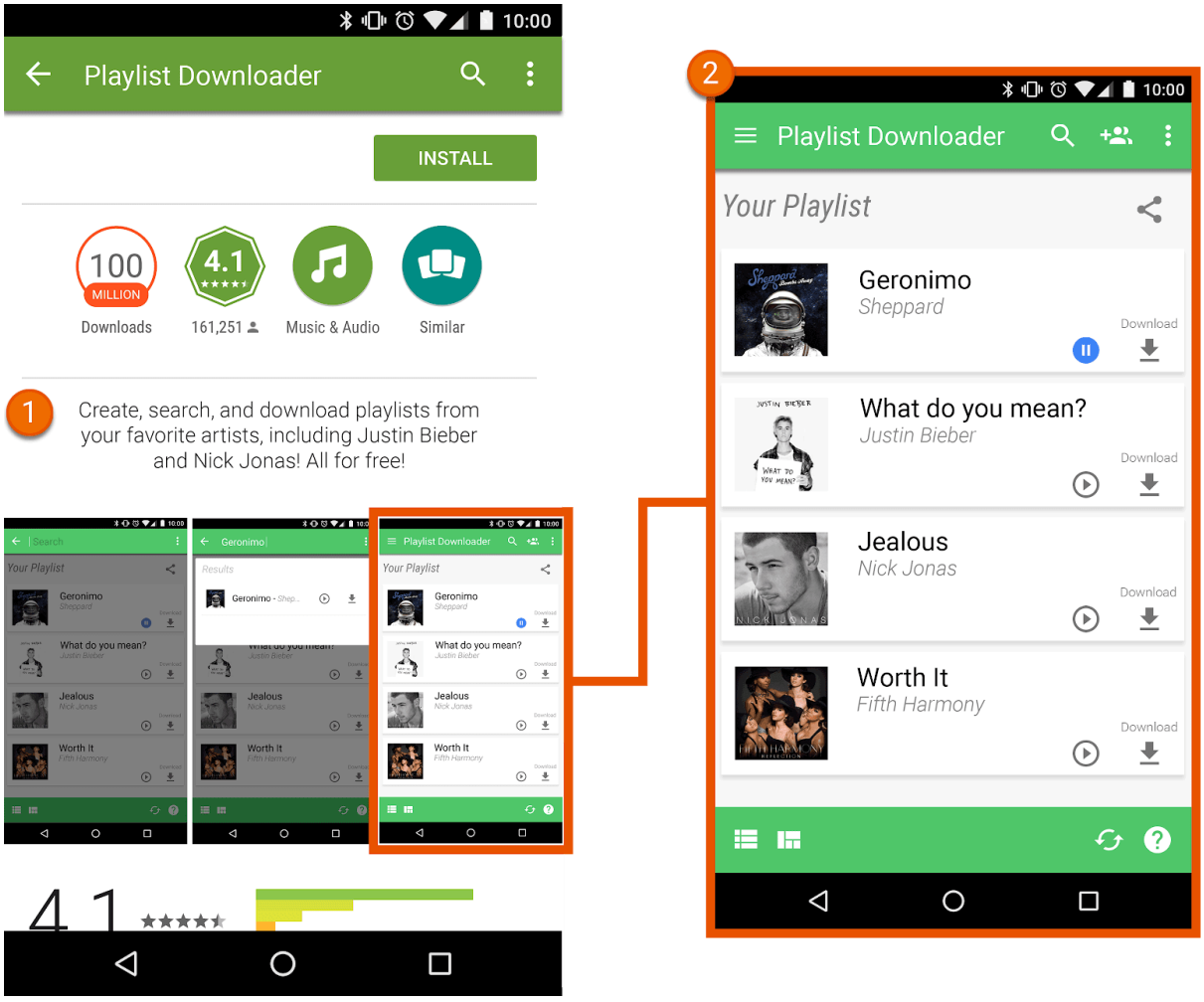
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

संगीत एल्बम, वीडियो गेम, और किताबों के लिए कवर आर्ट.
फ़िल्मों, टेलीविजन या वीडियो गेम की मार्केटिंग इमेज.
कॉमिक बुक, कार्टून, फ़िल्मों, संगीत वीडियो या टेलीविज़न के आर्टवर्क या इमेज.
कॉलेज और पेशेवर खेल टीम के लोगो.
किसी लोकप्रिय हस्ती के सोशल मीडिया खाते से ली गई फ़ोटो.
लोकप्रिय हस्तियों की पेशेवर फ़ोटो.
कॉपीराइट के तहत आने वाला ऐसा रीप्रोडक्शन या "फ़ैन-आर्ट" जिसे मूल काम से अलग न किया जा सकता हो.
वे ऐप्लिकेशन जिनमें ऐसे साउंडबोर्ड होते हैं जो कॉपीराइट वाले कॉन्टेंट की ऑडियो क्लिप चलाते हैं.
ऐसी किताबों का उत्पादन या अनुवाद जो सार्वजनिक डोमेन में मौजूद नहीं है.

कॉपीराइट के उल्लंघन को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो कॉपीराइट उल्लंघन को बढ़ावा देते हैं. अपना ऐप्लिकेशन प्रकाशित करने से पहले, पता लगाएं कि आपका ऐप्लिकेशन कॉपीराइट उल्लंघन को बढ़ावा तो नहीं दे रहा और अगर ज़रूरी हो तो कानूनी सलाह लें.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे स्ट्रीमिंग ऐप्लिकेशन जो उपयोगकर्ताओं को, कॉपीराइट कॉन्टेंट की स्थानीय कॉपी डाउनलोड करने देते हैं, वह भी बिना किसी अनुमति के.
ऐसे ऐप्लिकेशन जो लागू कॉपीराइट कानून का उल्लंघन करते हुए, उपयोगकर्ताओं को कॉपीराइट किए गए काम के साथ ही संगीत और वीडियो को स्ट्रीम करने और डाउनलोड करने के लिए बढ़ावा देते हैं:



① इस ऐप लिस्टिंग में दी गई जानकारी, उपयोगकर्ताओं को कॉपीराइट वाले कॉन्टेंट को बिना अनुमति के डाउनलोड करने के लिए बढ़ावा देती है.
② ऐप लिस्टिंग में दिया गया स्क्रीनशॉट, उपयोगकर्ताओं को कॉपीराइट वाले कॉन्टेंट को, बिना अनुमति के डाउनलोड करने के लिए बढ़ावा देता है.

ट्रेडमार्क का उल्लंघन करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो दूसरों के ट्रेडमार्क का उल्लंघन करते हैं. ट्रेडमार्क एक ऐसा शब्द, चिह्न या दोनों से मिला-जुला रूप है जिससे पता चलता है कि किसी सामान या सेवा का स्रोत क्या है. पहचान के बाद ट्रेडमार्क, मालिक को कुछ वस्तुओं या सेवाओं के संबंध में ट्रेडमार्क के इस्तेमाल के लिए खास अधिकार देता है.

ट्रेडमार्क के उल्लंघन का मतलब है किसी एक जैसे या मिलते-जुलते ट्रेडमार्क का गलत तरीके से या बिना अनुमति के इस तरह इस्तेमाल करना कि उत्पाद के स्रोत को लेकर गलतफ़हमी होने की संभावना हो जाए. अगर आप किसी दूसरे पक्ष के ट्रेडमार्क का इस्तेमाल इस तरीके से करते हैं जिससे इसे समझने में परेशानी होती है, तो आपका ऐप्लिकेशन निलंबित किया जा सकता है.

नकली

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो नकली सामान बेचते हैं या उनकी बिक्री के लिए प्रचार करते हैं. नकली सामान पर किसी अन्य उत्पाद के ट्रेडमार्क से मेल खाने वाला या साफ़ तौर पर पहचाना न जा सकने वाला एक ट्रेडमार्क या लोगो होता है. इस तरह के उत्पाद किसी ब्रैंड के उत्पाद में मिलने वाली सुविधाओं (ब्रैंड सुविधाएं) या पहचान की नकल करके उसे ब्रैंड मालिक के असली उत्पाद की तरह पेश करते हैं.

आपको इस बारे में पारदर्शी होना चाहिए कि आप ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का डेटा कैसे प्रबंधित करते हैं. इसमें किसी उपयोगकर्ता से इकट्ठा की गई या उसके बारे में जानकारी के अलावा, डिवाइस की जानकारी भी शामिल है. इसका मतलब है कि आपके ऐप्लिकेशन का ऐक्सेस, डेटा को इकट्ठा करने, इस्तेमाल करने, और उसे शेयर करने की जानकारी देना. साथ ही, डेटा का इस्तेमाल सिर्फ़ बताए गए उद्देश्यों के लिए करना. इसके अलावा, अगर आपका ऐप्लिकेशन उपयोगकर्ता का निजी या संवेदनशील डेटा प्रबंधित करता है, तो कृपया नीचे "निजी और संवेदनशील जानकारी" सेक्शन में बताई गई दूसरी ज़रूरतों को भी देखें. Google Play की ये ज़रूरतें, लागू निजता कानून, और डेटा सुरक्षा के तहत कानूनों में बताई गई ज़रूरतों के अतिरिक्त हैं.

निजी और संवेदनशील जानकारी

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का निजी और संवेदनशील डेटा, उसकी निजी तौर पर पहचानने लायक जानकारी, वित्तीय और पैसे चुकाने के बारे में जानकारी, पुष्टि करने की जानकारी, फ़ोनबुक, संपर्क, डिवाइस की जगह, मैसेज (एसएमएस), और फ़ोन से जुड़े डेटा, माइक्रोफ़ोन, कैमरा, और अन्य संवेदनशील डिवाइस या इस्तेमाल किए गए डेटा तक ही सीमित नहीं है. अगर आपका ऐप्लिकेशन लोगों का संवेदनशील डेटा प्रबंधित करता है, तो आपको ये करना चाहिए:

- ऐप्लिकेशन से मिले निजी और संवेदनशील डेटा के ऐक्सेस, संग्रह, इस्तेमाल, और शेयर करने को उन मकसदों तक सीमित करना जो ऐप्लिकेशन की सुविधाएं देने और उन्हें बेहतर बनाने से सीधे तौर पर जुड़े हैं (उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की उम्मीद के मुताबिक काम करने का तरीका जिसे दस्तावेज़ के तौर पर बताया गया है और 'Play स्टोर' में ऐप्लिकेशन के ब्यौरे में जिसका प्रचार किया गया है). विज्ञापन दिखाने के लिए इस डेटा के इस्तेमाल करने वाले ऐप्लिकेशन को हमारी विज्ञापन नीति का पालन करना चाहिए.
- 'Play कंसोल' में तय की गई फ़ील्ड और ऐप्लिकेशन, दोनों में निजता नीति पोस्ट करें. निजता नीति को ऐप्लिकेशन में ज़ाहिर की गई जानकारी के साथ, इस बात की पूरी जानकारी देनी चाहिए कि आपका ऐप्लिकेशन कैसे उपयोगकर्ता के डेटा को ऐक्सेस, इकट्ठा, शेयर, और इस्तेमाल करता है आपकी निजता नीति को बताना चाहिए कि आपका ऐप्लिकेशन किस तरह के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करता है. साथ ही, यह भी बताना चाहिए कि ये डेटा किस तरह के समूह के साथ शेयर किया जाता है.
- आधुनिक क्रिप्टोग्राफ़ी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करके, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का निजी और संवेदनशील डेटा दूसरी जगह तक पहुंचाने के साथ ही सुरक्षित रूप से प्रबंधित करना चाहिए.
- Android की अनुमतियों से सुरक्षित किया गया डेटा ऐक्सेस करने से पहले, उपलब्ध होने पर रनटाइम अनुमतियों के अनुरोध का इस्तेमाल करें.
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी या संवेदनशील डेटा की बिक्री न करें.

प्रमुखता से जानकारी देने और सहमति की ज़रूरत

उन स्थितियों में, जहां हो सकता है कि ऐप्लिकेशन इस्तेमाल करने वाले लोगों को इस बात की अपेक्षा न हो -- जैसा कि Play में बताया गया है -- कि उनका निजी या संवेदनशील डेटा, आपके ऐप्लिकेशन में नीति का पालन करने वाली

सुविधाओं या काम करने के तरीके में सुधार करने के लिए ज़रूरी होगा. साथ ही, आपको नीचे बताई गई ज़रूरतों को भी पूरा करना होगा:

आपको डेटा के ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करने के बारे में ऐप्लिकेशन में जानकारी देनी होगी. ऐप्लिकेशन में दी जाने वाली जानकारी:

- ऐप्लिकेशन के अंदर होनी चाहिए, न कि सिर्फ़ ऐप्लिकेशन के ब्यौरे में या किसी वेबसाइट पर;
- ऐप्लिकेशन के सामान्य इस्तेमाल के दौरान दिखाई जानी चाहिए और उपयोगकर्ता को इसके लिए मेन्यू या सेटिंग में जाने की ज़रूरत नहीं पड़नी चाहिए;
- में ऐक्सेस या इकट्ठा किए जा रहे डेटा के बारे में बताया जाना चाहिए;
- यह बताया जाना चाहिए कि डेटा को इस्तेमाल और/या शेयर कैसे किया जाएगा;
- इसे सिर्फ़ किसी निजता नीति या सेवा की शर्तों में नहीं रखा जा सकता; और
- निजी या संवेदनशील डेटा इकट्ठा करने से अलग दूसरी जानकारियों को शामिल नहीं किया जा सकता.

ऐप्लिकेशन में दी जाने वाली जानकारी के साथ, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति लेने का अनुरोध शामिल होना चाहिए. साथ ही, जहां यह उपलब्ध हो वहां एक रनटाइम अनुमति भी होनी चाहिए. आप ऐप्लिकेशन इस्तेमाल करने वाले लोगों की सहमति के बिना किसी भी निजी डेटा को ऐक्सेस या इकट्ठा नहीं कर पाएंगे. सहमति के लिए ऐप्लिकेशन का अनुरोध:

- सहमति संवाद साफ़ और स्पष्ट तरीके से दिया जाना चाहिए;
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के लिए यह ज़रूरी है कि वह स्वीकार करने लायक कार्रवाई करें (जैसे कि, स्वीकार करने के लिए टैप करना, सही का निशान लगाकर चुनना);
- सहमति से बाहर निकलने या कहीं और जाने को (टैप करके बाहर जाने या वापस जाने के लिए दबाना या होम बटन के साथ) सहमति नहीं समझा जाना चाहिए; और
- अपने-आप खारिज या खत्म होने वाले मैसेज का इस्तेमाल नहीं किया जाना चाहिए.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- ऐसा ऐप्लिकेशन, जो किसी व्यक्ति के इंस्टॉल किए गए ऐप्लिकेशन की इन्वेंट्री को ऐक्सेस करता है और इस डेटा को निजता नीति, सुरक्षित रूप से दूसरी जगह तक पहुंचाने, और खास तौर पर जानकारी देने की ज़रूरतों के तहत आने वाले निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन, जो किसी व्यक्ति के फ़ोन या संपर्क बुक का डेटा ऐक्सेस करता है और इस डेटा को निजता, सुरक्षित रूप से दूसरी जगह तक पहुंचाने, और खास तौर पर जानकारी देने की ज़रूरतों के तहत आने वाले निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन, जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की स्क्रीन रिकॉर्ड करता है और इस नीति के मुताबिक डेटा को निजी या संवेदनशील जानकारी के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन, जो डिवाइस की जगह की जानकारी को इकट्ठा करता है और ऊपर बताई गई ज़रूरतों के मुताबिक पूरी तरह से इसके इस्तेमाल की जानकारी नहीं देता है

संवेदनशील डेटा ऐक्सेस करने के लिए पाबंदियां

ऊपर दी गई जानकारियों के साथ ही, नीचे दिए गए टेबल में खास गतिविधियों के लिए ज़रूरी बातों के बारे में बताया गया है.

गतिविधि	ज़रूरत

आपका ऐप्लिकेशन वित्तीय या पैसे चुकाने के बारे में जानकारी या सरकारी पहचान की संख्याओं का प्रबंधन करता है	आपके ऐप्लिकेशन कभी भी वित्तीय या भुगतान से जुड़ी गतिविधियों या किसी भी सरकारी पहचान संख्या से संबंधित कोई भी व्यक्तिगत या संवेदनशील उपयोगकर्ता डेटा सार्वजनिक रूप से जाहिर नहीं करना चाहिए.
आपका ऐप्लिकेशन गैर-सार्वजनिक फ़ोनबुक या संपर्क जानकारी का प्रबंधन करता है	हम लोगों के गैर-सार्वजनिक संपर्कों को बिना मंज़ूरी प्रकाशित करने या उनकी जानकारी देने की अनुमति नहीं देते.
आपके ऐप्लिकेशन में एंटी-वायरस या सुरक्षा के लिए काम करने वाले फ़ंक्शन, जैसे कि एंटी-वायरस, एंटी-मैलवेयर या सुरक्षा से जुड़ी सुविधाएं हैं	आपके ऐप्लिकेशन को ऐसी निजता नीति पोस्ट करनी चाहिए जो, ऐप्लिकेशन में किए गए किसी भी खुलासे के साथ, यह बताए कि आपका ऐप्लिकेशन उपयोगकर्ता का कौनसा डेटा इकट्ठा करता है और उसे दूसरों तक पहुंचाता है, उसका इस्तेमाल किस तरह से किया जाता है, और वे पक्ष या समूह जिनके साथ उसे शेयर किया जाता है.

EU-U.S. Privacy Shield (यूरोपीय संघ–अमेरिका Privacy Shield)

अगर आप Google की ओर से उपलब्ध कराई गई ऐसी व्यक्तिगत जानकारी को ऐक्सेस करते हैं, इस्तेमाल या प्रोसेस करते हैं जो सीधे तौर पर या किसी दूसरे तरीके से, किसी ऐसे व्यक्ति की पहचान करती है जो मूल रूप से यूरोपीय संघ या स्विट्ज़रलैंड ("यूरोपीय संघ निजी जानकारी") का है, तो आपको ये काम करने होंगे:

- सभी लागू निजता, डेटा सुरक्षा, और डेटा संरक्षण कानूनों, निर्देशों, नियामकों और नियमों का पालन करना;
- ईयू (यूरोपीय संघ) निजी जानकारी सिर्फ़ ऐसे मकसद से एक्सेस करना, इस्तेमाल करना या प्रोसेस करना जो उस व्यक्ति से मिलने वाली सहमति के मुताबिक हो जिससे ईयू (यूरोपीय संघ) की निजी जानकारी जुड़ी है;
- ईयू (यूरोपीय संघ) की निजी जानकारी को नुकसान, गलत इस्तेमाल, और गलत या गैर-कानूनी ऐक्सेस, जानकारी देने, बदले जाने और नुकसान से बचाने के लिए, संगठन के स्तर पर और तकनीकी स्तर पर ज़रूरी कदम उठाना; और
- उसी स्तर की सुरक्षा मुहैया कराना जैसी Privacy Shield के सिद्धांतों में ज़रूरी बताई गई है.

आपको समय-समय पर देखना होगा कि इन शर्तों का पालन ठीक तरीके से हो रहा है या नहीं. अगर, किसी भी समय, आप इन शर्तों का पालन नहीं कर पाते हैं (या अगर इस बात का जोखिम ज़्यादा है कि आप उनका पालन नहीं कर पाएंगे), तो आपको हमें data-protection-office@google.com पर ईमेल करके तुरंत बताना चाहिए और यूरोपीय संघ निजी जानकारी से जुड़े काम तुरंत रोक देने चाहिए या सुरक्षा के स्तर को पहले जैसा बनाए रखने के लिए ज़रूरी कदम उठाने चाहिए.

ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए, अनुमति के अनुरोधों का कुछ मतलब होना चाहिए. आप सिर्फ़ वे अनुमतियां मांग सकते हैं जो आपके ऐप्लिकेशन में, उन सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं जिनके बारे में आपने 'Play स्टोर' के अपने पेज पर बताया है. आप ऐसी अनुमतियों का इस्तेमाल नहीं कर सकते हैं जिनसे उपयोगकर्ताओं या डिवाइस डेटा का ऐक्सेस, बताई नहीं गई, लागू नहीं की गई या मंज़ूर नहीं की गई सुविधाओं को मिल जाता है. अनुमतियों से एक्सेस किया गया निजी या संवेदनशील डेटा कभी भी बेचा नहीं जा सकता.

ज़रूरत के मुताबिक (बढ़ती हुई मंज़ूरी) डेटा एक्सेस करने का अनुरोध करें, ताकि इस्तेमाल करने वाले यह समझ सकें कि आपके ऐप्लिकेशन को अनुमति क्यों चाहिए. डेटा का इस्तेमाल सिर्फ़ उन्हीं मकसदों से करें जिनके लिए इस्तेमाल करने वाले ने सहमति दी है. अगर आप बाद में दूसरे मकसद के लिए डेटा का इस्तेमाल करना चाहते हैं, तो आपको इस्तेमाल करने वालों से पूछना होगा और यह पक्का करना होगा कि वे दूसरे इस्तेमाल के लिए सकारात्मक रूप से सहमत हों.

पाबंदी वाली अनुमतियां

ऊपर बताई गई के अलावा, पाबंदी वाली अनुमतियां वो होती हैं जिन्हें हमारे डेवलपर दस्तावेज़ में Signature या Dangerous के तौर पर शामिल किया गया है. साथ ही, इन पर आगे दी गई दूसरी ज़रूरी शर्तें और पाबंदियां लागू होती हैं:

> पाबंदी वाली अनुमति का ऐक्सेस लेकर उपयोगकर्ता या डिवाइस का संवेदनशील डेटा तीसरे पक्ष को ट्रांसफ़र तब ही किया जा सकता है जब उस ऐप्लिकेशन में मौजूदा सुविधाएं या सेवाएं देने या उन्हें बेहतर बनाने के लिए ज़रूरी हो जिससे डेटा इकट्ठा किया गया था. आप लागू कानून का पालन करने या किसी विलय, अधिग्रहण या परिसंपत्तियों की बिक्री के लिए भी उपयोगकर्ताओं को कानूनी रूप से उचित सूचना देकर डेटा ट्रांसफ़र कर सकते हैं. इसके अलावा, किसी भी तरह से उपयोगकर्ता के डेटा को ट्रांसफ़र करना या बेचना प्रतिबंधित है.
> अगर ऐप्लिकेशन इस्तेमाल करने वाले लोग पाबंदी वाली अनुमति देने से मना कर देते हैं, तो उनके फ़ैसले का सम्मान करें. साथ ही, किसी गैर ज़रूरी अनुमति पर सहमति देने के लिए ऐप्लिकेशन इस्तेमाल करने वाले लोगों पर दबाव नहीं बनाया जा सकता, न ही उनके फ़ैसले को बदलने की कोशिश की जा सकती है. ऐप्लिकेशन इस्तेमाल करने वाले वे लोग जो अपनी संवेदनशील जानकारी का ऐक्सेस नहीं देते, उनसे अनुमति लेने के लिए ज़रूरी कोशिशें करनी होंगी.(उदाहरण के तौर पर, अगर वे कॉल लॉग का ऐक्सेस नहीं देते, तो उन्हें मैन्युअल तरीके से फ़ोन नंबर डालने की अनुमति देना).

कुछ पाबंदी वाली अनुमतियों पर नीचे बताए गए शर्तों के मुताबिक, दूसरी ज़रूरी शर्तें भी लागू हो सकती हैं. इन पाबंदियों का उद्देश्य ऐप्लिकेशन को इस्तेमाल करने वालों की निजता को सुरक्षित रखना है. हम नीचे दी गई ज़रूरी शर्तों में गिनती के अपवादों की अनुमति दे सकते हैं. ऐसा हम उन बेहद खास मामलों में ही कर सकते हैं जहां ऐप्लिकेशन काफ़ी दमदार या बहुत ज़रूरी सुविधा देते हों और उसे मुहैया कराने का कोई दूसरा तरीका मौजूद नहीं हो. हम प्रस्तावित अपवादों का मूल्यांकन उपयोगकर्ताओं की निजता या सुरक्षा पर पड़ने वाले असर को ध्यान में रखते हुए करते हैं.

मैसेज (एसएमएस) और कॉल लॉग की अनुमतियां

मैसेज (एसएमएस) और कॉल लॉग की अनुमतियों को निजी और संवेदनशील जानकारी नीति और आगे दी गई पाबंदियों के तहत, इस्तेमाल करने वाले का संवेदनशील डेटा माना जाता है:

पाबंदी वाली अनुमति	ज़रूरत
कॉल लॉग अनुमति ग्रुप (जैसे READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमएस) या सहायक हैंडलर के रूप में सक्रिय तौर पर रजिस्टर किया जाना चाहिए.

मैसेज (एसएमएस) अनुमति ग्रुप (जैसे READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमए) या सहायक हैंडलर के रूप में सक्रिय रूप से रजिस्टर किया जाना चाहिए.

जिन ऐप्लिकेशन में डिफ़ॉल्ट मैसेज (एसएमएस), फ़ोन या सहायक हैंडलर की सुविधा नहीं है, हो सकता है कि वे मेनिफ़ेस्ट में ऊपर दी गई अनुमतियों के बारे में न बताएं. इसमें मेनिफ़ेस्ट का प्लेसहोल्डर टेक्स्ट भी शामिल है. इसके अलावा, ऐप्लिकेशन इस्तेमाल करने वालों को ऊपर दी गई कोई भी अनुमति स्वीकार करने का संकेत देने से पहले, मैसेज (एसएमएस), फ़ोन या सहायक हैंडलर के रूप में ऐप्लिकेशन रजिस्टर होने चाहिए और जब वे डिफ़ॉल्ट हैंडलर न रह जाएं, तो उन्हें उसी समय अनुमति का इस्तेमाल करना बंद कर देना चाहिए. अनुमति दिए गए इस्तेमाल और अपवाद इस सहायता केंद्र पेज पर दिए गए हैं.

ऐप्लिकेशन सिर्फ़ अनुमति मिली हुई मुख्य फ़ंक्शन की सुविधा देने के लिए अनुमति (और अनुमति से पाए हुए किसी भी डेटा) का इस्तेमाल कर सकते हैं. मुख्य फ़ंक्शन की सुविधा को ऐप्लिकेशन के खास मकसद के तौर पर बताया गया है. इसमें मुख्य सुविधाओं का एक सेट शामिल हो सकता है, जिन्हें ऐप्लिकेशन की जानकारी में खास तौर से बताया जाना चाहिए और उनका प्रचार किया जाना चाहिए. मुख्य सुविधा (सुविधाओं) के बिना ऐप्लिकेशन "अधूरा" रहता है या किसी काम का नहीं रहता. इस डेटा का ट्रांसफ़र, शेयर करना या लाइसेंस लेकर किया गया इस्तेमाल, सिर्फ़ ऐप्लिकेशन के अंदर मुख्य सुविधाओं या सेवाओं को देने के लिए होना चाहिए. इसका इस्तेमाल किसी और मकसद (जैसे दूसरे ऐप्लिकेशन या सेवाओं, विज्ञापन या मार्केटिंग उद्देश्यों में सुधार) के लिए बढ़ाया नहीं जा सकता है. डेटा पाने के लिए आप दूसरे तरीकों (दूसरी अनुमतियों, एपीआई, या तीसरे-पक्ष स्रोतों सहित) का इस्तेमाल नहीं कर सकते हैं. जिसमें ऊपर बताई गई अनुमतियां शामिल हैं.

जगह की जानकारी की अनुमतियां

16 अप्रैल, 2020 के लिए अपडेट: हम जानते हैं कि जगह की जानकारी से जुड़ी हमारी नीति का पालन करने के लिए, कई डेवलपर को अपने ऐप्लिकेशन पर बहुत काम करना हो सकता है. इसलिए, ऐप्लिकेशन में कोई भी ज़रूरी बदलाव करने के लिए हम आपको ज़्यादा समय दे रहे हैं. समयावधि और नए अपडेट की जानकारी पाने के लिए, कृपया सहायता केंद्र पर जाएं.

डिवाइस की जगह की जानकारी निजी और संवेदनशील मानी जाती है. यह निजी और संवेदनशील जानकारी नीति के तहत आती है और इसके लिए इन बातों का ध्यान रखा जाता है:

- ऐप्लिकेशन, जगह की जानकारी के ऐक्सेस से सुरक्षित डेटा तक नहीं पहुंच सकते हैं (उदाहरण के लिए, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) इसके बाद आपके ऐप्लिकेशन में मौजूदा सुविधाएं या सेवाएं देने की ज़रूरत नहीं है.
- सिर्फ़ विज्ञापन दिखाने या आंकड़े पाने के लिए, आपको कभी भी ऐप्लिकेशन इस्तेमाल करने वालों से जगह की जानकारी इस्तेमाल करने की अनुमति नहीं मांगनी चाहिए. विज्ञापन दिखाने के लिए इस डेटा के इस्तेमाल की अनुमति देने वाले ऐप्लिकेशन को हमारी विज्ञापन नीति के मुताबिक होना चाहिए.
- ऐप्लिकेशन को मौजूदा सुविधा या सेवा देने के लिए सबसे कम ज़रूरी दायरे (यानी, अच्छे की बजाय ठीक, और बैकग्राउंड की बजाय फ़ॉरग्राउंड) का अनुरोध करना चाहिए जो ज़रूरी है. साथ ही, इस्तेमाल करने वालों को यह उम्मीद करनी चाहिए कि सुविधा या सेवा को जगह की उतनी जानकारी की ज़रूरत है जितनी के ऐक्सेस का अनुरोध किया गया है. उदाहरण के लिए, हम ऐसे ऐप्लिकेशन अस्वीकार कर सकते हैं जो कोई खास वजह बताए बिना बैकग्राउंड की जगह की जानकारी का अनुरोध करते हैं या इसे ऐक्सेस करते हैं.

बैकग्राउंड में जगह की जानकारी का इस्तेमाल सिर्फ़ ऐसी सुविधाएं देने के लिए हो सकता है जो ऐप्लिकेशन इस्तेमाल करने वालों के लिए फ़ायदेमंद हों और ऐप्लिकेशन के मुख्य फ़ंक्शन से जुड़ी हों.

फ़ॉरग्राउंड सेवा (ऐप्लिकेशन के पास ऐक्सेस सिर्फ़ तब हो, जब वह स्क्रीन पर दिख रहा हो, जैसे कि "इस्तेमाल के दौरान") की अनुमति का इस्तेमाल करके, ऐप्लिकेशन की जगह की जानकारी को ऐक्सेस कर सकते हैं. ऐसा सिर्फ़ तब होना चाहिए, जब जगह की जानकारी का इस्तेमाल:

ऐप्लिकेशन इस्तेमाल करने वालों की शुरू की गई इन-ऐप्लिकेशन कार्रवाई को जारी रखने के लिए करना पड़े और
ऐप्लिकेशन इस्तेमाल करने वालों की शुरू की गई कार्रवाई के सभी चरण पूरे होने के बाद इसे तुरंत बंद कर दिया जाए.

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को परिवार के लिए बनाए गए ऐप्लिकेशन की नीति का पालन करना होगा.

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो उपयोगकर्ता के डिवाइस, किसी दूसरे डिवाइस या कंप्यूटर, सर्वर, नेटवर्क, ऐप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई) या सेवाओं में दखल देते हैं, उनमें गड़बड़ी या नुकसान करते हैं या गलत तरीके से उन्हें ऐक्सेस करते हैं. साथ ही, इनमें डिवाइस पर मौजूद दूसरे ऐप्लिकेशन, Google की कोई सेवा या अनुमति पा चुके इंटरनेट सेवा देने वाली कंपनी के नेटवर्क भी शामिल हैं. हालांकि, यह इन तक ही सीमित नहीं है.

Google Play के ऐप्लिकेशन को, Google Play पर मौजूद मुख्य ऐप्लिकेशन से जुड़े क्वालिटी के दिशा-निर्देशों में बताए गए, डिफ़ॉल्ट Android सिस्टम ऑप्टिमाइज़ेशन की ज़रूरी शर्तों को पूरा करना होगा.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने पर अन्य ऐप्लिकेशन को ब्लॉक कर देते हैं या फिर उसमें रुकावट डालते हैं.
गेम में धोखाधड़ी करने वाले ऐप्लिकेशन जो अन्य ऐप्लिकेशन के गेमप्ले पर असर डालते हैं.
ऐसे ऐप्लिकेशन जो ऐप्लिकेशन की सेवाओं, उसके सॉफ़्टवेयर या हार्डवेयर को हैक करने का तरीका बताते हैं. साथ ही, वे उसके सुरक्षा उपायों को बिगाड़ने में भी मदद करते हैं.
ऐसे ऐप्लिकेशन जो किसी सेवा या एपीआई का उपयोग इस तरह करते हैं जिससे उसके सेवा की शर्तों का उल्लंघन होता है.
ऐसे ऐप्लिकेशन जो सिस्टम के पावर प्रबंधन को अनदेखा करते हैं उन्हें व्हाइटलिस्ट करने की मंज़ूरी नहीं दी जाती.
ऐसे ऐप्लिकेशन जो तीसरे पक्ष के लिए प्रॉक्सी सेवा देते हैं. वे सिर्फ़ उन ऐप्लिकेशन में ऐसा कर सकते हैं जिनका मुख्य मकसद उपयोगकर्ता को प्रॉक्सी सेवा देना है.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो डेटा चुराते हैं, गुप्त तरह से उपयोगकर्ताओं पर निगरानी रखते हैं या उन्हें नुकसान पहुंचाते हैं.

Google Play के ज़रिए दिया जाने वाला ऐप्लिकेशन, Google Play के अपडेट करने के तरीके के अलावा किसी दूसरे तरीके का इस्तेमाल करके खुद में बदलाव, अपडेट नहीं कर सकता और न ही किसी की जगह ले सकता है. इसी तरह, कोई ऐप्लिकेशन Google Play के अलावा किसी दूसरे स्रोत से एक्ज़ीक्यूटेबल कोड (उदा. dex, JAR, .so फ़ाइलें) डाउनलोड नहीं कर सकता. यह प्रतिबंध ऐसे कोड पर लागू नहीं होता जो किसी वर्चुअल मशीन पर काम करता है और जिसके पास Android API (जैसे कि वेबव्यू या ब्राउज़र में JavaScript) का सीमित ऐक्सेस होता है.

ऐप्लिकेशन के दूसरे संसाधन (जैसे कि गेम एसेट) सिर्फ़ तब डाउनलोड किए जा सकेंगे, जब वे उपयोगकर्ता के ऐप्लिकेशन में इस्तेमाल के लिए बहुत ज़रूरी हों और डाउनलोड किए गए संसाधन, Google Play नीतियों के मुताबिक बने हों. इसके साथ ही, डाउनलोड करने से पहले ऐप्लिकेशन में उपयोगकर्ताओं को डाउनलोड साइज़ के बारे में साफ़ तौर पर बताया जाना चाहिए.

Google Play पर निगरानी और कारोबारी स्पायवेयर ऐप्लिकेशन की साफ़ तौर पर पाबंदी है. स्टोर पर सिर्फ़ ऐसे ऐप्लिकेशन की अनुमति है जो नीति का पालन करते हैं, जिन्हें खास तौर पर अभिभावकों (परिवार के साथ) की निगरानी या एंटरप्राइज़ प्रबंधन के लिए बनाया और प्रचार किया गया है. उनमें ट्रैक करने और रिपोर्ट करने की सुविधा होनी चाहिए, चाहें वे नीचे दी गई ज़रूरतों को पूरी तरह से पालन करते हों.

नीचे दी गई चीज़ें साफ़ तौर से प्रतिबंधित हैं:

- वायरस, ट्रोजन हॉर्स, मैलवेयर, स्पायवेयर या कोई भी दूसरा नुकसान पहुंचाने वाला सॉफ़्टवेयर.
- ऐसे ऐप्लिकेशन जो नुकसान पहुंचाने वाले सॉफ़्टवेयर से जुड़े होते हैं या उनके वितरण या इंस्टॉल करने को बढ़ावा देते हैं.
- ऐसे ऐप्लिकेशन या SDK जो Google Play के बजाय किसी दूसरे स्रोत से इस्तेमाल किए जा सकने वाला कोड डाउनलोड करते हैं. इस तरह के कोड में dex फ़ाइलें और स्थानीय कोड शामिल हैं.
- ऐसे ऐप्लिकेशन जो सुरक्षा में जोखिम की संभावना पैदा करते हैं या उनका फ़ायदा उठाते हैं.
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले की पुष्टि करने की जानकारी (जैसे कि उपयोगकर्ता नाम और पासवर्ड) चुराते हैं. ये किसी दूसरे ऐप्लिकेशन या वेबसाइट की नकल करके, उपयोगकर्ताओं को धोखे से अपनी निजी जानकारी या पुष्टि करने की जानकारी देने के लिए कहते हैं.
- ऐसे ऐप्लिकेशन जो यह नहीं बताते हैं कि उनकी पुष्टि नहीं हुई है या असली फ़ोन नंबर, संपर्क, पता नहीं दिखाते हैं या किसी कंपनी या व्यक्ति की सहमति के बिना व्यक्तिगत रूप से पहचान करने वाली जानकारी दिखाते हैं.
- ऐसे ऐप्लिकेशन जो उपयोगकर्ता की पहले से सहमति लिए बिना किसी डिवाइस पर दूसरे ऐप्लिकेशन इंस्टॉल करते हैं.
- कॉन्टेंट डिलीवरी नेटवर्क (सीडीएन) से डाउनलोड किए जा सकने वाले ऐसे ऐप्लिकेशन जो डाउनलोड होने से पहले उपयोगकर्ता को डाउनलोड साइज़ के बारे में साफ़ तौर पर नहीं बताते हैं.
- ऐसे ऐप्लिकेशन जिन्हें गुप्त तरह से डिवाइस के इस्तेमाल की जानकारी एकत्रित करने के लिए डिज़ाइन किया गया है, जैसे कि कारोबारी स्पायवेयर ऐप्लिकेशन.

ऐसे ऐप्लिकेशन जो किसी डिवाइस पर इस्तेमाल करने वाले के व्यवहार को ट्रैक या मॉनिटर करते हैं, उनके लिए ये शर्तें ज़रूरी हैं:

- ऐप्लिकेशन को जासूसी के काम के लिए बने या गुप्त निगरानी समाधान के तौर पर खुद को पेश नहीं करना चाहिए.
- ऐप्लिकेशन को निगरानी से जुड़ी गतिविधियां नहीं छिपानी चाहिए या उससे जुड़ी गलत जानकारी नहीं देनी चाहिए. साथ ही, इसे इस तरह की किसी भी सुविधा के बारे में उपयोगकर्ता को गुमराह नहीं करना चाहिए.
- उपयोगकर्ताओं को लगातार सूचनाएं और एक खास तरह का आइकॉन दिखाया जाना चाहिए जिससे ऐप्लिकेशन को आसानी से पहचाना जा सके.
- Google Play पर ऐप्लिकेशन या ऐप लिस्टिंग, कुछ शर्तों का उल्लंघन करने वाले ऐप्लिकेशन को किसी भी तरीके से चालू करने या उसे ऐक्सेस करने का कोई भी तरीका उपलब्ध नहीं कराना चाहिए. इन शर्तों में Google Play के बाहर होस्ट किए गए गैर-अनुपालन वाले APK से लिंक करना शामिल है.

अपने ऐप्लिकेशन के लिए टारगेट की गई स्थान-भाषा की सभी कानूनी ज़िम्मेदारी आपकी है. जिन जगहों पर ऐप्लिकेशन प्रकाशित है. अगर वहां उसे गैरकानूनी बताया जाता है, तो उस ऐप्लिकेशन को हटा दिया जाएगा.

Google Play पर डेवलपर के लिए हाल ही में फ़्लैग की गई सुरक्षा की समस्याओं के बारे में जानने के लिए हमारी ऐप्लिकेशन की सुरक्षा बढ़ाने वाला प्रोग्रामदेखें. जोखिम की संभावना और उससे निपटने के बारे में जानकारी, हर कैंपेन के सहायता पेज के लिंक पर उपलब्ध है.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो उपयोगकर्ताओं के साथ धोखाधड़ी करते हों या बेईमानी करते हों. साथ ही, ऐसे ऐप्लिकेशन के बारे में गुमराह करते हों जिनका फ़ंक्शन करना संभव नहीं है. ऐप्लकेशन के लिए ज़रूरी है कि वे पूरे मेटाडेटा में अपनी कार्रवाइयों और सुविधाओं के बारे में सटीक जानकारी, विवरण और फ़ोटो/वीडियो दें. साथ ही, इस जानकारी के आधार पर उपयोगकर्ताओं की उम्मीद के हिसाब से काम भी करें. ऐप्लिकेशन को ऑपरेटिंग सिस्टम या दूसरे ऐप्लिकेशन के फ़ंक्शन या चेतावनियों की नकल करने की कोशिश नहीं करनी चाहिए. डिवाइस की सेटिंग में किया जाने वाला कोई भी बदलाव उपयोगकर्ता की जानकारी और सहमति से किया जाना चाहिए. ये बदलाव ऐसे हों जिन्हें उपयोगकर्ता आसानी से पहले जैसा कर सके.

गुमराह करने वाले दावे

हम उन ऐप्लिकेशन की अनुमति नहीं देते हैं जिनमें झूठी या गुमराह करने वाली जानकारी या दावे शामिल होते हैं. इस जानकारी में, ब्यौरा, शीर्षक, आइकॉन, और स्क्रीनशॉट शामिल हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

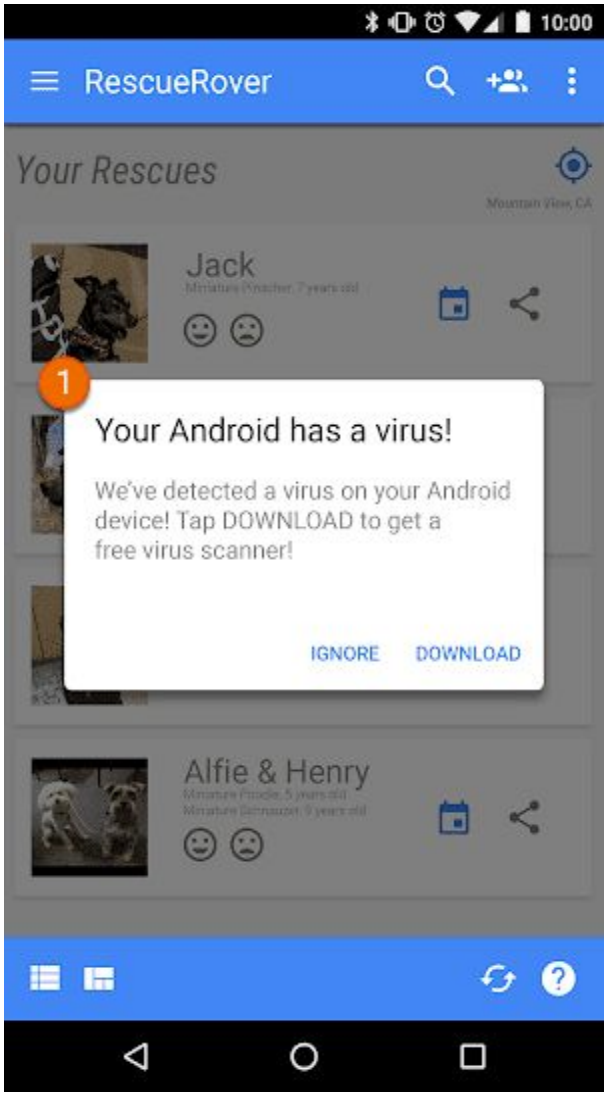
वैसे ऐप्लिकेशन जो अपने फ़ंक्शन को गलत तरीके से पेश करते हैं या पूरी जानकारी नहीं देते हैं:
- वो ऐप्लिकेशन जो ब्यौरे और स्क्रीनशॉट में रेसिंग गेम होने का दावा करता है, लेकिन वास्तव में, वह पहेली वाला गेम होता है जिसमें कार की फ़ोटो का इस्तेमाल किया जाता है.
- वो ऐप्लिकेशन जो एंटीवायरस ऐप्लिकेशन होने का दावा करता है, लेकिन उसमें सिर्फ़ वायरस हटाने का तरीका बताने वाली गाइड दी गई हो.

ऐसे डेवलपर और ऐप्लिकेशन के नाम जो Google Play पर अपनी मौजूदा स्थिति या प्रदर्शन को गलत तरीके से दिखाते हैं. (उदाहरण के लिए, "संपादक की पसंद," "नंबर 1 ऐप्लिकेशन," "टॉप सशुल्क").
वैसे ऐप्लिकेशन जिनमें दवाई या स्वास्थ्य से जुड़ा ऐसा कॉन्टेंट शामिल हैं जो गुमराह करने वाला या संभावित रूप से हानि पहुंचा सकता हो.
वैसे ऐप्लिकेशन जो ऐसी सुविधाएं देने का दावा करते हैं जो नहीं दी जा सकती हैं.
वैसे ऐप्लिकेशन जिन्हें गलत तरह के ऐप्लिकेशन के साथ रखा गया हो.
गुमराह करने वाला ऐसा कॉन्टेंट जिसका इस्तेमाल मतदान की प्रक्रिया में दखल देने के लिए हो सकता है.
वैसे ऐप्लिकेशन जो सरकार की किसी इकाई से संबद्धता का झूठा दावा करते हैं या ऐसी सरकारी सेवाएं देने का दावा करते हैं जिनकी उन्हें अनुमति नहीं है.

सिस्टम के फंक्शन का गलत या गैरकानूनी इस्तेमाल

हम ऐसे ऐप्लिकेशन या विज्ञापनों की अनुमति नहीं देते हैं जो सूचना या चेतावनी जैसे सिस्टम के फ़ंक्शन की नकल करते हैं या उसमें दखल देते हैं. सिस्टम के लेवल से मिलने वाली सूचनाओं का उपयोग सिर्फ़ किसी ऐप्लिकेशन की अंदरूनी सुविधाओं के लिए किया जा सकता है, जैसे कोई ऐसा एयरलाइन ऐप्लिकेशन जो उपयोगकर्ताओं को विशेष ऑफ़र के बारे में सूचित करता है या ऐसा गेम जो उपयोगकर्ताओं को गेम में प्रचारों के बारे में सूचित करता है.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे ऐप्लिकेशन या विज्ञापन जिन्हें सूचना या चेतावनी के रूप में भेजा जाता है:



① इस ऐप्लिकेशन में नज़र आ रही सूचना का इस्तेमाल विज्ञापन देने के लिए किया जा रहा है.

विज्ञापनों से जुड़े अन्य उदाहरणों के लिए, कृपया विज्ञापन नीति देखें.

डिवाइस की सेटिंग में, गुमराह करने वाले बदलाव

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो उपयोगकर्ता की जानकारी और सहमति के बगैर, उनके डिवाइस की सेटिंग या सुविधाओं में बदलाव कर देते हैं. डिवाइस की सेटिंग और सुविधाओं में, सिस्टम और ब्राउज़र की सेटिंग, बुकमार्क, शॉर्टकट, आइकॉन, विजेट, और होमस्क्रीन पर ऐप्लिकेशन के दिखने से जुड़ी चीज़ें शामिल हैं.

इसके अलावा, हम इस तरह के ऐप्लिकेशन को भी अनुमति नहीं देते हैं:

> वैसे ऐप्लिकेशन जो डिवाइस की सेटिंग या सुविधाओं में बदलाव तो उपयोगकर्ता की सहमति से करते हैं, लेकिन ये बदलाव इस तरह किए जाते हैं कि इन्हें पहले जैसा करना आसान नहीं होता.

वैसे ऐप्लिकेशन या विज्ञापन जो तीसरे पक्ष की सेवाओं को पूरा करने या विज्ञापन दिखाने के मकसद से, डिवाइस की सेटिंग या सुविधाओं में बदलाव कर देते हैं.
वैसे ऐप्लिकेशन जो तीसरे पक्ष के ऐप्लिकेशन को हटाने या बंद करने के लिए या डिवाइस की सेटिंग या सुविधा में बदलाव के लिए, उपयोगकर्ताओं को गुमराह करते हैं.
वैसे ऐप्लिकेशन जो उपयोगकर्ताओं को, तीसरे पक्ष के ऐप्लिकेशन हटाने या बंद करने या डिवाइस की सेटिंग और सुविधाओं में बदलाव करने का बढ़ावा देते हैं. ऐसे ऐप्लिकेशन को तब तक अनुमति नहीं दी जाती है, जब तक वह किसी ऐसी सुरक्षा सेवा का हिस्सा न हो जिसकी पुष्टि हो चुकी हो.

धोखाधड़ी को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो लोगों को गुमराह करने में उपयोगकर्ताओं की मदद करते हैं या जिनका मकसद किसी भी तरीके की धोखाधड़ी हो. ऐसे ही कुछ ऐप्लिकेशन के उदाहरण हैं: आईडी कार्ड, सामाजिक सुरक्षा संख्या, पासपोर्ट, डिप्लोमा, क्रेडिट कार्ड, और ड्राइविंग लाइसेंस. ऐप्लिकेशन के कॉन्टेंट और उसके इस्तेमाल के बारे में सटीक जानकारी देनी होगी. जैसे, ऐप्लिकेशन का शीर्षक, उसका ब्यौरा, और इमेज/वीडियो वगैरह. साथ ही, ऐप्लिकेशन को इस्तेमाल करने का अनुभव बिल्कुल वैसा ही होना चाहिए जैसा उपयोगकर्ता ने उम्मीद की थी.

अगर किसी ऐप्लिकेशन के लिए दावा किया जाता है कि उसका मकसद "मनोरंजन के लिए" (या ऐसी ही मिलती-जुलती बात) "शरारत" करने से जुड़ा है, तो इससे ऐप्लिकेशन को हमारी नीतियों से छूट नहीं मिल जाती.

ऐसा कॉन्टेंट जिसमें छेड़छाड़ की गई हो

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो गुमराह करने वाली जानकारी का प्रचार करते हैं या इसे बनाने में मदद करते हैं. ये ऐप्लिकेशन तस्वीरों वीडियो और/या टेक्स्ट से गुमराह करने वाले दावे करते हैं या जानकारी का प्रचार करते हैं. हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो हमेशा गुमराह करने वाली जानकारी का प्रचार करते हैं या ऐसी तस्वीरों, वीडियो और/या टेक्स्ट का प्रचार करते हैं जो धोखाधड़ी को बढ़ावा देते है. इनकी वजह से संवेदनशील कार्यक्रम, राजनीतिक, सामाजिक या दूसरे सार्वजनिक मामलों को नुकसान पहुंच सकता है.

कुछ ऐप्लिकेशन चीज़ों को साफ़ तौर पर दिखाने या क्वालिटी सुधारने के लिए, पारंपरिक और संपादकीय रूप से स्वीकार किए गए कॉन्टेंट में बदलाव करते हैं या उन्हें दूसरे तरीके से दिखाते हैं. ऐसे ऐप्लिकेशन को साफ़ तौर पर कॉन्टेंट में बदलाव की जानकारी देनी चाहिए या वॉटरमार्क के साथ पेश करना चाहिए. इससे एक आम व्यक्ति को यह पता चल सकेगा कि सामग्री में बदलाव किया गया है. लोगों की रुचि, व्यंग्य या पैरोडी वाली सामग्री के लिए छूट मिल सकती है.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

वैसे ऐप्लिकेशन जो किसी जानी-मानी हस्ती को, राजनीतिक रूप से संवेदनशील कार्यक्रम के विरोध-प्रदर्शनों से जोड़कर दिखाते हैं.
वैसे ऐप्लिकेशन जो अपने स्टोर पेज पर वीडियो/फ़ोटो में बदलाव करने की अपनी सुविधा का प्रचार करने के लिए, किसी संवेदनशील कार्यक्रम से ली गई मीडिया या जानी-मानी हस्ती के फ़ुटेज का इस्तेमाल करते हैं.
वैसे ऐप्लिकेशन जो मीडिया क्लिप में बदलाव करके, किसी न्यूज़ ब्रॉडकास्ट की नकल करते हैं.

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को मंज़ूरी नहीं देते जो किसी दूसरे व्यक्ति या संगठन के नाम पर काम करते हों. साथ ही, हम उन ऐप्लिकेशन या डेवलपर खातों को भी मंज़ूरी नहीं देते जो किसी दूसरे व्यक्ति या संगठन के मालिकाना हक या असल मकसद को छिपाते हों या गलत तरीके से पेश करते हों. हम ऐसे ऐप्लिकेशन या डेवलपर

खातों को मंज़ूरी नहीं देते हैं, जिनमें उपयोगकर्ताओं को गुमराह करने वाली गतिविधियां की जा रही हों. इसमें ऐसे ऐप्लिकेशन या डेवलपर खाते शामिल हैं, जो अपने मूल देश के बारे में गलतबयानी करते हैं या अपने मूल देश को छिपाते हैं या किसी दूसरे देश के उपयोगकर्ताओं को टारगेट करते हैं. लेकिन यह इन्हीं तक सीमित नहीं है.

हमारी मैलवेयर नीति बहुत आसान है. Android इकोसिस्टम, 'Google Play स्टोर' और उपयोगकर्ता के डिवाइस को इसमें शामिल करते हैं, जो उन्हें नुकसान पहुंचाने वाली गतिविधियों (जैसे कि मैलवेयर) से दूर रखने में मदद करता हैं. अपने इस बुनियादी सिद्धांत से हम लोगों को और उनके Android डिवाइस को एक सुरक्षित Android इकोसिस्टम देने की कोशिश कर रहे हैं.

मैलवेयर एक ऐसा कोड है जो उपयोगकर्ता को, उनके डेटा या डिवाइस को खतरे में डाल सकता है. मैलवेयर में नुकसान पहुंचा सकने वाले ऐप्लिकेशन (पीएचए), बाइनरी या फ़्रेमवर्क में बदलाव के साथ दूसरी खतरनाक चीज़ें भी शामिल हो सकती हैं. इसमें ट्रोजन, फ़िशिंग, और स्पायवेयर ऐप्लिकेशन जैसी श्रेणियां शामिल हैं जिसमें हम लगातार नई श्रेणियों को अपडेट और जोड़ रहे हैं.

हालांकि, मैलवेयर कई तरह के होते हैं और उसके नुकसान पहुंचाने की क्षमता अलग-अलग होती है, फिर भी उनका मकसद इनमें से एक होता है:

- उपयोगकर्ता के डिवाइस की सुरक्षा खतरे में डालना.
- उपयोगकर्ता के डिवाइस को कंट्रोल करना.
- किसी साइबर हमलावर को कहीं से भी उपयोगकर्ता का डिवाइस ऐक्सेस करने देना, ताकि वह डिवाइस का गलत इस्तेमाल कर सके या डिवाइस को नुकसान पहुंचा सके.
- उपयोगकर्ता की सहमति या जानकारी के बिना, डिवाइस से निजी डेटा शेयर करना या क्रेडेंशियल चुराना.
- किसी मैलवेयर वाले डिवाइस से दूसरे डिवाइस को प्रभावित करने के लिए नेटवर्क पर स्पैम या खतरा पैदा करने वाले निर्देश फैलाना.
- उपयोगकर्ता से धोखाधड़ी करना.

किसी ऐप्लिकेशन, बाइनरी या फ़्रेमवर्क में बदलाव करना खतरनाक हो सकता है, क्योंकि इसमें नुकसान पहुंचाने वाली चीज़ें भी शामिल हो सकती हैं, भले ही उसका इरादा खतरा पैदा करना न हो. ऐसा इसलिए होता है, क्योंकि ऐप्लिकेशन, बाइनरी, या फ़्रेमवर्क में बदलाव होने पर, कई तरह के वैरिएबल के मौजूद होने की वजह से यह गलत काम करता है. इसलिए, अगर कोई चीज़ एक Android डिवाइस के लिए खतरनाक है, तो यह ज़रूरी नहीं कि वह दूसरे डिवाइस के लिए भी खतरनाक हो. उदाहरण के लिए, कुछ ऐप्लिकेशन डिवाइस को नुकसान पहुंचाने के लिए पुराने एपीआई का इस्तेमाल करते हैं. Android के नए वर्शन का इस्तेमाल करने वाले डिवाइस पर ऐसे ऐप्लिकेशन का असर नहीं पड़ता. हालांकि, पुराने वर्शन वाले Android डिवाइस को इससे खतरा हो सकता है. ऐप्लिकेशन, बाइनरी या फ़्रेमवर्क में हुए बदलाव को मैलवेयर या पीएचए के रूप में फ़्लैग किया जाता है. ऐसा तब किया जाता है, जब वे कुछ या सभी Android डिवाइस और उपयोगकर्ताओं के लिए खतरा पैदा करते हों.

नीचे दी गई मैलवेयर श्रेणियां, हमारी उस सोच के बारे में बताती हैं कि उपयोगकर्ता इस बात को समझें कि कैसे उनके डिवाइस को सुरक्षित तरीके से इस्तेमाल करने के लिए बनाया जा रहा है. यह सुरक्षित इकोसिस्टम को बेहतर बनाने में बढ़ावा देता है, ताकि उपयोगकर्ता का अनुभव भरोसेमंद हो.

ज़्यादा जानकारी के लिए Google Play Protect पर जाएं.

बैकडोर

इस कोड की मदद से डिवाइस पर अनचाही, नुकसान पहुंचाने वाली, और कहीं से भी कंट्रोल की जाने वाली कार्रवाइयां की जा सकती हैं.

इन कार्रवाइयों में ऐसी गतिविधि शामिल हो सकती है जो उपयोगकर्ता की अनुमति के बिना ही, ऐप्लिकेशन, बाइनरी या फ़्रेमवर्क में हुए बदलाव को किसी भी तरह के मैलवेयर में शामिल कर सकती है. सामान्य तौर पर, बैकडोर की मदद से यह देखा जाता है कि किसी डिवाइस पर किस तरह नुकसान पहुंचा रहा है. इसीलिए, यह बिलिंग से जुड़ी धोखाधड़ी करने वाली या कारोबारी स्पायवेयर से थोड़ा अलग होता है. इस वजह से, कुछ मामलों में बैकडोर के खास सेट को Google Play Protect को जोख़िम से भरा माना जाता है.

बिलिंग से जुड़ी धोखाधड़ी करना

ऐसा कोड जिसके ज़रिए उपयोगकर्ता से जान-बूझकर और धोखाधड़ी करके, अपने-आप शुल्क लिया जाता है.

मोबाइल बिलिंग से जुड़ी धोखाधड़ी में, मैसेज (एसएमएस), कॉल, और टोल नंबर से धोखाधड़ी करना शामिल है.

मैसेज से धोखाधड़ी करने वाला

ऐसा कोड जो उपयोगकर्ताओं से बिना उनकी अनुमति के प्रीमियम मैसेज भेजने पर शुल्क लेता है. इसके अलावा, पहचान ज़ाहिर करने वाले समझौतों को छिपाते हुए, ऐसे मैसेज भेजता है जिससे उपयोगकर्ता को अनजाने में शुल्क देना पड़ता है. इतना ही नहीं, धोखाधड़ी करने वाला, उपयोगकर्ताओं को मोबाइल सेवा देने वाली कंपनी की तरफ़ से ऐसे मैसेज भेजता है जिनमें शुल्क काटने या सदस्यताएं लेने की पुष्टि करने की जानकारी होती है.

कुछ कोड भले ही तकनीकी रूप से मैसेज भेजने से जुड़ी शर्तों को ज़ाहिर करते हैं, लेकिन उनमें दूसरे तरीकों से मैसेज से की जाने वाली धोखाधड़ी शामिल होती है. इसमें उपयोगकर्ता से किसी शर्त को ज़ाहिर करने के समझौते का हिस्सा छिपाया जाता है और इन शर्तों को न पढ़ने लायक भी बनाया जाता है. साथ ही, इसमें वे मैसेज शामिल होते हैं जो लोगों को मोबाइल सेवा देने वाली कंपनी की तरफ़ से शुल्क काटने या सदस्यता लेने की पुष्टि करने की जानकारी देते हैं.

कॉल से धोखाधड़ी

करने वाला कोड, वह कोड होता है जो उपयोगकर्ता से बिना उनकी अनुमति के प्रीमियम नंबर पर कॉल करके, शुल्क लेता है.

टोल नंबर से धोखाधड़ी

करने वाला कोड, वह कोड होता है जिससे उपयोगकर्ता अनजाने में अपने मोबाइल फ़ोन के बिल से सामग्री खरीदते या सदस्यता लेते हैं.

टोल नंबर से होने वाली धोखाधड़ी में प्रीमियम मैसेज और प्रीमियम कॉल को छोड़कर बिलिंग से जुड़ी किसी भी तरह की धोखाधड़ी शामिल होती है. इसमें डायरेक्ट कैरियर बिलिंग, वायरलेस ऐक्सेस पॉइंट (WAP), और मोबाइल सेवा के इस्तेमाल पर लगने वाले शुल्क को ट्रांसफ़र करना शामिल है. टोल नंबर से होने वाली धोखाधड़ी में सबसे ज़्यादा धोखाधड़ी WAP से होती है. WAP से होने वाली धोखाधड़ी में, उपयोगकर्ताओं को धोखे से किसी बटन पर क्लिक करवाकर फंसाया जाता है. यह बटन ऐसे वेबव्यू पर होता है जिसे इस्तेमाल करने वाला देख नहीं पाता है और न ही इसके लोड होने का पता चल पाता है. इस कार्रवाई को करने से, बार-बार पैसे देकर ली जाने वाली सदस्यता शुरू हो जाती है. वहीं, इसकी पुष्टि करने वाला मैसेज या ईमेल आम तौर पर हाईजैक कर लिया जाता है, ताकि उपयोगकर्ता को पैसे के लेन-देन की जानकारी न मिल.सके.

कारोबारी स्पायवेयर

ऐसा कोड जो बिना सहमति या सूचना दिए, डिवाइस में मौजूद निजी जानकारी शेयर करता है और इस बारे में लगातार सूचना भी नहीं दिखाता है.

कारोबारी स्पायवेयर ऐप्लिकेशन, पीएचए की सेवा देने वालों के अलावा, किसी दूसरे पक्ष को डेटा उपलब्ध कराते हैं. इन वैध स्पायवेयर ऐप्लिकेशन का इस्तेमाल करके, अभिभावक अपने बच्चों की गतिविधियों को ट्रैक कर सकते हैं. अगर डेटा शेयर होते समय लगातार दिखने वाली सूचना नहीं दिखती है, तो इन ऐप्लिकेशन से किसी व्यक्ति (उदाहरण के लिए, पति/पत्नी) को बिना बताए या अनुमति लिए बिना, उसकी गतिविधियों को ट्रैक नहीं किया जा सकता है.

सेवा में रुकावट (DoS)

यह कोड लोगों को बिना बताए, सेवा में रुकावट (DoS) की समस्या पैदा करता है. इसके अलावा, यह कोड किसी दूसरे सिस्टम और संसाधनों पर सेवा में रुकावट की समस्या पैदा करने वाले मैलवेयर का हिस्सा भी हो सकता है.

उदाहरण के लिए, ऐसा हो सकता है कि अगर भारी संख्या में एचटीटीपी में अनुरोध भेजा, तो इससे रिमोट सर्वर पर काफ़ी लोड हो सकता है.

गलत तरीके से डाउनलोड करने वाले मैलवेयर

वो कोड जो डिवाइस को नुकसान नहीं पहुंचाता हो, लेकिन दूसरे तरह के पीएचए डाउनलोड करता है.

वह कोड जो गलत तरीके से डाउनलोड करने वाला हो सकता है, अगर:

> यह वजह हो सकती है कि इसे पीएचए फ़ैलाने के लिए बनाया गया हो या यह पीएचए डाउनलोड कर सकता है. इसके अलावा, इसमें ऐसा कोड शामिल है जो ऐप्लिकेशन इंस्टॉल और डाउनलोड कर सकता है; इसके ज़रिए डाउनलोड किए गए कम से कम 5% ऐप्लिकेशन ऐसे हो सकते हैं जो पीएचए हों. हमने ऐसा, डाउनलोड किए गए 500 ऐप्लिकेशन में पाया (इनमें 25 पीएचए डाउनलोड देखे गए) है.

मुख्य ब्राउज़र और फ़ाइल शेयर करने वाले ऐप्लिकेशन को तब तक गलत तरीके से डाउनलोड करने वाला नहीं माना जाता, जब तक:

> वे उपयोगकर्ता की अनुमति के बिना डाउनलोड नहीं होते; और
> उपयोगकर्ताओं की अनुमति मिलने पर ही सभी पीएचए डाउनलोड होते हैं.

उस डिवाइस को नुकसान पहुंचाने वाले मैलवेयर जो Android प्लैटफ़ॉर्म पर काम नहीं करते हैं

ऐसा कोड जो Android प्लैटफ़ॉर्म पर काम न करने वाले डिवाइस को नुकसान पहुंचाता है.

ये ऐप्लिकेशन Android उपयोगकर्ता या डिवाइस को नुकसान नहीं पहुंचाते हैं. हालांकि, इनमें ऐसे कॉम्पोनेंट होते हैं जो Android के अलावा, अन्य प्लैटफ़ॉर्म पर चलने वाले डिवाइस को नुकसान पहुंचा सकते हैं.

फ़िशिंग

ऐसा कोड जो किसी भरोसेमंद स्रोत से आने का दावा करता है, उपयोगकर्ता की पुष्टि करने वाले क्रेडेंशियल या बिलिंग जानकारी पाने के लिए अनुरोध करता है, और डेटा को किसी तीसरे पक्ष को भेजता है. यह श्रेणी उस कोड पर भी लागू होती है जो उपयोगकर्ता के क्रेडेंशियल शेयर करते समय उसमें रोक लगाता है.

आम तौर पर, सोशल नेटवर्क और गेम के लिए, फ़िशिंग के टारगेट, बैंकिंग क्रेडेंशियल, क्रेडिट कार्ड नंबर, और खाते के ऑनलाइन क्रेडेंशियल होते हैं.

खास अधिकारों का गलत इस्तेमाल

ऐसा कोड जो ऐप्लिकेशन के सैंडबॉक्स और खास अधिकारों को ऐक्सेस करता है. इसके अलावा, सुरक्षा से जुड़ी मुख्य गतिविधियों के ऐक्सेस को बदलता या उसे ऐक्सेस करने से रोकता है. ऐसा करके, यह कोड उपयोगकर्ता के डिवाइस को खतरे में डालता है.

उदाहरणों में ये शामिल हैं:

- ऐसा ऐप्लिकेशन जो Android की अनुमतियों के मॉडल का उल्लंघन करता है या दूसरे ऐप्लिकेशन से क्रेडेंशियल (जैसे कि OAuth टोकन) चुराता है.
- ऐसे ऐप्लिकेशन जो सुविधाओं का गलत इस्तेमाल करते हैं और खुद को अनइंस्टॉल होने या बंद होने से रोकते हैं.
- ऐसा ऐप्लिकेशन जो SELinux को काम करने से रोकता है.

प्रिविलेज एस्केलेशन ऐप्लिकेशन, जो लोगों की अनुमति के बिना, डिवाइस को रूट करते हैं. वे डिवाइस रूट करने वाले ऐप्लिकेशन की श्रेणी में आते हैं.

रैंसमवेयर

ऐसा कोड जो डिवाइस पर कुछ या पूरा कंट्रोल या डिवाइस में मौजूद डेटा का कंट्रोल अपने पास रखता है. साथ ही, उपयोगकर्ता से पैसे चुकाने या डिवाइस पर ऐसी कार्रवाई करने की मांग करता है जिससे उपयोगकर्ता अपना कंट्रोल ऐप्लिकेशन को सौंप दे.

कुछ रैंसमवेयर, डिवाइस पर डेटा को एन्क्रिप्ट करते हैं और डेटा को पढ़ने लायक बनाने के लिए उपयोगकर्ता से पैसे चुकाने की मांग करते हैं. साथ ही, डिवाइस के एडमिन की सुविधाओं का फ़ायदा उठाते हैं, ताकि उन्हें कोई भी डिवाइस से न हटा सके. उदाहरणों में ये शामिल हैं:

- उपयोगकर्ता को उनके डिवाइस को ऐक्सेस करने से रोकना और उन्हें फिर से कंट्रोल देने के लिए पैसे की मांग करना.
- डिवाइस के डेटा को एन्क्रिप्ट करके, फिर उसी ही डेटा को पढ़ने लायक बनाने के लिए उपयोगकर्ता से पैसे चुकाने की मांग करना.
- डिवाइस नीति प्रबंधक की सुविधाओं का फ़ायदा उठाना और उपयोगकर्ता उन्हें हटा न पाएं, इसलिए उनके ऐक्सेस पर रोक लगाना.

ऐसा कोड जो डिवाइस में पहले से मौजूद होता है उसे रैंसमवेयर की श्रेणी से बाहर रखा जा सकता है. इसका मुख्य काम डिवाइस के प्रबंधन को सब्सडाइज करना है. यह कोड, सुरक्षित लॉक और प्रबंधन के लिए ज़रूरी शर्तें पूरी करता है. साथ ही, उपयोगकर्ताओं को पूरी जानकारी देता है और उनसे सहमति लेने की ज़रूरी शर्तें पूरी करता है.

रूट किया जा रहा है

ऐसा कोड जो डिवाइस को रूट करता है.

नुकसान पहुंचाने के लिए डिवाइस को रूट करने वाला कोड और नुकसान नहीं पहुंचाने वाला कोड, दोनों में अंतर है. उदाहरण के लिए, नुकसान नहीं पहुंचाने के लिए डिवाइस को रूट करने वाले ऐप्लिकेशन, लोगों को डिवाइस रूट करने

की जानकारी पहले ही दे देते हैं. साथ ही, ये ऐप्लिकेशन ऐसी कार्रवाइयां नहीं करते हैं जो डिवाइस की अन्य पीएचए की श्रेणियों पर लागू होती हैं.

नुकसान पहुंचाने के लिए डिवाइस रूट करने वाले ऐप्लिकेशन, लोगों को बिना जानकारी दिए, डिवाइस रूट कर देते हैं. या यह लोगों को रूट करने की जानकारी पहले नहीं देते हैं. इसके अलावा, ये ऐप्लिकेशन दूसरी ऐसी कार्रवाइयां करते हैं जो डिवाइस की अन्य पीएचए श्रेणियों पर लागू होती हैं.

स्पैम

ऐसा कोड जो उपयोगकर्ता के डिवाइस की संपर्क सूची में मौजूद लोगों को अनचाहे मैसेज भेजता है या उनके डिवाइस का इस्तेमाल ईमेल स्पैम भेजने के लिए करता है.

स्पायवेयर

ऐसा कोड जो बिना अनुमति या सूचना के, डिवाइस में मौजूद निजी डेटा को शेयर करता है.

उदाहरण के लिए, ऐसा कोड जो यहां दी गई किसी भी जानकारी को बिना अनुमति के शेयर करता है या ऐसी कार्रवाई करता है जिसकी उम्मीद उपयोगकर्ता नहीं कर सकता, उसे स्पायवेयर माना जाता है:

संपर्क सूची
एसडी कार्ड में सेव फ़ोटो या दूसरी फ़ाइलें जो ऐप्लिकेशन से जुड़ी नहीं हैं
उपयोगकर्ता के ईमेल का कॉन्टेंट
कॉल लॉग
मैसेज (एसएमएस) लॉग
डिफ़ॉल्ट ब्राउज़र का वेब इतिहास या ब्राउज़र के बुकमार्क
दूसरे ऐप्लिकेशन के /डेटा/ डायरेक्ट्री से मिली जानकारी.

ऐसी गतिविधियां जो उपयोगकर्ता की जासूसी कर सकती हैं, उन्हें भी स्पायवेयर माना जा सकता है. उदाहरण के लिए, फ़ोन से ऑडियो रिकॉर्ड करना या फ़ोन कॉल रिकॉर्ड करना और ऐप्लिकेशन का डेटा चुराना.

ट्रोजन

ऐसा कोड जिसकी पहचान बेनाइन के तौर पर होती है, जैसे कि एक ऐसा गेम जो सिर्फ़ गेम होने का दावा करता है, लेकिन ऐप्लिकेशन इस्तेमाल करने वाले लोगों की अनुमति के बिना कार्रवाइयां करता हैं.

आम तौर पर, इस तरह के मैलवेयर किसी दूसरे पीएचए श्रेणियों के साथ मिलकर काम करते हैं. ट्रोजन में एक नुकसान न पहुंचाने वाला कॉम्पोनेंट और एक नुकसान पहुंचाने वाला, छिपा हुआ कॉम्पोनेंट होता है. उदाहरण के लिए, एक गेम जो उपयोगकर्ता की जानकारी के बिना, बैकग्राउंड में ही उसके डिवाइस से प्रीमियम मैसेज भेजता है.

असामान्य ऐप्लिकेशन पर नोट

अगर Google Play Protect के पास किसी नए और असामान्य ऐप्लिकेशन को सुरक्षित बताने के लिए पूरी जानकारी नहीं है, तो इन ऐप्लिकेशन को असामान्य की श्रेणी में रखा जाएगा. इसका मतलब यह नहीं है कि वह ऐप्लिकेशन नुकसान पहुंचाने वाला है. हालांकि, उसकी बिना समीक्षा किए इसे सुरक्षित भी नहीं कहा जा सकता.

बैकडोर वाले मैलवेयर पर नोट

कोड की कार्रवाइयों के आधार पर, बैकडोर मैलवेयर की श्रेणी तय होती है. किसी कोड को तब बैकडोर माना जाता है, जब वह डिवाइस पर नुकसान पहुंचाने वाली गतिविधि को बिना अनुमित के कार्रवाई करने देता है. इसकी वजह से वह कोड किसी अन्य मैलवेयर श्रेणी में शामिल हो सकता है. उदाहरण के लिए, अगर कोई ऐप्लिकेशन डाइनैमिक कोड को लोड होने की अनुमति देता है और यह कोड, मैसेज की जानकारी हासिल करता है, तो इसे बैकडोर मैलवेयर की तरह माना जाएगा.

हालांकि, अगर कोई ऐप्लिकेशन आर्बिट्रेरी कोड को कार्रवाई करने की अनुमति देता है और हमें लगता है कि इस कोड की वजह से डिवाइस को नुकसान पहुंचाने वाली गतिविधि को बढ़ावा नहीं मिला है, तो उस ऐप्लिकेशन को बैकडोर मैलवेयर के तौर पर देखने के बजाय, जोखिम की संभावना वाले ऐप्लिकेशन के तौर पर देखा जाएगा. साथ ही, डेवलपर से इसे पैच करने के लिए कहा जाएगा.

हम ऐसे ऐप्लिकेशन की अनुमति नहीं देते हैं जिनमें धोखाधड़ी या परेशान करने वाले विज्ञापन होते हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं. हम आपके ऐप्लिकेशन में पेश किए गए विज्ञापनों को उस ऐप्लिकेशन का हिस्सा मानते हैं. ऐप्लिकेशन में दिखने वाले विज्ञापन हमारी सभी नीतियों के हिसाब से होने चाहिए. जुए के विज्ञापनों से जुड़ी नीतियों के लिए, कृपया यहां क्लिक करें.
Google Play, डेवलपर और उपयोगकर्ताओं को फ़ायदे देने के लिए कमाई करने के कई तरीके उपलब्ध कराता है. इनमें पैसे देकर खरीदे जाने वाले ऐप्लिकेशन मुहैया कराना, ऐप्लिकेशन में उत्पादों की पेशकश करना, सदस्यताएं देना, और अलग-अलग तरह के विज्ञापन मॉडल के हिसाब से ऐप्लिकेशन तैयार करने जैसे तरीके शामिल हैं. अपने उपयोगकर्ताओं को बेहतर अनुभव देने के लिए, हम चाहते हैं कि आप इन नीतियों का पालन करें.

पैसे चुकाना

ऐसे ऐप्लिकेशन जो इन-स्टोर या इन-ऐप्लिकेशन खरीदारी की सुविधा देते हैं उन्हें नीचे दिए गए दिशा-निर्देशों का पालन करना होगा:

इन-स्टोर खरीदारी:Google Play से ऐप्लिकेशन और डाउनलोड करने के लिए शुल्क लेने वाले डेवलपर को, Google Play के पैसे चुकाने के तरीके का इस्तेमाल करना होगा.

इन-ऐप्लिकेशन खरीदारी:

- Google Play पर डाउनलोड किए गए गेम में उत्पाद ऑफ़र करने वाले या गेम के कॉन्टेंट का ऐक्सेस देने वाले डेवलपर को पैसे चुकाने तरीके के लिए, Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करना चाहिए.
- नीचे दिए गए मामलों को छोड़कर, Google Play पर डाउनलोड किए गए ऐप्लिकेशन की किसी अन्य श्रेणी में उत्पाद ऑफ़र करने वाले डेवलपर को पैसे चुकाने के लिए, Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करना चाहिए:
  - सिर्फ़ असल उत्पादों के लिए पैसे चुकाएं
  - ऐसे डिजिटल कॉन्टेंट के लिए पैसे चुकाना जिन्हें ऐप्लिकेशन के बाहर भी इस्तेमाल किया जा सकता है (उदाहरण के लिए, ऐसे गाने जिन्हें किसी दूसरे म्यूज़िक प्लेयर पर चलाया जा सकता है).
- इन-ऐप्लिकेशन वर्चुअल मुद्राओं का इस्तेमाल सिर्फ़ ऐसे ऐप्लिकेशन या गेम के शीर्षक में किया जाना चाहिए जिसके लिए उन्हें खरीदा गया था.
- डेवलपर को अपने बेचे जा रहे किसी ऐप्लिकेशन, इन-ऐप्लिकेशन सेवाओं, सामान, सामग्री या खरीदारी के लिए ऑफ़र किए जा रहे किसी फ़ंक्शन के बारे में ऐप्लिकेशन इस्तेमाल करने वाले लोगों को गुमराह नहीं करना चाहिए. अगर Google Play पर आपके उत्पाद के ब्यौरे में ऐसे इन-ऐप्लिकेशन फ़ीचर के बारे में

बताया गया हो जिनके लिए खास या किसी अन्य शुल्क की ज़रूरत हो सकती है, तो उपयोगकर्ताओं को साफ़ तौर पर बताना चाहिए कि उन फ़ीचर का इस्तेमाल करने के लिए पैसे चुकाना ज़रूरी है.
कुछ ऐप्लिकेशन किसी खरीदारी से बीच-बीच में वर्चुअल आइटम हासिल करने के तरीके (यानी "लूट बॉक्स") मुहैया कराते हैं. ऐसे ऐप्लिकेशन को खरीदारी से पहले ही साफ़ तौर पर बताना होगा कि उन आइटम को हासिल करने की संभावना कितनी है.

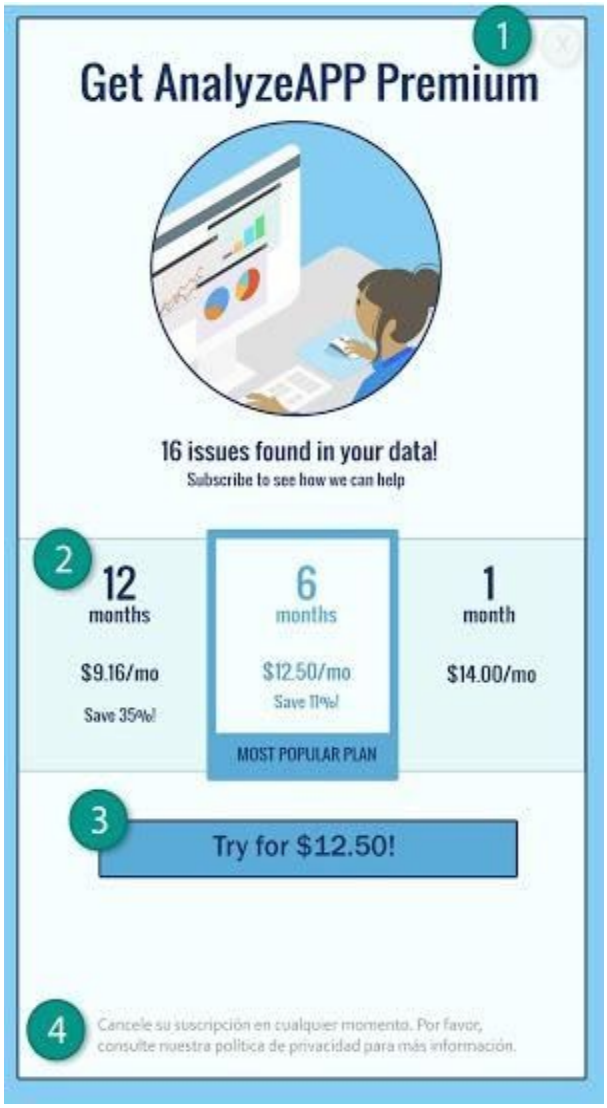
सदस्यताएं

You, as a developer, must not mislead users about any subscription services or content you offer within your app. It is critical to communicate clearly in any in-app promotions or splash screens.

In your app: You must be transparent about your offer. This includes being explicit about your offer terms, the cost of your subscription, the frequency of your billing cycle, and whether a subscription is required to use the app. Users should not have to perform any additional action to review the information.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

Monthly subscriptions that do not inform users they will be automatically renewed and charged every month.
Annual subscriptions that most prominently display their pricing in terms of monthly cost.
Subscription pricing and terms that are incompletely localized.
In-app promotions that do not clearly demonstrate that a user can access content without a subscription (when available).
SKU names that do not accurately convey the nature of the subscription, such as "Free Trial" for a subscription with an auto-recurring charge.



① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.

② Offer only displays pricing in terms of monthly cost and users may not understand that they will be charged a six month price at the time they subscribe.

③ Offer only shows the introductory price and users may not understand what they will automatically be charged at the end of the introductory period.

④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

Free Trials & Introductory Offers

Before a user is enrolled in your subscription: You must clearly and accurately describe the terms of your offer, including the duration, pricing, and description of accessible content or services. Be sure to let your users know how and when a free trial will convert to a paid subscription, how much the paid subscription will cost, and that a user can cancel if they do not want to convert to a paid subscription.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

Offers that do not clearly explain how long the free trial or introductory pricing will last.
Offers that do not clearly explain that the user will be automatically enrolled in a paid subscription at the end of the offer period.
Offers that do not clearly demonstrate that a user can access content without a trial (when available).
Offer pricing and terms that are incompletely localized.

① Dismiss button is not clearly visible and users may not understand that they can access functionality without signing up for the free trial.

② Offer emphasizes the free trial and users may not understand that they will automatically be charged at the end of the trial.

③ Offer does not state a trial period and users may not understand how long their free access to subscription content will last.

④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

Subscription Management & Cancellation

डेवलपर के तौर पर, आपको अपने ऐप्लिकेशन में यह ज़रूर बताना चाहिए कि उपयोगकर्ता अपनी सदस्यता कैसे प्रबंधित या रद्द कर सकता है.

अगर कोई उपयोगकर्ता Google Play पर किसी ऐप्लिकेशन से खरीदी गई सदस्यता रद्द करता है, तो हमारी नीति के मुताबिक उपयोगकर्ता को चालू बिलिंग अवधि के लिए रिफ़ंड नहीं मिलेगा. हालांकि, उन्हें चालू बिलिंग अवधि के बाकी बचे समय में अपनी सदस्यता वाले कॉन्टेंट मिलते रहेंगे चाहे सदस्यता रद्द करने की तारीख जो भी हो. उपयोगकर्ता की ओर से रद्द किए जाने की प्रक्रिया, चालू बिलिंग अवधि के खत्म हो जाने के बाद लागू होती है.

आप (कॉन्टेंट या ऐक्सेस देने वाले के रूप में) अपने उपयोगकर्ताओं के साथ सीधे ऐसी रिफ़ंड नीति लागू कर सकते हैं जो ज़्यादा सुविधाजनक हो. यह आपकी ज़िम्मेदारी है कि आप सदस्यता, उन्हें रद्द कराने की नीतियां, और रिफ़ंड नीतियों में होने वाले किसी भी बदलाव के बारे में उपयोगकर्ताओं को बताएं. साथ ही, यह पक्का करें कि नीतियां, लागू कानून के मुताबिक हों.

हम ऐसे ऐप्लिकेशन की अनुमति नहीं देते हैं जिनमें धोखाधड़ी या परेशान करने वाले विज्ञापन होते हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं. हम आपके ऐप्लिकेशन में पेश किए गए विज्ञापनों को उस ऐप्लिकेशन का हिस्सा मानते हैं. ऐप्लिकेशन में दिखने वाले विज्ञापन हमारी सभी नीतियों के हिसाब से होने चाहिए. जुए के विज्ञापनों से जुड़ी नीतियों के लिए, कृपया यहां क्लिक करें.
हम ऐसे ऐप्लिकेशन की अनुमति नहीं देते हैं जिनमें धोखाधड़ी या परेशान करने वाले विज्ञापन होते हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं. हम आपके ऐप्लिकेशन में पेश किए गए विज्ञापनों को उस ऐप्लिकेशन का हिस्सा मानते हैं. ऐप्लिकेशन में दिखने वाले विज्ञापन हमारी सभी नीतियों के हिसाब से होने चाहिए. जुए के विज्ञापनों से जुड़ी नीतियों के लिए, कृपया यहां क्लिक करें.

विज्ञापनों के लिए जगह की जानकारी के डेटा का इस्तेमाल

ऐसे ऐप्लिकेशन जो अनुमति मांगकर लिए गए डिवाइस की जगह की जानकारी का इस्तेमाल विज्ञापन दिखाने के लिए करते हैं, वे निजी और संवेदनशील जानकारी की नीति के तहत आते हैं. साथ ही, उन्हें नीचे दी गई ज़रूरी शर्तों का भी पालन करना होगा:

> ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को ठीक से पता होना चाहिए कि विज्ञापन दिखाने के लिए, अनुमति मांगकर डिवाइस की जगह की जानकारी का डेटा क्यों लिया जाता है या उसका इस्तेमाल किस तरह किया जाता है. साथ ही, यह जानकारी ऐप्लिकेशन की ज़रूरी निजता नीति में दस्तावेज़ के रूप में दर्ज होनी चाहिए. इसके अलावा, किसी ऐसे काम के विज्ञापन नेटवर्क की निजता नीतियों का उदाहरण दिया जाना चाहिए जिसमें जगह की जानकारी के डेटा के इस्तेमाल के बारे में बताया गया हो.

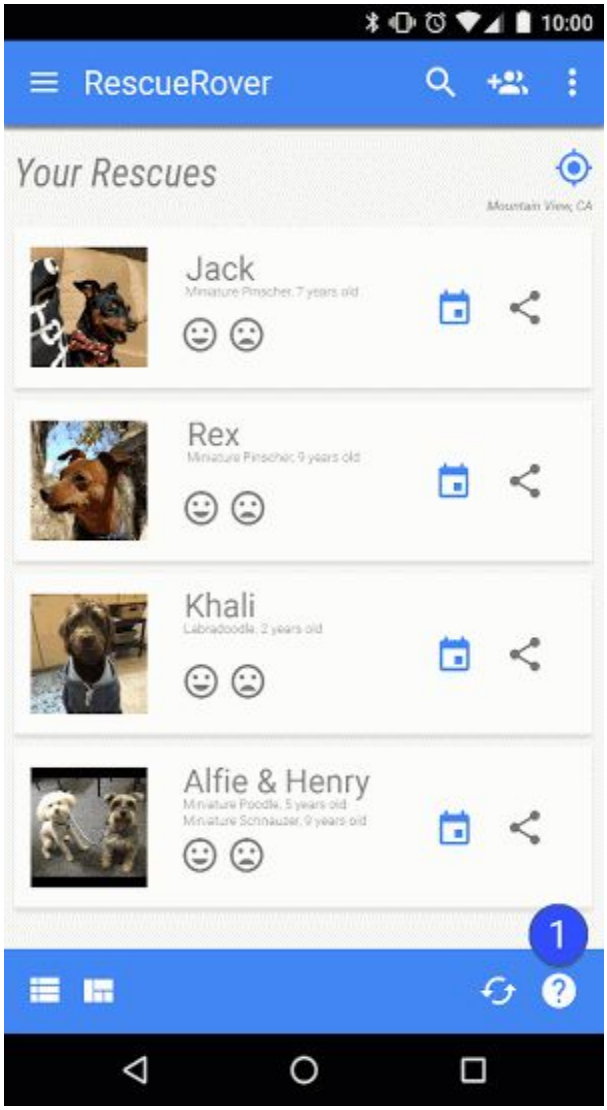
जगह की जानकारी के ऐक्सेस की ज़रूरतों के मुताबिक, जगह की जानकारी की अनुमति ऐप्लिकेशन में मौजूदा सुविधाओं और सेवाओं को लागू करने के लिए मांगी जा सकती है, लेकिन सिर्फ़ विज्ञापनों के लिए नहीं.

धोखाधड़ी करने वाले विज्ञापन

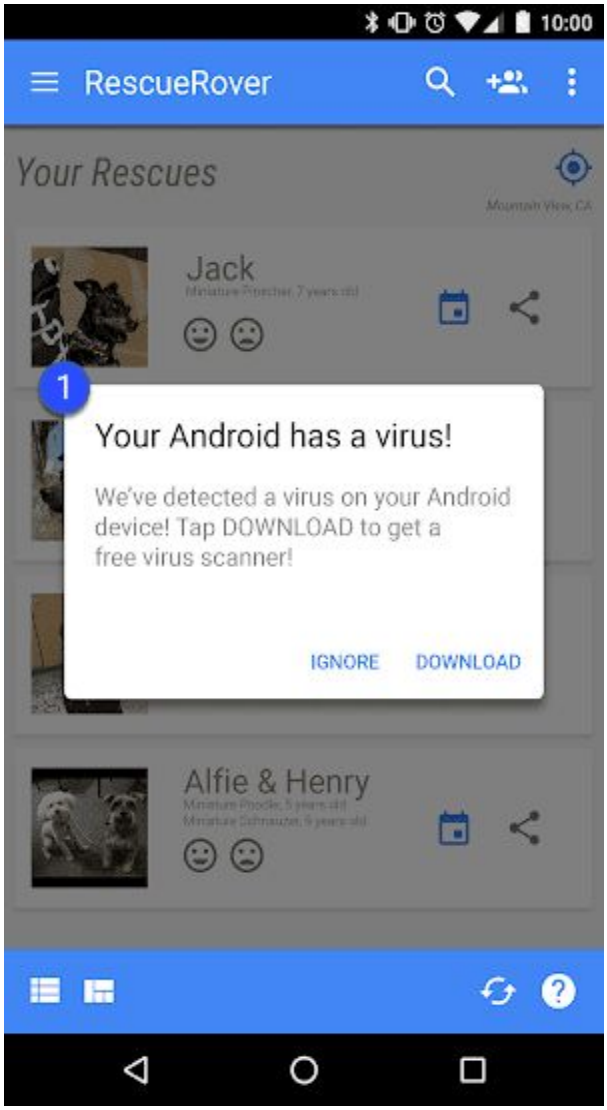
विज्ञापनों को किसी भी ऐप्लिकेशन के यूज़र इंटरफ़ेस या किसी ऑपरेटिंग सिस्टम की सूचनाओं या चेतावनी देने के तरीकों की नकल या उन्हें किसी दूसरी पहचान के साथ इस्तेमाल नहीं करना चाहिए. ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को यह साफ़ तौर पर बताया जाना चाहिए कि हर एक विज्ञापन, कौनसा ऐप्लिकेशन उपलब्ध करा रहा है.

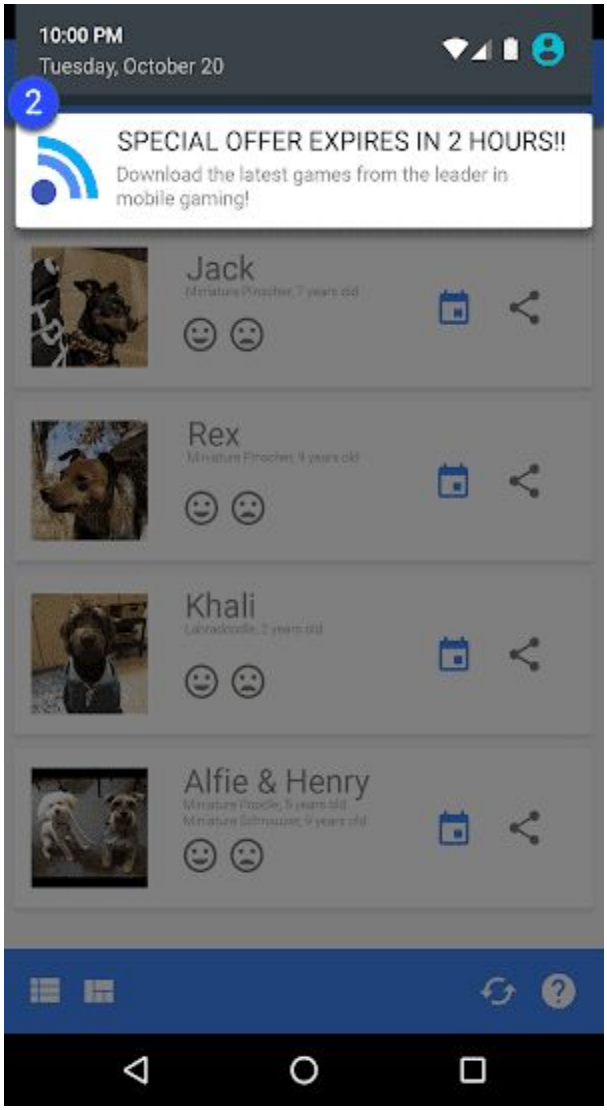
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे विज्ञापन जो किसी ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) की नकल करते हैं:



① इस ऐप्लिकेशन में दिया गया प्रश्नवाचक चिह्न का आइकॉन एक ऐसा विज्ञापन है जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को किसी बाहरी लैंडिंग पेज पर ले जाता है.
ऐसे विज्ञापन जो सिस्टम सूचना की नकल करते हैं:





① ② ऊपर दिए गए उदाहरण, अलग-अलग सिस्टम सूचनाओं की नकल करने वाले विज्ञापनों के बारे में बताते हैं.

लॉकस्क्रीन पर कमाई कराने की सुविधा

जब तक कि ऐप्लिकेशन किसी खास उद्देश्य के लिए लॉकस्क्रीन का इस्तेमाल ना करे, तब तक ऐप्लिकेशन पर ऐसे विज्ञापन या सुविधाएं नहीं दिखाए जाते जो डिवाइस की लॉकस्क्रीन पर कमाई करें.

परेशान करने वाले विज्ञापन

विज्ञापन इस तरह नहीं दिखाने चाहिए जिसकी वजह से अनजाने में क्लिक हो जाएं. किसी व्यक्ति को ऐप्लिकेशन का पूरी तरह से इस्तेमाल करने से पहले, उसे विज्ञापन पर क्लिक करना या विज्ञापन देने के लिए निजी जानकारी सबमिट करने के लिए मजबूर करना पूरी तरह से मना है.

'पेज पर अचानक दिखने वाले विज्ञापन', सिर्फ़ उस ऐप्लिकेशन में दिखाए जा सकते हैं जिसमें उन्हें उपलब्ध कराया गया है. अगर आपका ऐप्लिकेशन 'पेज पर अचानक दिखने वाले विज्ञापन' या ऐसे अन्य विज्ञापन दिखाता है जो

आम तौर पर ऐप्लिकेशन इस्तेमाल करने में रुकावट डालते हैं, तो उन्हें ऐसा होना चाहिए कि पेनल्टी के बिना आसानी से खारिज किए जा सकें.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे विज्ञापन जो पूरी स्क्रीन पर दिखते हैं या ऐप्लिकेशन इस्तेमाल करने में रुकावट डालते हैं और विज्ञापन हटाने का तरीका सही से नहीं बताते हैं:

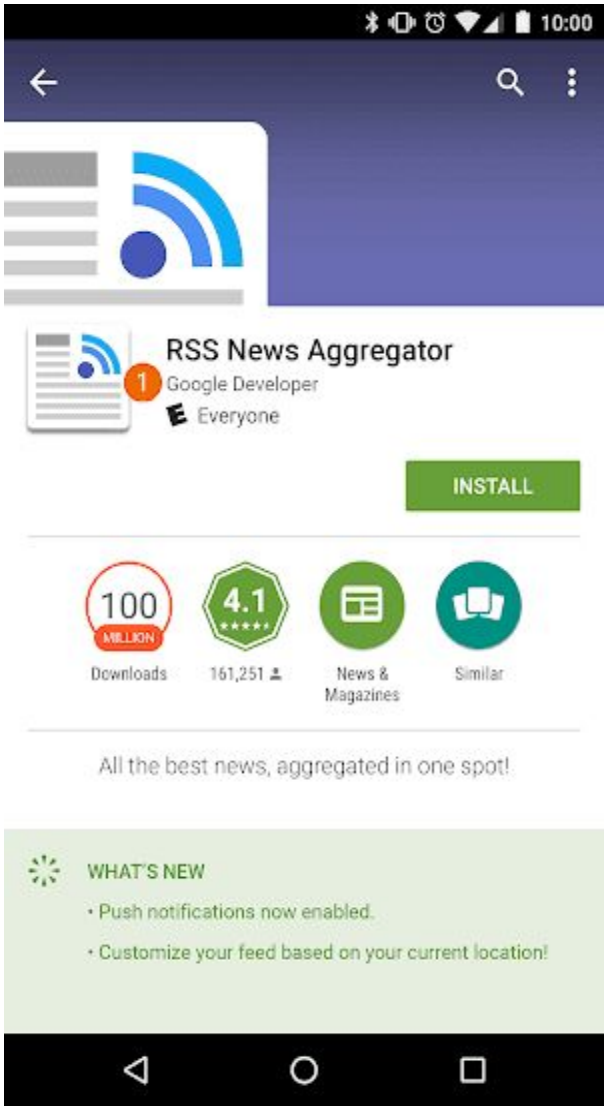
① इस विज्ञापन में हटाने का कोई बटन नहीं है.

ऐप्लिकेशन, तीसरे पक्ष के विज्ञापन या डिवाइस के काम करने के तरीके में रुकावट डालना

आपके ऐप्लिकेशन के विज्ञापनों को अन्य ऐप्लिकेशन, विज्ञापनों या डिवाइस के काम में रुकावट नहीं डालनी चाहिए. इनमें सिस्टम या डिवाइस बटन और पोर्ट भी शामिल हैं. इसमें ओवरले, सहयोगी कार्यक्षमता, और विजेट के रूप में बनाई गई विज्ञापन इकाइयां शामिल हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं.

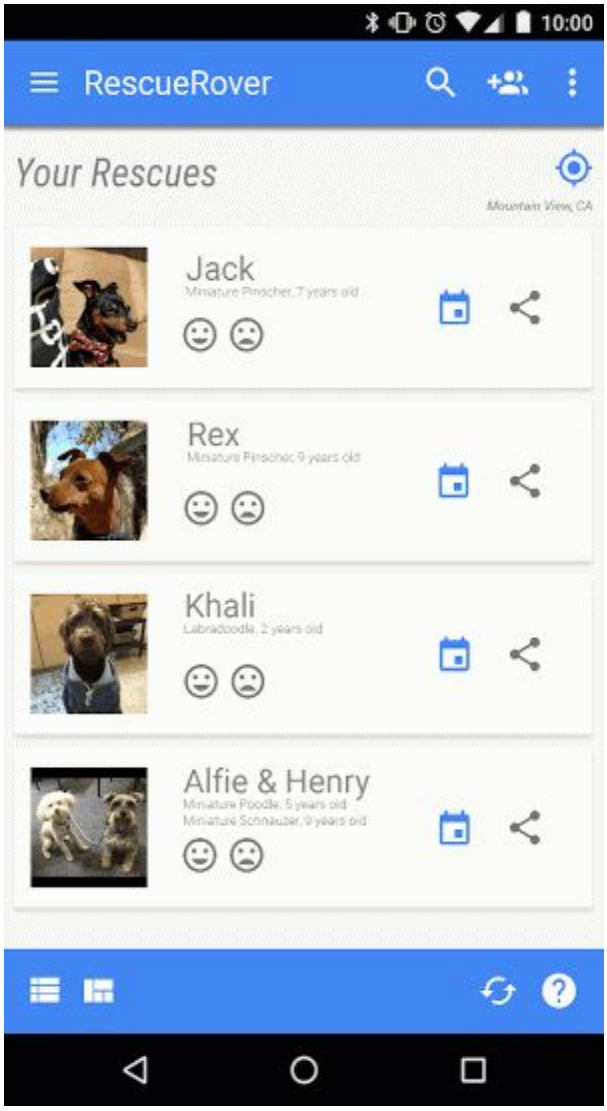
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे विज्ञापन जो उन्हें उपलब्ध कराने वाले ऐप्लिकेशन के बाहर दिखते हैं:



ब्यौरा: जब उपयोगकर्ता इस ऐप्लिकेशन से होम स्क्रीन पर जाता है, तो उसे होमस्क्रीन पर अचानक एक विज्ञापन दिखने लगता है.

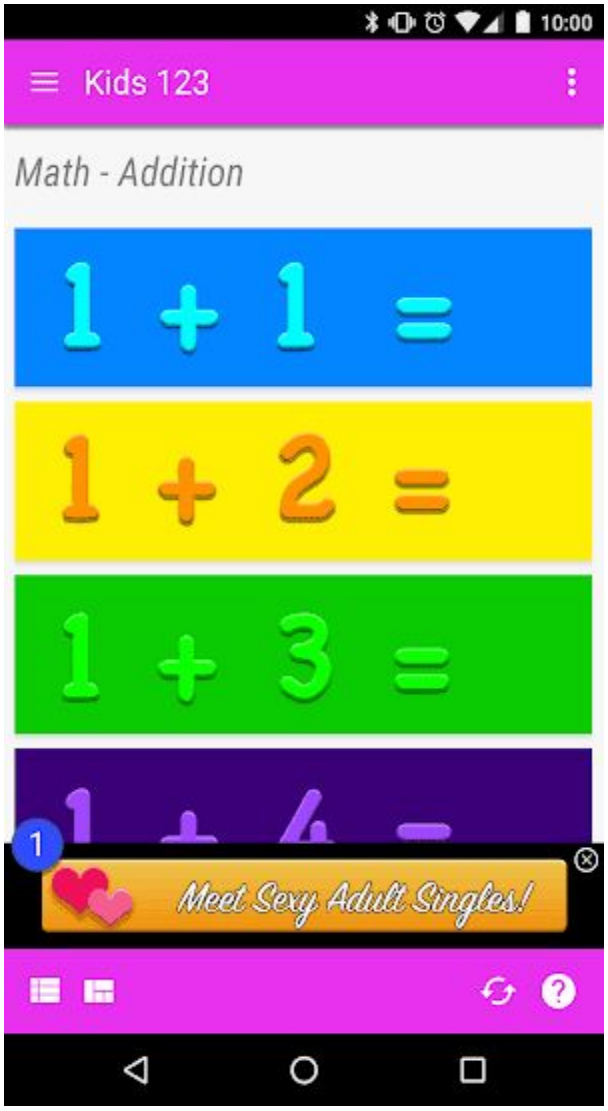
ऐसे विज्ञापन जो होम बटन या ऐसी दूसरी सुविधाओं से ट्रिगर होते हैं, वे साफ़ तौर पर ऐप्लिकेशन से बाहर निकलने के लिए बनाए गए हैं:



ब्यौरा: उपयोगकर्ता ऐप्लिकेशन से बाहर निकलने और होम स्क्रीन पर जाने की कोशिश करता है, लेकिन इसके बजाय, किसी विज्ञापन की वजह से ऐसा करने में रुकावट आ जाती है.

आपत्तिजनक विज्ञापन

आपके ऐप्लिकेशन में दिखाए गए विज्ञापन, उन लोगों के हिसाब से सही होने चाहिए जिनके लिए यह ऐप्लिकेशन बनाया गया है. भले ही सामग्री हमारी नीतियों का अन्यथा अनुपालन करती हो.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.



① यह विज्ञापन उन लोगों के लिए सही नहीं है जिनके लिए ऐप्लिकेशन बनाया गया है.

Android विज्ञापन आईडी का इस्तेमाल

'Google Play सेवाएं' के वर्शन 4.0 में विज्ञापन और आंकड़े देने वालों के इस्तेमाल के लिए, नए एपीआई और एक आईडी बनाया गया है. इस आईडी के इस्तेमाल की शर्तें नीचे दी गई हैं.

> इस्तेमाल. Android के विज्ञापन पहचानकर्ता का इस्तेमाल सिर्फ़ विज्ञापन और उपयोगकर्ता के आंकड़े के लिए ही किया जाना चाहिए. "रुचि के हिसाब से विज्ञापन से ऑप्ट-आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन से ऑप्ट-आउट करने" की सेटिंग की स्थिति की पुष्टि, हर बार आईडी ऐक्सेस करने पर जानी चाहिए.
> निजी तौर पर पहचान योग्य जानकारी या दूसरे पहचानकर्ता से जुड़ना. विज्ञापन पहचानकर्ता को ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति के बिना, निजी तौर पर पहचानने लायक जानकारी से दूर रहना चाहिए या किसी भी डिवाइस पहचानकर्ता (उदाहरण के लिए: SSAID, MAC का पता, IMEI, इन जैसों) से संपर्क में नहीं होना चाहिए.

उपयोगकर्ताओं ने जो चुना है उसके मुताबिक. अगर रीसेट किया जाता है, तो नए विज्ञापन पहचानकर्ता को उपयोगकर्ता की सहमति के बिना किसी पिछले विज्ञापन पहचानकर्ता से संपर्क या किसी पिछले विज्ञापन पहचानकर्ता से मिले हुए डेटा का इस्तेमाल नहीं करना चाहिए. साथ ही, आपको उपयोगकर्ता की "रुचि के हिसाब से विज्ञापन से ऑप्ट आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन से ऑप्ट आउट करने" की सेटिंग के हिसाब से काम करना चाहिए. अगर किसी उपयोगकर्ता ने इस सेटिंग को चालू किया हुआ है, तो आप विज्ञापन उद्देश्यों के लिए उपयोगकर्ता प्रोफ़ाइल बनाने या पसंद को ध्यान में रखते हुए विज्ञापन बनाकर उपयोगकर्ताओं को टार्गेट करने के लिए विज्ञापन पहचानकर्ता का इस्तेमाल नहीं कर सकते. जिन गतिविधियों की अनुमति दी गई है उनमें सामग्री के हिसाब से विज्ञापन, फ़्रीक्वेंसी कैपिंग, कन्वर्ज़न ट्रैकिंग, रिपोर्टिंग और सुरक्षा, और धोखाधड़ी की पहचान करना शामिल है.
उपयोगकर्ताओं के लिए पारदर्शिता. विज्ञापन पहचानकर्ता का संग्रह, इस्तेमाल, और इन शर्तों को पूरा करने के वादे को उपयोगकर्ता के सामने कानूनी रूप से उचित गोपनीयता अधिसूचना के रूप में ज़ाहिर की जानी चाहिए. निजता मानकों के बारे में ज़्यादा जानकारी के लिए, कृपया हमारे उपयोगकर्ता का डेटा नीति देखें.
इस्तेमाल की शर्तों को मानना. विज्ञापन पहचानकर्ता का इस्तेमाल सिर्फ़ इन शर्तों के मुताबिक ही किया जा सकता है. इसमें वह पक्ष भी शामिल है जिसके साथ आप इसे कारोबार के दौरान शेयर कर सकते हैं. Google Play पर अपलोड या प्रकाशित किए गए सभी ऐप्लिकेशन को किसी भी विज्ञापन मकसदों के लिए, किसी दूसरे डिवाइस पहचानकर्ता के बदले विज्ञापन आईडी (डिवाइस पर उपलब्ध होने पर) का इस्तेमाल करना पड़ेगा.

अगर आप अपने ऐप्लिकेशन में विज्ञापन दिखाते हैं और आपके ऐप्लिकेशन के टारगेट किए जाने वाले दर्शकों में सिर्फ़ बच्चे शामिल हैं, जैसा कि परिवार नीति में बताया गया है, तो आपके लिए Google Play की नीतियों के हिसाब से खुद प्रमाणित किया हुआ विज्ञापन SDK टूल इस्तेमाल करना ज़रूरी है. साथ ही, इसे विज्ञापन SDK टूल प्रमाणित करने की नीचे दी गई ज़रूरी शर्तों के मुताबिक होना चाहिए. अगर आपके ऐप्लिकेशन का टारगेट बच्चे और बड़े दोनों हैं, तो आपको उम्र तय करने के तरीके लागू करने होंगे. साथ ही, यह पक्का करना होगा कि बच्चों को दिखाए जाने वाले विज्ञापन, खुद प्रमाणित किए हुए इन विज्ञापन SDK टूल में से किसी एक से ही आएं. 'परिवार के लिए बनाए गए' कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़ खुद प्रमाणित किए हुए विज्ञापन SDK टूल का इस्तेमाल करें.

Google Play के प्रमाणित विज्ञापन SDK टूल की ज़रूरत सिर्फ़ तब होती है, जब आप अपने विज्ञापन SDK टूल का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए करते हैं. यहां बताई गई परिस्थितियों में Google Play पर, विज्ञापन SDK टूल की ओर से खुद प्रमाणित करने की ज़रूरत नहीं होती. हालांकि, इस बात को पक्का करने की ज़िम्मेदारी अब भी आपकी है कि विज्ञापन सामग्री और डेटा इकट्ठा करने के तरीके Play की उपयोगकर्ता डेटा नीति और परिवार नीति का पालन करते हों:

खुद बनाए गए विज्ञापन दिखाना. इसमें आप SDK टूल का इस्तेमाल करके, अपने ऐप्लिकेशन या दूसरी मालिकाना हक वाली मीडिया और प्रचार के लिए बेची जाने वाली चीज़ों के, दूसरी जगहों पर किए जा रहे प्रचार को प्रबंधित करते हैं
विज्ञापन देने वालों के साथ प्रत्यक्ष डील करना, जिसमें आप इन्वेंट्री प्रबंधन के लिए, SDK टूल का इस्तेमाल करते हैं

विज्ञापन SDK टूल प्रमाणित करने के लिए ज़रूरी शर्तें

आपत्तिजनक विज्ञापन सामग्री और व्यवहार की परिभाषा तय करें और विज्ञापन SDK टूल की शर्तों और नीतियों के तहत उन पर पाबंदी लगाएं. इन परिभाषाओं की वजह से, Google Play की डेवलपर कार्यक्रम नीतियों का उल्लंघन नहीं होना चाहिए.

अपने विज्ञापन क्रिएटिव को रेट करने का तरीका बनाएं. ये तरीका उम्र के हिसाब से बने समूहों के अनुसार हो. साथ ही, इसमें कम से कम 'सभी' और 'वयस्क' समूह शामिल हों. रेटिंग का तरीका उसी तरीके के हिसाब से होना चाहिए जो Google, SDK टूल को तब देता है, जब वे अपनी रुचि बताने के लिए नीचे दिया गया फ़ॉर्म भरते हैं.

हर अनुरोध या हर ऐप्लिकेशन के आधार पर प्रकाशकों को विज्ञापन देने के लिए, बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव का अनुरोध करने दें. इस तरह के बर्ताव को नियम और कानूनों जैसे कि, यूएस चिल्ड्रन ऑनलाइन प्राइवेसी एंड प्रोटेक्शन एक्ट (कोपा) और यूरोपीय संघसामान्य डेटा से जुड़े सुरक्षा कानून (जनरल डेटा प्रोटेक्शन रेगुलेशन) (जीडीपीआर) के मुताबिक होना चाहिए. बच्चों को ध्यान में रखते हुए, Google Play में दर्शकों की पसंद को ध्यान में रखकर बनाए गए विज्ञापन, रुचि के हिसाब से बनाए गए विज्ञापन, और रीमार्केटिंग को बंद करना ज़रूरी है.

पक्का करें कि जब रीयल-टाइम बोली-प्रक्रिया का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए किया जाता है, तो क्रिएटिव की समीक्षा की जाती है और निजता बनाए रखने के संकेत, बोली लगाने वालों को दिए जाते हैं.

Google को इस बात की पुष्टि करने के लिए ज़रूरी जानकारी दें कि विज्ञापन SDK टूल, प्रमाणित होने के लिए सभी ज़रूरी शर्तों को पूरा करता है. साथ ही, बाद में मांगी जाने वाली किसी भी जानकारी के लिए समय पर जवाब दें.

ध्यान दें: विज्ञापन SDK टूल में ऐसे विज्ञापन देने की सुविधा होनी चाहिए, जो बच्चों से जुड़े सभी ज़रूरी कानूनों और नियमों का पालन करती है. साथ ही, ये नियम और कानून उनके प्रकाशकों पर लागू हो सकते हों.

बच्चों के लिए विज्ञापन दिखाते समय, इसकी सुविधा देने वाले प्लैटफ़ॉर्म के लिए मीडिएशन की शर्तें:

यह पक्का करने के लिए कि मीडिएशन से दिखाए जाने वाले सभी विज्ञापन इन शर्तों को पूरा करते हों, सिर्फ़ Google Play से प्रमाणित विज्ञापन SDK टूल का इस्तेमाल करें या सुरक्षा के ज़रूरी उपाय लागू करें. साथ ही

विज्ञापन सामग्री की रेटिंग और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव को दिखाने के लिए ज़रूरी संकेत भेजें.

डेवलपर यहां खुद को प्रमाणित करने वाले विज्ञापन SDK टूल की सूची देख सकते हैं.

इसके साथ ही, डेवलपर रुचि बताने वाला फ़ॉर्म भी उन विज्ञापन SDK टूल के साथ शेयर कर सकते हैं जो खुद प्रमाणित होना चाहते हैं.

स्टोर पेज और प्रचार

आपका ऐप्लिकेशन किसको दिखेगा और उसका प्रचार किस तरह हुआ है, इन बातों का स्टोर की क्वालिटी पर काफ़ी असर पड़ता है. स्पैम वाले स्टोर पेज, कम क्वालिटी वाला प्रचार, और Google Play पर आर्टिफ़िशियल तरीके से लोगों तक ऐप्लिकेशन पहुंचाने (दिखाने) की कोशिशों से बचें.

ऐप्लिकेशन का प्रचार

हम ऐसे किसी ऐप्लिकेशन की अनुमति नहीं देते हैं जो सीधे तौर पर या किसी और तरीके से उपयोगकर्ताओं या डेवलपर के साथ धोखाधड़ी करते हैं या उन्हें नुकसान पहुंचाते हैं. इसके अलावा, फ़ायदा उठाने के लिए गलत तरीकों से भी प्रचार करने की अनुमति नहीं है. इसमें ऐसे ऐप्लिकेशन शामिल हैं जो इन तरीकों को अपनाते हैं:

- वेबसाइट, ऐप्लिकेशन या अन्य प्रॉपर्टी पर धोखाधड़ी करने वाले विज्ञापनों का इस्तेमाल करना. इनमें ऐसी सूचनाएं भी शामिल हैं जो सिस्टम की सूचना और चेतावनी जैसी ही होती हैं.
- प्रचार या इंस्टॉल कराने के ऐसे तरीके जो उपयोगकर्ताओं को Google Play पर ले जाते हैं या उपयोगकर्ताओं को कार्रवाई की सूचना दिए बिना ही ऐप्लिकेशन डाउनलोड कर देते हैं.
- मैसेज (एसएमएस) सेवाओं के ज़रिए अनचाहा प्रचार करना.

यह पक्का करना आपकी ज़िम्मेदारी है कि कोई भी विज्ञापन नेटवर्क कंपनी या आपके ऐप्लिकेशन के सहयोगी, इन नीतियों का पालन करते हैं. साथ ही, प्रचार करने के किसी भी प्रतिबंधित तरीके का इस्तेमाल नहीं करते हैं.

हम उन ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह करने वाला, गलत तरीके से फ़ॉर्मैट किया गया, बिना किसी ब्यौरे वाला, गैर-ज़रूरी, हद से ज़्यादा या गलत मेटाडेटा शामिल होता है. इनमें ऐप्लिकेशन की जानकारी, डेवलपर का नाम, शीर्षक, आइकॉन, स्क्रीनशॉट, और प्रमोशन की इमेज भी शामिल होती हैं. हालांकि, यह इन तक ही सीमित नहीं है. डेवलपर को साफ़ तौर पर और सही तरीके से लिखी जानकारी देनी चाहिए. हम ऐप्लिकेशन की जानकारी में बिना एट्रिब्यूशन वाले या बिना पहचान वाले किसी व्यक्ति के टेस्टीमोनियल को शामिल करने की मंज़ूरी नहीं देते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

① बिना एट्रिब्यूशन वाले या बिना पहचान वाले उपयोगकर्ता टेस्टीमोनियल

② ऐप्लिकेशन या ब्रैंड के डेटा की तुलना

③ वर्ड ब्लॉक और वर्टिकल (ऊपर-नीचे)/हॉरिज़ॉन्टल (दाएं-बाएं) वर्ड लिस्ट

यहां आपके स्टोर पेज में मौजूद गलत टेक्स्ट, इमेज या वीडियो के कुछ उदाहरण दिए गए हैं:

ऐसी तस्वीरें या वीडियो जिनमें यौन भावना को भड़काने वाला अश्लील कॉन्टेंट शामिल हो. ऐसी अश्लील तस्वीरों के संग्रह से बचें जिनमें स्तन, कूल्हे, जननांग या इसी तरह का आकर्षित करने वाला कोई दूसरा अंग शामिल हो. साथ ही, इस तरह के मिलते-जुलते कॉन्टेंट से भी बचें. फिर भले ही, उसे चित्र या असल रूप में दिखाया गया हो.

आम दर्शक के लिए गलत भाषा. अपनी ऐप्लिकेशन के स्टोर पेज में अपमानजनक और अश्लील भाषा से बचें. अगर वह आपके ऐप्लिकेशन का खास हिस्सा है, तो आपको स्टोर पेज में उसे सेंसर कर देना चाहिए. खास तौर पर, ऐप्लिकेशन आइकॉन, प्रचार से जुड़े चित्रों या वीडियो में दिखाए गए दिल दहलाने वाले वीडियो ग्राफ़िक कॉन्टेंट.

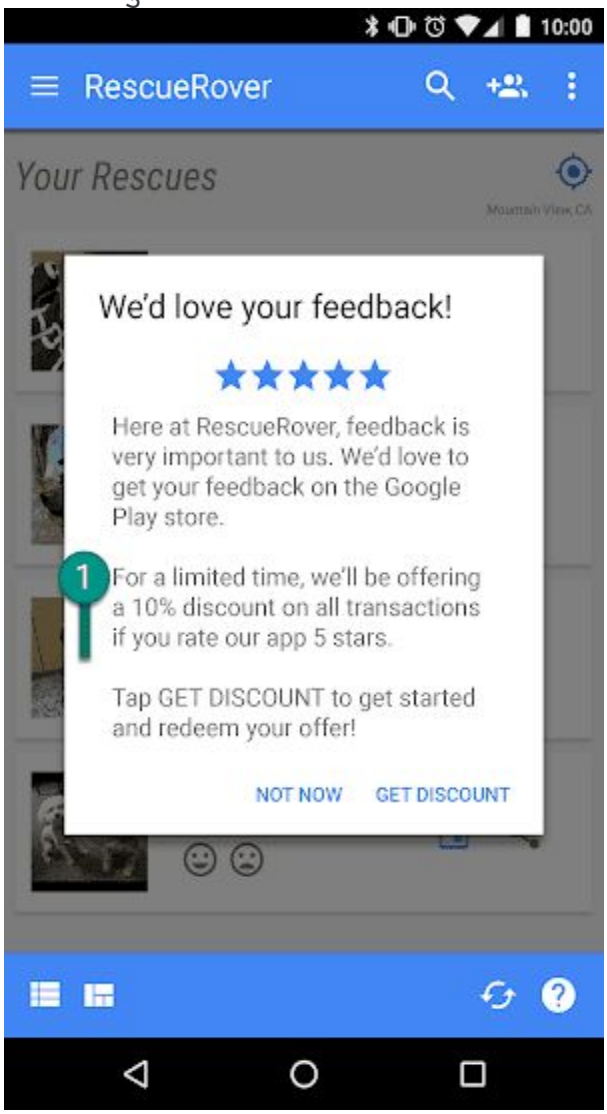
दवाओं के गैरकानूनी इस्तेमाल को दिखाना. यहां तक कि EDSA (शिक्षा, डॉक्यूमेंट्री, विज्ञान या कला) कॉन्टेंट को भी सभी दर्शकों की सुविधा के हिसाब से स्टोर पेज में शामिल किया जाना चाहिए.

यहां कुछ सबसे सही तरीके दिए गए हैं:

- अपने ऐप्लिकेशन की सबसे अच्छी बातों को हाइलाइट करें. दिलचस्प और मज़ेदार जानकारी शेयर करें, ताकि लोगों को यह पता चल सके कि आपके ऐप्लिकेशन में क्या खास है.
- पक्का करें कि आपके ऐप्लिकेशन का शीर्षक और विवरण, ऐप्लिकेशन के फ़ंक्शन के बारे में सही जानकारी देता हो.
- दोहराए जाने वाले या बेवजह के कीवर्ड या संदर्भों का इस्तेमाल करने से बचें.
- अपने ऐप्लिकेशन की जानकारी कम और आसान शब्दों में दें. कम शब्दों में जानकारी का मकसद, खास तौर पर छोटे डिसप्ले वाले डिवाइस पर बेहतरीन उपयोगकर्ता अनुभव देना है. हद से ज़्यादा लंबे, विवरण, गलत फ़ॉर्मैट या दोहराई जाने वाली जानकारी से, इस नीति का उल्लंघन हो सकता है.
- ध्यान रखें कि आपका स्टोर पेज, आम दर्शक के हिसाब से होना चाहिए. अपने स्टोर पेज में गलत टेक्स्ट, इमेज या वीडियो के इस्तेमाल से बचें. साथ ही, ऊपर बताए गए दिशा-निर्देशों का पालन करें.

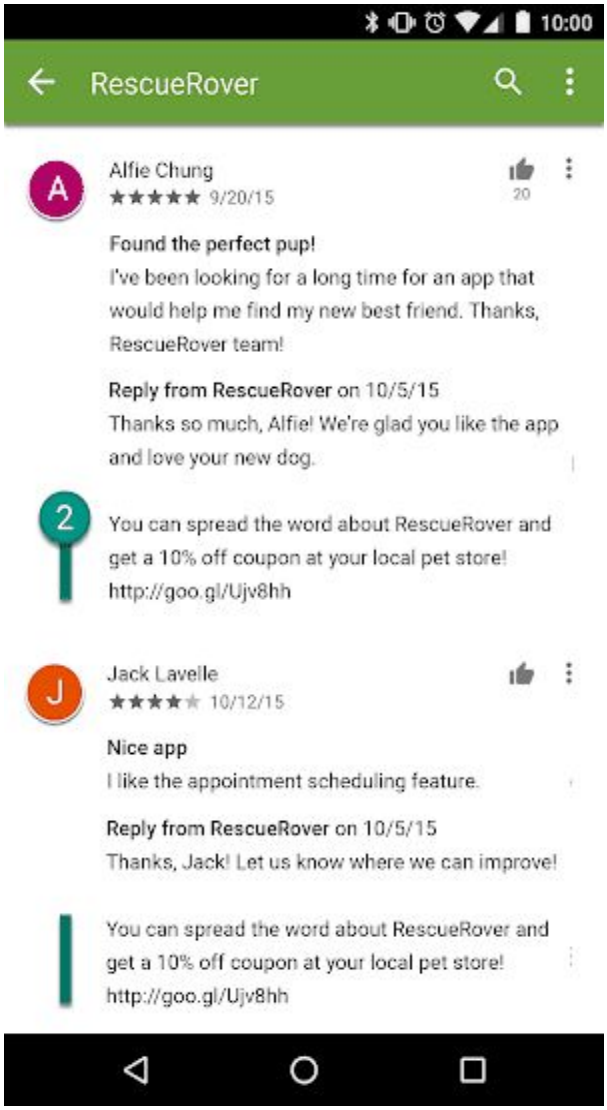
डेवलपर को Google Play में किसी भी ऐप्लिकेशन के प्लेसमेंट में हेरफेर करने की कोशिश नहीं करनी चाहिए. इसमें धोखाधड़ी या कोई फ़ायदा देकर कराए गए इंस्टॉल, समीक्षाएं और रेटिंग जैसे अवैध तरीकों से, उत्पाद रेटिंग, समीक्षाएं या इंस्टॉलेशन की संख्याओं को बढ़ाना शामिल है, लेकिन यह इन ही चीज़ों तक सीमित नहीं है.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

फ़ायदा देते हुए, उपयोगकर्ताओं से अपने ऐप्लिकेशन को रेट करने के लिए कहना:



① ① यह सूचना उपयोगकर्ताओं को ज़्यादा रेटिंग के बदले में छूट ऑफ़र करती है.

Google Play पर ऐप्लिकेशन के प्लेसमेंट को प्रभावित करने के लिए बार-बार रेटिंग सबमिट करना. आपत्तिजनक कॉन्टेंट वाली समीक्षाएं सबमिट करना या इस्तेमाल करने वाले को ऐसी समीक्षाएं सबमिट करने के लिए बढ़ावा देना, जिनमें सहयोगी, कूपन, गेम के कोड, ईमेल पते या वेबसाइट और अन्य ऐप्लिकेशन के लिंक शामिल होते हैं:



② यह समीक्षा इस्तेमाल करने वालों को एक कूपन का ऑफ़र देकर RescueRover ऐप्लिकेशन का प्रचार करने के लिए बढ़ावा देती है.

रेटिंग और समीक्षाएं ऐप्लिकेशन की गुणवत्ता के मानदंड हैं. इस्तेमाल करने वाले ऐसे ऐप्लिकेशन की पुष्टि करने और इसके ज़रूरी होने के लिए रेटिंग और समीक्षाओं पर निर्भर करते हैं. यहां इस्तेमाल करने वालों की समीक्षाओं के जवाब देने के लिए सबसे सही तरीके दिए गए हैं:

अपने जवाब में उपयोगकर्ता की टिप्पणियों में उठाई गईं समस्याओं को हल करने पर ध्यान दें, न कि ज़्यादा रेटिंग की मांग करें.
सहायता पता या अक्सर पूछे जाने वाले सवालों के पेज जैसे उपयोगी संसाधनों को शामिल करें.

हमारे कॉन्टेंट रेटिंग सिस्टम में इंटरनैशनल एज रेटिंग कोएलिशन (आईएआरसी) की आधिकारिक रेटिंग शामिल होती हैं. इसे डेवलपर की मदद करने के लिए इस तरह से डिज़ाइन किया गया है कि वह लोगों तक स्थानीय रूप से ज़रूरी कॉन्टेंट रेटिंग मुहैया करा सके.

कॉन्टेंट रेटिंग का इस्तेमाल कैसे किया जाता है

कॉन्टेंट रेटिंग का इस्तेमाल उपभोक्ताओं, खासकर अभिभावकों को ऐप्लिकेशन में संभावित रूप से मौजूद आपत्तिजनक कॉन्टेंट की जानकारी देने के लिए किया जाता है. ये कुछ जगहों पर आपके कॉन्टेंट को फ़िल्टर करने या कुछ लोगों तक इस तरह के कॉन्टेंट की पंहुच को रोकने में मदद करते हैं, जहां भी कानूनी तौर पर ऐसा करना ज़रूरी होता है. साथ ही, यह इस बात का पता लगाने में भी मदद करते हैं कि आपका ऐप्लिकेशन खास डेवलपर प्रोग्राम की ज़रूरी शर्तों को पूरा करता है या नहीं.

कॉन्टेंट रेटिंग किस तरह दी जाती हैं

कॉन्टेंट रेटिंग पाने के लिए, आपको 'Play कंसोल' में रेटिंग से जुड़े सवालों की सूची भरनी होगी, जिसमें यह पूछा जाता है कि आपके ऐप्लिकेशन का कॉन्टेंट कैसा है. सवालों की सूची में दिए गए आपके जवाबों के मुताबिक, आपके ऐप्लिकेशन को अलग-अलग रेटिंग प्राधिकरणों की तरफ़ से कॉन्टेंट रेटिंग दी जाएगी. आपके ऐप्लिकेशन की सामग्री को गलत ढंग से प्रस्तुत किए जाने से, निकालने की प्रक्रिया या निलंबन हो सकता है इसलिए कॉन्टेंट रेटिंग प्रश्नावली में सही-सही जवाब देना महत्वपूर्ण है.

अपने ऐप्लिकेशन को “बगैर रेटिंग वाला” सूची में शामिल होने से रोकने के लिए, आपको 'Play कंसोल' में सबमिट किए गए हर नए ऐप्लिकेशन की कॉन्टेंट रेटिंग से जुड़े सवालों की सूची पूरी करना ज़रूरी है. साथ ही, ऐसा करना Google Play में काम कर रहे मौजूदा सभी ऐप्लिकेशन के लिए भी ज़रूरी है. बिना कॉन्टेंट रेटिंग वाले ऐप्लिकेशन 'Play स्टोर' से हटा दिए जाएंगे.

अगर आप अपने ऐप्लिकेशन के कॉन्टेंट या सुविधाओं में ऐसे बदलाव करते हैं जिनसे रेटिंग के सवालों की सूची में दिए गए जवाबों पर असर पड़ता है, तो आपको 'Play कंसोल' में कॉन्टेंट रेटिंग से जुड़े सवालों की नई सूची सबमिट करनी होगी.

अलग-अलग रेटिंग प्राधिकरणों के बारे में ज़्यादा जानने और कॉन्टेंट रेटिंग से जुड़े सवालों की सूची को पूरा करने का तरीका जानने के लिए सहायता केंद्र पर जाएं.

रेटिंग से जुड़ी अपील

अगर आप अपने ऐप्लिकेशन को मिली रेटिंग से सहमत नहीं हैं, तो अपने प्रमाणपत्र ईमेल में दिए गए लिंक का इस्तेमाल करके, आप सीधे आईएआरसी रेटिंग प्राधिकरण में अपील कर सकते हैं.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों को या Google Play को स्पैम भेजते हैं, जैसे कि वे ऐप्लिकेशन जो लोगों को अनचाहे मैसेज भेजते हैं या ऐसे ऐप्लिकेशन जो बार-बार एक ही चीज़ दिखाते हैं या जिनकी क्वालिटी कम अच्छी होती है.

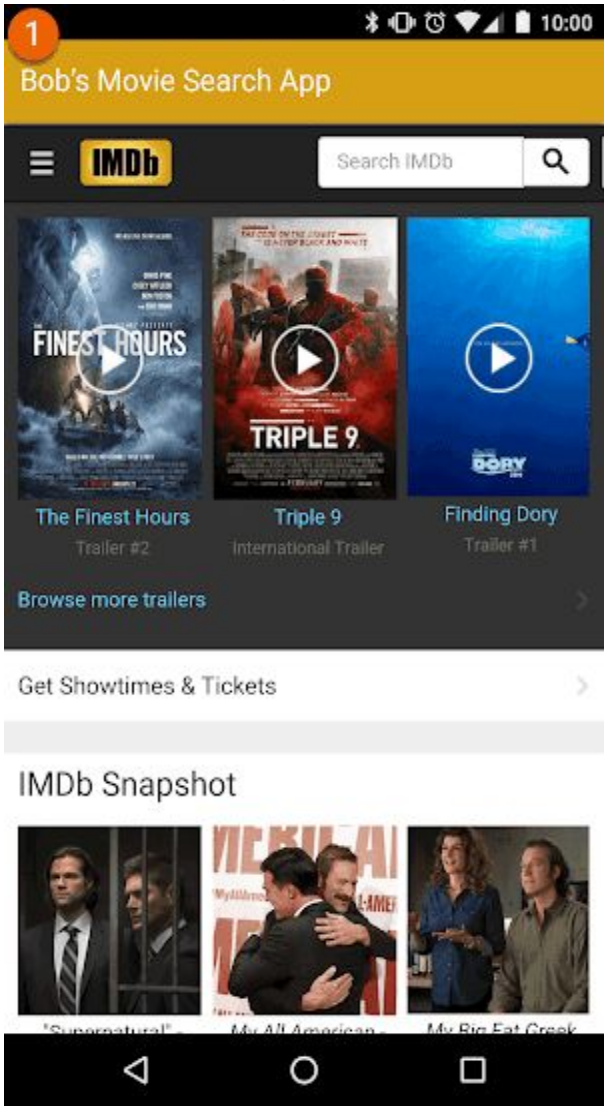
मैसेज स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो उपयोगकर्ता को कॉन्टेंट और चुने हुए लोगों की पुष्टि करने की सुविधा दिए बिना, उपयोगकर्ता की तरफ़ से SMS, ईमेल या अन्य मैसेज भेजते हैं.

वेबव्यू और उससे जुड़े स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जिनका मुख्य उद्देश्य अफ़िलिएट ट्रैफ़िक को किसी वेबसाइट पर भेजना या किसी वेबसाइट का वेबव्यू उस वेबसाइट के मालिक या एडमिन के अनुमति के बिना दिखाना हो.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसा ऐप्लिकेशन जिसका मुख्य उद्देश्य रेफ़रल ट्रैफ़िक को किसी वेबसाइट पर भेजना होता है जिससे उस वेबसाइट पर उपयोगकर्ता के साइन-अप या खरीदारी करने से क्रेडिट पा सके.
ऐसे ऐप्लिकेशन जिनका मुख्य उद्देश्य अनुमति के बिना, किसी वेबसाइट का वेबव्यू दिखाना होता है:



① यह ऐप्लिकेशन "बॉब का मूवी खोजने वाला ऐप्लिकेशन" कहलाता है और यह IMDb का वेबव्यू दिखाता है.

बार-बार एक ही तरह के कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो Google Play पर पहले से मौजूद दूसरे ऐप्लिकेशन के जैसा ही अनुभव देते हों. ऐप्लिकेशन ऐसे होने चाहिए जो सबसे अलग कॉन्टेंट या सेवाएं देकर लोगों के लिए फ़ायदेमंद साबित हों.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

कोई मूल कॉन्टेंट या उसमें कुछ नया जोड़े बिना दूसरे ऐप्लिकेशन से कॉन्टेंट कॉपी करना.

इसके अलावा, ऐसे कई सारे ऐप्लिकेशन बनाना जिनका काम करने का तरीका, कॉन्टेंट, और ऐप्लिकेशन को इस्तेमाल करने का अनुभव बहुत ही मिलता-जुलता हो. अगर इनमें से हर ऐप्लिकेशन पर कम कॉन्टेंट है, तो डेवलपर को सभी कॉन्टेंट के लिए एक ही ऐप्लिकेशन बनाना चाहिए.

ऐसे ऐप्लिकेशन को अनुमति नहीं दी जाती है जिसे किसी अपने-आप चलने वाले टूल, विज़ार्ड सेवा ने बनाया हो या जो ऐप्लिकेशन टेंप्लेट पर आधारित हों और उन्हें Google Play पर दूसरे लोगों की तरफ़ से उस सेवा का ऑपरेटर सबमिट करता है. ऐसे ऐप्लिकेशन को सिर्फ़ तभी अनुमति दी जाती है, जब वे किसी सेवा के ऑपरेटर की तरफ़ से नहीं, बल्कि अपने-आप चलने वाले टूल के उपयोगकर्ता के रजिस्टर किए गए डेवलपर खाते से प्रकाशित किए जाते हैं.

विज्ञापन के लिए बनाए गए ऐप्लिकेशन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जिनका मुख्य काम विज्ञापन दिखाना है.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

वे ऐप्लिकेशन जिन पर उपयोगकर्ता के हर कार्रवाई के बाद, पेज पर अचानक दिखने वाले विज्ञापन आ जाते हैं. इनमें क्लिक, स्वाइप वगैरह शामिल हैं लेकिन ये इन्हीं तक सीमित नहीं हैं.

पक्का करें कि आपका ऐप्लिकेशन भरोसेमंद, दिलचस्प, और बेहतर उपयोगकर्ता अनुभव देता है.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे ऐप्लिकेशन जिन्हें बेवजह बनाया गया है या जिनमें कोई सुविधा नहीं है

अधूरी सुविधाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो क्रैश हो जाते हैं, ज़बरदस्ती बंद हो जाते हैं, फ़्रीज़ हो जाते हैं या फिर असामान्य तरह से काम करते हैं.
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे ऐप्लिकेशन जो इंस्टॉल नहीं होते
ऐसे ऐप्लिकेशन जो इंस्टॉल तो होते हैं, लेकिन लोड नहीं होते
ऐसे ऐप्लिकेशन जो लोड तो होते हैं, लेकिन काम नहीं करते

हमारा मकसद है कि Android Instant Apps के साथ उपयोगकर्ता को शानदार और बिना रुकावट वाले अनुभव मिलें. साथ ही, निजता और सुरक्षा के सबसे ऊंचे मानकों का पालन भी किया जाए. हमारी नीतियां इस तरह से बनाई गई हैं कि वे यह मकसद पूरा करने में मददगार हों.

Google Play से Android Instant Apps को उपयोगकर्ताओं तक पहुंचाने के लिए, डेवलपर को सभी Google Play की डेवलपर कार्यक्रम नीतियों का पालन करना होगा. इनके अलावा, नीचे दी गई नीतियों का भी पालन करना होगा.

पहचान

लॉगिन की सुविधा देने वाले झटपट ऐप्लिकेशन में, डेवलपर को पासवर्ड के लिए Smart Lock की सुविधा जोड़नी होगी.

लिंक देकर मदद करना

Android Instant Apps के डेवलपर के लिए ज़रूरी है कि वे अपने झटपट ऐप्लिकेशन में दूसरे ऐप्लिकेशन के लिंक सही तरीके से शामिल करें. अगर डेवलपर के झटपट ऐप्लिकेशन या इंस्टॉल किए गए ऐप्लिकेशन में ऐसे लिंक मौजूद हैं जो उपयोगकर्ताओं को किसी झटपट ऐप्लिकेशन तक ले जा सकते हैं, तो डेवलपर को अपने ऐप्लिकेशन के वेबव्यू में अन्य लिंक नहीं दिखाने चाहिए. डेवलपर के लिए ज़रूरी है कि वह ऐसे तरीके इस्तेमाल करने के बजाय, उपयोगकर्ताओं को उस झटपट ऐप्लिकेशन तक भेजे.

तकनीकी जानकारी

डेवलपर को Android Instant Apps से जुड़ी उन तकनीकी बातों और ज़रूरी शर्तों का पालन करना होगा जिनके बारे में Google ने बताया है. इनमें समय-समय पर बदलाव भी हो सकते हैं. हमारे सार्वजनिक दस्तावेज़ में मौजूद जानकारी और ज़रूरी शर्तें भी इनमें शामिल हैं.

ऐप्लिकेशन इंस्टॉल करने की सुविधा का ऑफ़र देना

झटपट ऐप्लिकेशन, उपयोगकर्ता को ऐसे ऐप्लिकेशन का ऑफ़र दे सकता है जिसे इंस्टॉल किया जा सके. हालांकि, यह झटपट ऐप्लिकेशन का मुख्य मकसद नहीं होना चाहिए. इंस्टॉल करने का ऑफ़र देते समय, डेवलपर को:

- मटीरियल डिज़ाइन वाला "ऐप्लिकेशन डाउनलोड करें" आइकॉन और इंस्टॉल करने वाले बटन के लिए, "इंस्टॉल करें" लेबल इस्तेमाल करना चाहिए.
- अपने झटपट ऐप्लिकेशन में, किसी ऐप्लिकेशन को इंस्टॉल करने के दो या तीन से ज़्यादा अनुरोध शामिल नहीं करने चाहिए.
- किसी ऐप्लिकेशन को इंस्टॉल करने का अनुरोध उपयोगकर्ता को दिखाने के लिए, बैनर का या विज्ञापन जैसी दूसरी तकनीक का इस्तेमाल नहीं करना चाहिए.

झटपट ऐप्लिकेशन के बारे में ज़्यादा जानकारी और UX से जुड़े दिशा-निर्देश, उपयोगकर्ता को बेहतर अनुभव देने के सबसे सही तरीके पर जाकर देखे जा सकते हैं.

डिवाइस में बदलाव करने की स्थिति

झटपट ऐप्लिकेशन को उपयोगकर्ता के डिवाइस में ऐसे बदलाव नहीं करने चाहिए जो झटपट ऐप्लिकेशन के सत्र के समय से ज़्यादा देर तक बने रहें. उदाहरण के लिए, झटपट ऐप्लिकेशन उपयोगकर्ता के डिवाइस का वॉलपेपर नहीं बदल सकते. इसके अलावा, कोई होमस्क्रीन विजेट भी नहीं बना सकते.

ऐप्लिकेशन कैसा दिखेगा

डेवलपर को यह पक्का करना चाहिए कि उपयोगकर्ता को झटपट ऐप्लिकेशन इस तरह दिखाई दें कि उसे अपने डिवाइस पर झटपट ऐप्लिकेशन चलते रहने के बारे में हर समय पता रहे.

डिवाइस पहचानकर्ता

झटपट ऐप्लिकेशन ऐसे डिवाइस पहचानकर्ताओं को ऐक्सेस नहीं कर सकते जो (1) झटपट ऐप्लिकेशन बंद होने के बाद भी बने रहते हैं और (2) जिन्हें उपयोगकर्ता फिर से सेट नहीं कर सकते. इनके उदाहरणों में नीचे दी गई जानकारी शामिल है. हालांकि, इनमें अन्य डिवाइस पहचानकर्ता भी शामिल हो सकते हैं:

बिल्ड सीरियल
किसी भी नेटवर्किंग चिप के Mac पते
IMEI, IMSI

अगर फ़ोन नंबर रनटाइम अनुमति के दौरान मिला है, तो झटपट ऐप्स उसे ऐक्सेस कर सकते हैं. डेवलपर को इन पहचानकर्ताओं या दूसरे किसी भी तरीके का इस्तेमाल करके, उपयोगकर्ता को फ़िंगरप्रिंट करने की कोशिश नहीं करनी चाहिए.

नेटवर्क ट्रैफ़िक

झटपट ऐप्लिकेशन में चलने वाले नेटवर्क ट्रैफ़िक को एचटीटीपीएस जैसे किसी TLS प्रोटोकॉल का इस्तेमाल करके, एन्क्रिप्ट (सुरक्षित) किया जाना ज़रूरी है.

परिवारों की ज़िंदगी बेहतर बनाने के टूल के तौर पर टेक्नोलॉजी का इस्तेमाल बढ़ता जा रहा है. अभिभावक अपने बच्चों से शेयर करने के लिए सुरक्षित और अच्छी क्वालिटी के कॉन्टेंट खोज रहे हैं. हो सकता है कि आप खास तौर पर बच्चों के लिए ऐप्लिकेशन बना रहे हों या फिर आपका ऐप्लिकेशन ऐसा हो जो उनका ध्यान खींचता हो. Google Play यह पक्का करने में आपकी मदद करना चाहता है कि आपका ऐप्लिकेशन सभी उपयोगकर्ताओं के लिए सुरक्षित है, जिसमें परिवार भी शामिल हैं.

अलग-अलग जगह-भाषा और परिस्थितियों में "बच्चे" शब्द का मतलब अलग हो सकता है. आप अपने कानूनी सलाहकार से पूछ सकते हैं कि आपके ऐप्लिकेशन पर किस तरह की कानूनी जवाबदेही और/या उम्र से जुड़े प्रतिबंध लागू हो सकते हैं. आपका ऐप्लिकेशन कैसा है इस बारे में आपसे बेहतर कोई नहीं जानता. इसलिए, हम आप पर भरोसा करके यह पक्का करना चाहते हैं कि Google Play पर मौजूद ऐप्लिकेशन परिवारों के लिए सुरक्षित हैं.

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को, परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेना चाहिए. हालांकि, अगर आपका ऐप्लिकेशन सिर्फ़ बच्चों के लिए नहीं है, तब भी आपको परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने का सुझाव दिया जाता है. यह आपके ऐप्लिकेशन को सही लोगों तक पहुंचाने का एक बेहतर तरीका है. अगर आप परिवार के लिए बनाए गए कार्यक्रम में हिस्सा नहीं लेते हैं, तो भी आपको नीचे दी गई Google Play की परिवार के लिए बनाई गई नीति का पालन करना होगा. साथ ही, आपको Google Play की डेवलपर कार्यक्रम की नीतियों और डेवलपर डिस्ट्रीब्यूशन एग्रीमेंट का भी पालन करना होगा.

Play Console से जुड़ी ज़रूरी शर्तें

टारगेट ऑडियंस और कॉन्टेंट

ऐप्लिकेशन प्रकाशित करने से पहले, आपको Google Play Console के टारगेट ऑडियंस और कॉन्टेंट सेक्शन में जाकर, उम्र समूहों की सूची में से अपनी टारगेट ऑडियंस चुननी होगी. भले ही आपने Google Play Console में किसी भी उम्र समूह को टारगेट ऑडियंस के तौर पर चुना हो, लेकिन अगर आप अपने ऐप्लिकेशन में ऐसी तस्वीरों और शब्दों को शामिल करते हैं जिन्हें बच्चों को टारगेट करने वाला माना जा सकता है, तो इसका असर आपकी दी गई जानकारी के आकलन पर दिख सकता है. यह आकलन Google Play करता है, ताकि पक्का हो सके कि टारगेट

ऑडियंस के बारे में आपने जो जानकारी दी है वह सही है या नहीं. Google Play को यह अधिकार है कि वह ऐप्लिकेशन के बारे में आपकी दी गई जानकारी की समीक्षा कर सके. समीक्षा के बाद यह तय किया जाता है कि अपनी टारगेट ऑडियंस के बारे में आपने जो जानकारी दी है वह सही या नहीं.

अगर आप ऐसी टारगेट ऑडियंस चुनते हैं जिनमें सिर्फ़ वयस्क शामिल हैं, लेकिन Google को पता चलता है कि यह सही नहीं है, क्योंकि आपका ऐप्लिकेशन बच्चों और वयस्कों दोनों को टारगेट कर रहा है. ऐसे में आपके पास यह बताने का विकल्प होगा कि आपका ऐप्लिकेशन बच्चों को टारगेट नहीं करता है. इसके लिए आपको एक चेतावनी लेबल लगाने की सहमति देनी होगी.

आपको अपने ऐप्लिकेशन की टारगेट ऑडियंस के लिए एक से ज़्यादा उम्र समूह तभी चुनने चाहिए, जब आपने ऐप्लिकेशन को उन चुने हुए उम्र समूह (समूहों) के लोगों को ध्यान में रखकर बनाया हो. साथ ही, आप पक्के तौर पर यह जानते हो कि आपका ऐप्लिकेशन उनके लिए पूरी तरह सही है. उदाहरण के लिए, अगर आपका ऐप्लिकेशन बच्चों, छोटे बच्चों, और प्रीस्कूल में पढ़ने वाले बच्चों के लिए है, तो उम्र समूह टारगेट करते समय "पांच साल और उससे कम" उम्र का समूह ही चुनना चाहिए. अगर आपका ऐप्लिकेशन किसी खास कक्षा में पढ़ने वाले छात्र/छात्राओं के लिए है, तो वह उम्र समूह चुने जो उस कक्षा में पढ़ने वालों के हिसाब से सबसे सही हो. आपको वयस्कों और बच्चों, दोनों को शामिल करने वाला उम्र समूह तभी चुनना चाहिए, जब वाकई आपका ऐप्लिकेशन सभी उम्र के लोगों के लिए हो.

टारगेट ऑडियंस और कॉन्टेंट सेक्शन के अपडेट

आप जब चाहें, Google Play Console के टारगेट ऑडियंस और कॉन्टेंट सेक्शन में जाकर, अपने ऐप्लिकेशन की जानकारी अपडेट कर सकते हैं. 'Google Play स्टोर' पर यह जानकारी दिखाई देने से पहले ऐप्लिकेशन अपडेट ज़रूरी है. हालांकि, आप Google Play Console के इस सेक्शन में जो भी बदलाव करेंगे उनकी समीक्षा ऐप्लिकेशन अपडेट सबमिट किए जाने से पहले भी यह देखने के लिए की जा सकती है कि वे नीति का पालन करते हैं या नहीं.

हमारा सुझाव है कि अगर आप अपने ऐप्लिकेशन के टारगेट उम्र समूह में बदलाव करते हैं या फिर इन-ऐप्लिकेशन खरीदारी या विज्ञापनों की शुरुआत करते हैं, तो अपने मौजूदा दर्शकों को इसकी जानकारी दें. ऐसा करने के लिए, आप ऐप्लिकेशन के स्टोर पेज के "नया क्या है" सेक्शन का या फिर इन-ऐप्लिकेशन सूचनाओं का इस्तेमाल कर सकते हैं.

Play Console में गलत तरीके से पेश करना

अगर आप टारगेट ऑडियंस और कॉन्टेंट सेक्शन सहित Play Console में अपने ऐप्लिकेशन की किसी जानकारी को गलत तरीके से पेश करते हैं, तो आपका खाता हटाया या निलंबित किया जा सकता है. इसलिए, सही जानकारी देना ज़रूरी है.

परिवार नीति से जुड़ी ज़रूरी शर्तें

अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो आपको आगे दी गई ज़रूरी शर्तों का पालन करना होगा. ये शर्तें पूरी नहीं करने पर, ऐप्लिकेशन हटाया या निलंबित किया जा सकता है.

1. ऐप्लिकेशन का कॉन्टेंट: आपके ऐप्लिकेशन का वह कॉन्टेंट जिसे बच्चे ऐक्सेस कर सकते हैं उसे बच्चों के लिए सही होना चाहिए.
2. Google Play Console में सवालों के जवाब: आपको Google Play Console में अपने ऐप्लिकेशन से जुड़े सवालों के सही जवाब देने चाहिए. साथ ही, अपने ऐप्लिकेशन में कोई भी बदलाव होने पर उन जवाबों को अपडेट करना चाहिए.
3. विज्ञापन: अगर आपका ऐप्लिकेशन बच्चों को या ऐसे लोगों को विज्ञापन दिखाता है जिनकी उम्र के बारे में पता नहीं है, तो आप:

ऐप्लिकेशन इस्तेमाल करने वाले उन लोगों को विज्ञापन दिखाने के लिए, सिर्फ़ Google Play से प्रमाणित किए गए विज्ञापन SDK टूल इस्तेमाल करें;
यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में, रीमार्केटिंग या रुचि के हिसाब से विज्ञापन शामिल नहीं हैं;
यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों का कॉन्टेंट बच्चों के लिए सही है;
यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में ऐसी सामग्री है जो परिवार के लिए बनाए गए विज्ञापन फ़ॉर्मैट की शर्तें पूरी करती है; और
यह भी पक्का करें कि बच्चों को विज्ञापन दिखाने से जुड़े सभी लागू कानूनी नियमों और उद्योग मानकों का पालन हो रहा है.

4. डेटा इकट्ठा करना: आपको अपने ऐप्लिकेशन में, बच्चों से मिली किसी भी तरह की निजी और संवेदनशील जानकारी इकट्ठा करने के बारे में बताना चाहिए. इसमें आपके ऐप्लिकेशन में इस्तेमाल किए गए एपीआई और SDK टूल से मिलने वाली जानकारी भी शामिल है. बच्चों से मिली संवेदनशील जानकारी में पहचान की पुष्टि करने की जानकारी, माइक्रोफ़ोन और कैमरा सेंसर का डेटा, डिवाइस का डेटा, Android आईडी, विज्ञापन देखने का डेटा, और विज्ञापन आईडी की जानकारी शामिल है. इसके अलावा, दूसरी तरह की जानकारी भी शामिल है.
5. एपीआई और SDK टूल:आपको यह पक्का करना चाहिए कि आपका ऐप्लिकेशन हर एपीआई और SDK टूल को सही तरीके से लागू करे.
   सिर्फ़ बच्चों को टारगेट करने वाले ऐप्लिकेशन में ऐसा कोई एपीआई या SDK टूल नहीं होना चाहिए जिसे बच्चों से जुड़ी सेवाओं में इस्तेमाल करने की मंज़ूरी न मिली हो. इसमें, Google साइन-इन (या किसी Google खाते से जुड़ा डेटा ऐक्सेस करने वाली कोई भी अन्य Google API सेवा), Google Play गेम सेवाएं, और पुष्टि करने और अनुमति देने के लिए OAuth तकनीक का इस्तेमाल करने वाली कोई भी दूसरी एपीआई सेवा शामिल है.
   बच्चों और बड़ों, दोनों तरह के दर्शकों को टारगेट करने वाले ऐप्लिकेशन को ऐसे एपीआई या SDK टूल लागू नहीं करने चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल करने की मंज़ूरी नहीं मिली है. इन्हें तभी लागू किया जा सकता है, जब ये न्यूट्रल एज स्क्रीन के तहत इस्तेमाल किए जाते हों. इसके अलावा, इन्हें ऐसे तरीके से लागू न किया जाए जिससे बच्चों से डेटा इकट्ठा हो (जैसे कि वैकल्पिक सुविधा के तौर पर, 'Google साइन-इन' का विकल्प देना). इस बात का ध्यान रखें कि सभी उपयोगकर्ताओं के पास आपके ऐप्लिकेशन और उसकी सुविधाएं का ऐक्सेस हो.
6. निजता नीति: आपको अपने ऐप्लिकेशन के स्टोर पेज पर, ऐप्लिकेशन की निजता नीति के बारे में बताने वाला लिंक देना चाहिए. जब तक ऐप्लिकेशन 'स्टोर' में मौजूद हो, तब तक यह लिंक हमेशा रहना चाहिए. साथ ही, इसे किसी ऐसी निजता नीति से जोड़ा जाना चाहिए जो आपके ऐप्लिकेशन के डेटा संग्रह और उसके इस्तेमाल के साथ दूसरी चीज़ों की सही जानकारी देती हो.
7. खास पाबंदियां:
   अगर आपके ऐप्लिकेशन में ऑगमेंटेड रिएलिटी (एआर) का इस्तेमाल किया जाता है, तो आपको एआर सेक्शन लॉन्च होते ही एक सुरक्षा चेतावनी शामिल करनी चाहिए. चेतावनी में नीचे दी गई जानकारी शामिल होनी चाहिए:
      माता-पिता के निरीक्षण की अहमियत के बारे में सही मैसेज.
      असली दुनिया के असली खतरों को लेकर सजग रहने का रिमाइंडर (उदाहरण के लिए, अपने आस-पास होने वाली चीज़ों के बारे में सजग रहना).
   आपके ऐप्लिकेशन को ऐसे डिवाइस के इस्तेमाल करने की ज़रूरत नहीं पड़नी चाहिए जिसके लिए यह सलाह दी गई हो कि बच्चे इसका इस्तेमाल न करें. (उदाहरण के लिए, Daydream, Oculus)
8. कानूनी अनुपालन: आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन (साथ ही, ऐसे सभी एपीआई या SDK टूल जिनकी मांग या इस्तेमाल आपका ऐप्लिकेशन करता है) अमेरिका में लागू बच्चों की ऑनलाइन

निजता और संरक्षण अधिनियम (कोपा), यूरोपीय संघ में लागू सामान्य डेटा से जुड़े सुरक्षा कानून (जीडीपीआर), और किसी भी अन्य लागू कानून या नियम का पालन करता है.

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

ऐसे ऐप्लिकेशन जो अपने स्टोर पेज में बच्चों के लिए खेल को बढ़ावा देते हैं, लेकिन ऐप्लिकेशन का कॉन्टेंट सिर्फ़ वयस्को के लिए है.
ऐसे ऐप्लिकेशन जो उन एपीआई को लागू करते हैं जिनकी सेवा की शर्तें ऐसी हैं जो बच्चों के लिए बने ऐप्लिकेशन में इनके इस्तेमाल पर पाबंदी लगाती हैं.
ऐसे ऐप्लिकेशन जिनमें शराब, तंबाकू के बारे में बढ़ा-चढ़ाकर बताया जाता है या ऐसे केमिकल या दवाइयों का बखान किया जाता है जो आपके शरीर को नुकसान पहुंचा सकती हैं और जिन्हें सरकार की देख-रेख में बनाया और रखा जाता है.
ऐसे ऐप्लिकेशन जिनमें असली या नकली जुआ शामिल होता है.
ऐसे ऐप्लिकेशन जिनमें हिंसा, खून खराबे या चौंकाने वाला ऐसा कॉन्टेंट शामिल है जो बच्चों के लिए सही नहीं है.
डेटिंग सेवाएं देने वाले या ऐसे ऐप्लिकेशन जो शादीशुदा ज़िंदगी से जुड़ी या यौन सलाह देते हैं.
ऐसे ऐप्लिकेशन जो बच्चों को वे विज्ञापन दिखाते हैं जो बड़ों के लिए बनाए गए हैं.

परिवार के लिए बनाए गए कार्यक्रम

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को, परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेना चाहिए. अगर आपका ऐप्लिकेशन बच्चों और परिवारों सहित सभी के लिए है, तो आप भी इस कार्यक्रम में हिस्सा लेने के लिए आवेदन कर सकते हैं.

कार्यक्रम में शामिल होने के लिए स्वीकार किए जाने से पहले, आपके ऐप्लिकेशन को Google Play की डेवलपर कार्यक्रम की नीतियों और डेवलपर डिस्ट्रीब्यूशन एग्रीमेंट की शर्तों को पूरा करना होगा. साथ ही, परिवार नीति और परिवार के लिए बनाए गए कार्यक्रम की सभी शर्तों को भी पूरा करना होगा.

इस कार्यक्रम में अपने ऐप्लिकेशन को शामिल कराने की प्रोसेस के बारे में ज़्यादा जानने के लिए, यहां क्लिक करें.

कार्यक्रम की ज़रूरी शर्तें

परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने वाले सभी ऐप्लिकेशन का और उनमें शामिल विज्ञापन का कॉन्टेंट ऐसा होना चाहिए जो बच्चों के लिए सही और उनके काम का हो. साथ ही, इन ऐप्लिकेशन को नीचे दी गई सभी ज़रूरी शर्तें भी पूरी करनी होंगी. परिवार के लिए बनाए गए कार्यक्रम में स्वीकार किए गए ऐप्लिकेशन को कार्यक्रम की सभी ज़रूरी शर्तों का हमेशा पालन करते रहना होगा. Google Play किसी भी ऐप्लिकेशन को परिवार के लिए बनाए गए कार्यक्रम के लिए गलत पाए जाने पर उसे अपनी समझदारी से अस्वीकार करने या हटाने का अधिकार सुरक्षित रखता है.

परिवार के लिए बनाए गए कार्यक्रम की ज़रूरी शर्तें

1. ऐप्लिकेशन को ईएसआरबी (एंटरटेनमेंट सॉफ्टवेयर रेटिंग बोर्ड) से 'सभी' या 'सभी 10+' या इसके बराबर रेटिंग मिलनी चाहिए.
2. आपको Google Play Console की कॉन्टेंट रेटिंग वाली सवालों की सूची में, इस बात की सही जानकारी देनी चाहिए कि ऐप्लिकेशन के कॉन्टेंट और उसे इस्तेमाल करने वाले लोगों की एक-दूसरे तक किस तरह पहुंच है. इसमें यह जानकारी भी शामिल है कि क्या:

ऐप्लिकेशन इस्तेमाल करने वाले लोग जानकारी ऐक्सेस कर सकते हैं या उसे शेयर कर सकते हैं; आपका ऐप्लिकेशन उपयोगकर्ताओं की जानकारी तीसरे पक्षों के साथ शेयर करता है; और आपका ऐप्लिकेशन उपयोगकर्ता की मौजूदा जगह की जानकारी अन्य उपयोगकर्ताओं के साथ शेयर करता है.

3. अगर आपका ऐप्लिकेशन Android स्पीच एपीआई का इस्तेमाल करता है, तो उसके RecognizerIntent.EXTRA_CALLING_PACKAGE को PackageName पर सेट किया जाना चाहिए.
4. ऐप्लिकेशन को सिर्फ़ Google Play से प्रमाणित किए गए विज्ञापन SDK टूल इस्तेमाल करने चाहिए.
5. बच्चों के लिए बनाए गए ऐप्लिकेशन, जगह की जानकारी की अनुमतियां नहीं मांग सकते.
6. ऐप्लिकेशन को ब्लूटूथ कनेक्शन का अनुरोध करते समय कंपैनियन डिवाइस मैनेजर (सीडीएम) का इस्तेमाल करना ज़रूरी है. हालांकि, अगर आपका ऐप्लिकेशन ऐसे डिवाइस ऑपरेटिंग सिस्टम वर्शन को टारगेट करता है जो कंपैनियन डिवाइस मैनेजर (सीडीएम) के साथ काम नहीं करते तो.यह ज़रूरी नहीं है.
   ऐसे ऐप्लिकेशन जिन्हें 'ईएसआरबी सभी' रेटिंग दी गई है, लेकिन उनमें जुए के कॉन्टेंट के विज्ञापन शामिल हैं
   अभिभावकों या देखभाल करने वालों के लिए बने ऐप्लिकेशन (उदाहरण के लिए, स्तनपान कराने की गतिविधि ट्रैक करने वाला ऐप्लिकेशन, डेवलपर गाइड)
   माता-पिता के लिए गाइड या ऐसे डिवाइस मैनेजमेंट ऐप्लिकेशन जिनका इस्तेमाल सिर्फ़ माता-पिता या देखभाल करने वाले लोग ही कर सकते हैं

श्रेणियां

अगर आपको परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने की मंज़ूरी दी गई है, तो आप खास तौर पर परिवारों के लिए बनी दूसरी श्रेणी चुन सकते हैं जिसमें आपके ऐप्लिकेशन की जानकारी दी जाती है. यहां परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने वाले ऐप्लिकेशन के लिए मौजूद श्रेणियां दी गई हैं:

ऐक्शन और रोमांच: ऐक्शन वाले ऐप्लिकेशन/गेम जिनमें आसान रेसिंग गेम से लेकर परी कथा के रोमांच तक सब कुछ शामिल है. साथ ही, ऐसे ऐप्लिकेशन और गेम भी हैं जिन्हें रोमांच पैदा करने के मकसद से बनाया गया है.

दिमाग लगाने वाले गेम: ऐसे गेम जिनमें गेम खेलने वालों को सोचना पड़ता है. इनमें पहेलियां, मिलान करने वाले गेम, सवाल-जवाब, और दूसरे गेम शामिल हैं जो याददाश्त, काबिलियत या तर्क को चुनौती देते हैं.

रचनात्मकता: ऐसे ऐप्लिकेशन और गेम जो रचनात्मकता को बढ़ावा देते हैं. इनमें ड्रॉइंग, पेंटिंग, कोडिंग, और अन्य ऐप्लिकेशन और गेम शामिल हैं जिनमें आप चीज़ें बना सकते हैं.

शिक्षा: ऐसे ऐप्लिकेशन और गेम जिन्हें कुछ विशेषज्ञों (उदाहरण के लिए, शिक्षकों, सिखाने में महारत रखने वालों, शोध करने वालों) से मिली जानकारी की मदद से बनाया गया है, ताकि सीखने को बढ़ावा मिल सके. इनमें शिक्षा देने वाले, रचनात्मक तरीके से सिखाने वाले, सामाजिक-भावनात्मक, और शारीरिक शिक्षा से जुड़े गेम शामिल हैं. साथ ही, बुनियादी जीवन कौशल, तर्क के साथ सोचना, और समस्याएं सुलझाने से जुड़ी शिक्षा भी शामिल है.

संगीत और वीडियो: संगीत या वीडियो वाले ऐसे ऐप्लिकेशन और गेम जिनमें इंस्ट्रूमेंट सिम्युलेशन वाले ऐप्लिकेशन से लेकर वीडियो और म्यूज़िकल ऑडियो कॉन्टेंट मुहैया कराने वाले ऐप्लिकेशन तक सब कुछ शामिल है.

किरदार निभाना: ऐसे ऐप्लिकेशन और गेम जिनमें गेम खेलने वाला या ऐप्लिकेशन को इस्तेमाल करने वाला कोई किरदार निभा सकता है, जैसे कि शेफ़, देखभाल करने वाले, राजकुमार/राजकुमारी, फ़ायर फ़ाइटर, पुलिसकर्मी या किसी काल्पनिक किरदार की भूमिका निभाना.

नीचे दी गई नीतियां किसी भी तरह के विज्ञापन (जिसमें आपके ऐप्लिकेशन और तीसरे पक्षों के लिए विज्ञापन शामिल हैं), इन-ऐप्लिकेशन खरीदारी के ऑफ़र या किसी भी अन्य व्यावसायिक कॉन्टेंट (जैसे कि सशुल्क उत्पाद प्लेसमेंट) पर लागू होती हैं, जिन्हें ऐप्लिकेशन इस्तेमाल करने वाले लोगों को मुहैया कराया जाता है. इन लोगों पर 'परिवार नीति' और 'परिवार के लिए बनाए गए' कार्यक्रम की ज़रूरी शर्तें लागू होती हैं. सभी तरह के विज्ञापन, इन-ऐप्लिकेशन खरीदारी के ऑफ़र, और इन ऐप्लिकेशन की वाणिज्यिक सामग्री को सभी लागू कानूनों और विनियमों (जिनमें कोई भी प्रासंगिक स्व-विनियामक या उद्योग दिशा-निर्देश शामिल हैं) का पालन करना चाहिए.

Google Play, व्यावसायिक फ़ायदे के लिए ज़्यादा आक्रामक विज्ञापन दिखाने वाले ऐप्लिकेशन पर नीति उल्लंघन ठीक करने के तरीके(एनफ़ोर्समेंट) को लागू करने का अधिकार सुरक्षित रखता है.

विज्ञापन फ़ॉर्मैट की शर्तें

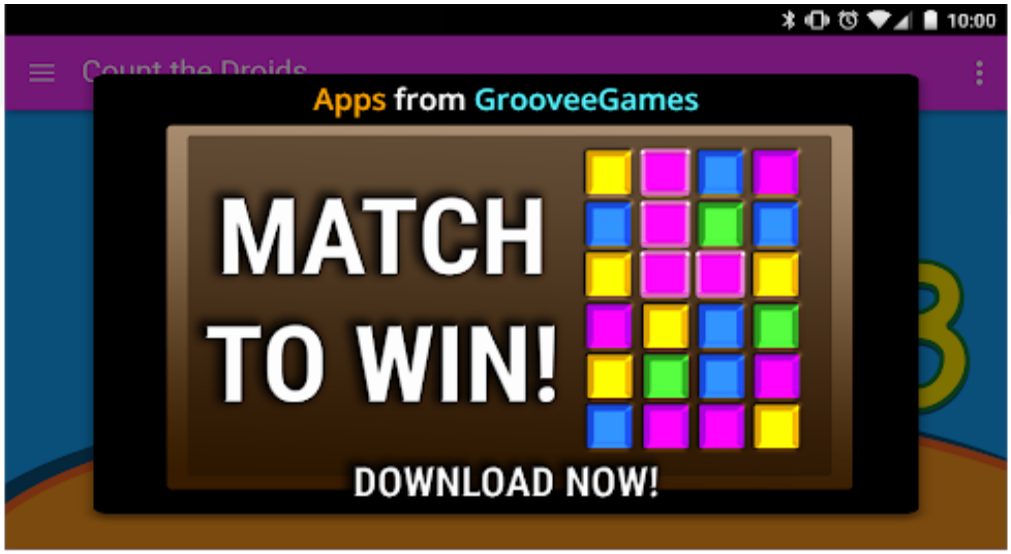
विज्ञापनों और इन-ऐप्लिकेशन खरीदारी के ऑफ़र देने वाले कॉन्टेंट को गुमराह करने वाला नहीं होना चाहिए. साथ ही, उन्हें इस तरह से डिज़ाइन किया जाए कि बच्चे अनजाने में क्लिक न करें. नीचे दी गई चीज़ों पर पाबंदी है:

- विज्ञापन वॉल का इस्तेमाल
- ऐसे विज्ञापन जो ऐप्लिकेशन के सामान्य इस्तेमाल में रुकावट डालते हैं और 5 सेकंड तक चलने के बाद भी इन्हें बंद नहीं किया जा सकता
- ऐप्लिकेशन लॉन्च होते ही पेज पर अचानक दिखने वाले विज्ञापन या इन-ऐप्लिकेशन खरीदारी के ऑफ़र
- किसी पेज पर दिखाई देने वाले कई सारे विज्ञापन प्लेसमेंट
- ऐसे विज्ञापन या इन-ऐप्लिकेशन खरीदारी के ऑफ़र जिनकी आपके ऐप्लिकेशन के कॉन्टेंट से साफ़ तौर पर अलग पहचान नहीं की जा सकती
- विज्ञापन के दर्शकों की संख्या बढ़ाने या इन-ऐप्लिकेशन खरीदारी को बढ़ाने के लिए, भावनात्मक रूप से गुमराह करने या चौंकाने वाले तरीकों का इस्तेमाल करना
- इन-ऐप्लिकेशन खरीदारी करने के लिए, आभासी गेम के सिक्कों और असली पैसों के बीच फ़र्क़ न दिखाना

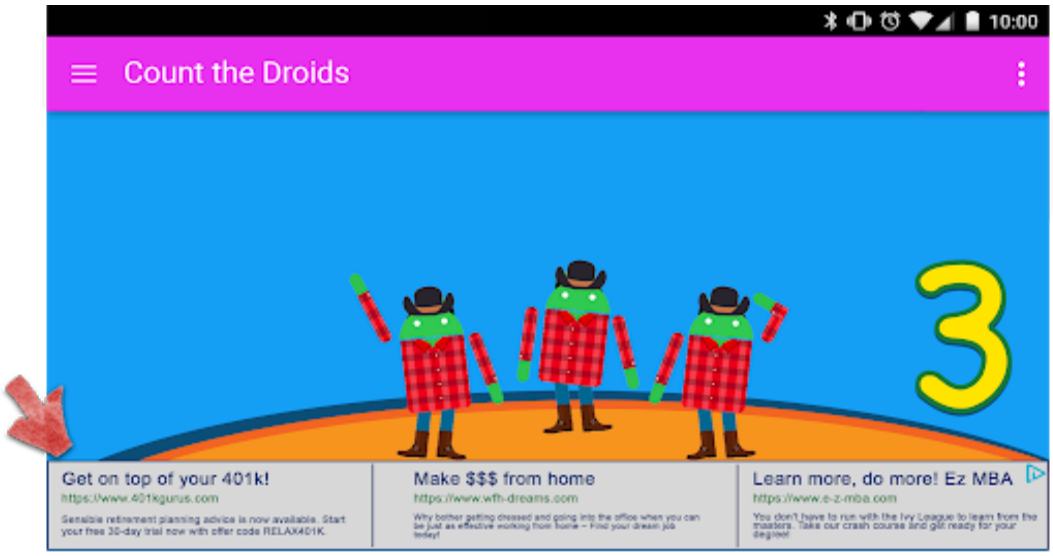
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- ऐसे विज्ञापन जो उस समय उपयोगकर्ता की पहुंच से दूर हो जाते हैं, जब वह उन्हें बंद करने की कोशिश करता है

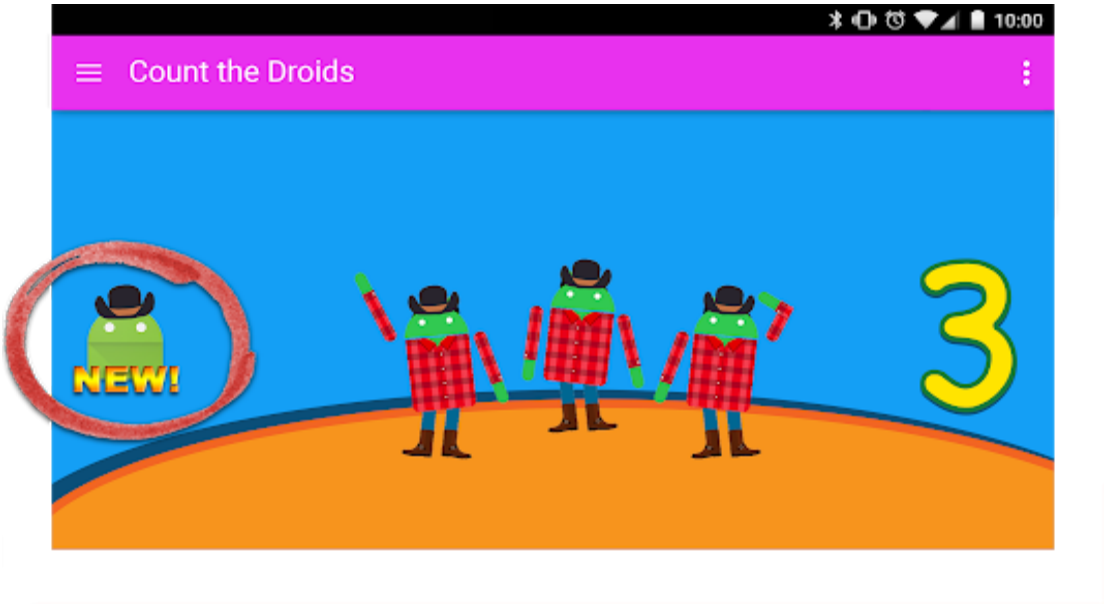
ऐसे विज्ञापन जो उपयोगकर्ता को विज्ञापन हटाने का तरीका बताए बिना, डिवाइस की पूरी स्क्रीन या ज़्यादातर हिस्से पर दिखने लगते हैं. इसका उदाहरण नीचे देखिए:



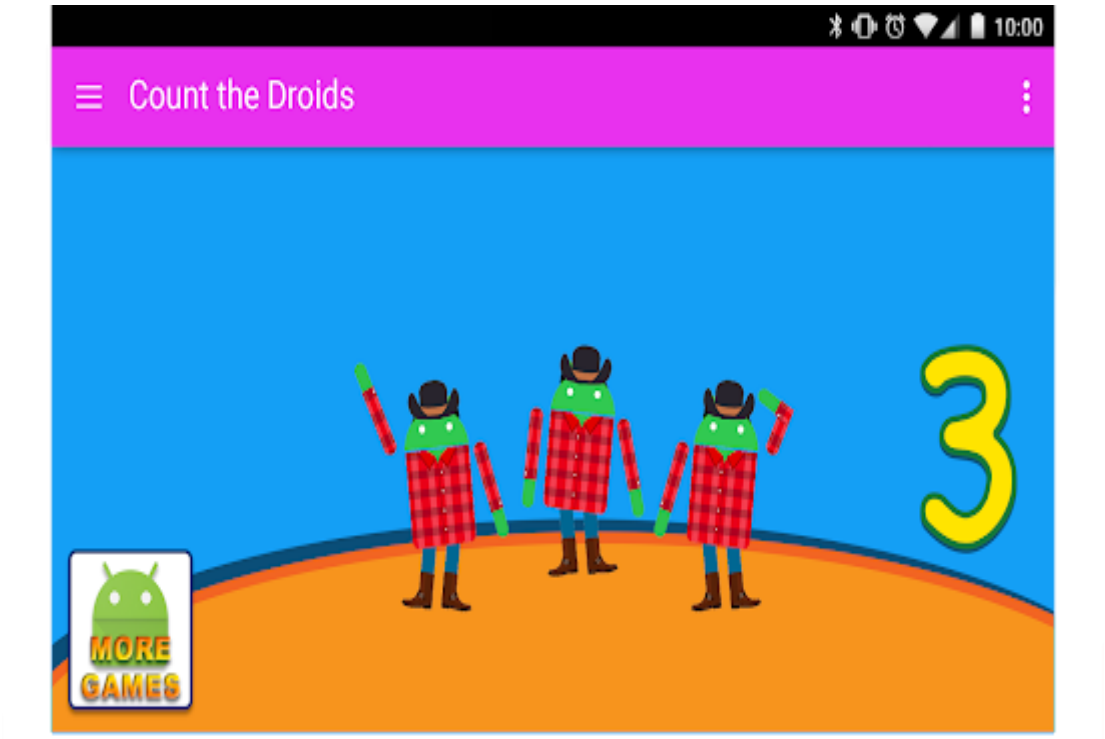
ऐसे बैनर विज्ञापन जिनमें एक से ज़्यादा ऑफ़र दिखाए जा रहे हों. इसका उदाहरण नीचे देखिए:



ऐसे विज्ञापन जिन्हें उपयोगकर्ता गलती से ऐप्लिकेशन का कॉन्टेंट समझ सकता है. इसका उदाहरण नीचे देखिए:



ऐसे बटन या विज्ञापन जो आपके दूसरे Google Play स्टोर पेज का प्रचार करते हैं और उन्हें ऐप्लिकेशन के कॉन्टेंट से अलग नहीं पहचाना जा सकता. इसका उदाहरण नीचे देखिए:



यहां कुछ ऐसी विज्ञापन सामग्री के उदाहरण दिए जा रहे हैं, जो बच्चों को नहीं दिखाए जाने चाहिए.

गलत मीडिया कॉन्टेंट: टीवी शो, फिल्मों, म्यूज़िक एल्बम या किसी भी दूसरे मीडिया आउटलेट के ऐसे विज्ञापन जो बच्चों के लिए उचित नहीं हैं.
गलत वीडियो गेम और डाउनलोड किए जा सकने वाले सॉफ़्टवेयर: डाउनलोड किए जा सकने वाले सॉफ़्टवेयर और इलेक्ट्रॉनिक वीडियो गेम के ऐसे विज्ञापन जो बच्चों के लिए उचित नहीं हैं.
नशीली दवाएं या नुकसान पहुंचाने वाली चीज़ें: शराब, तंबाकू, नशीली दवाएं या नुकसान पहुंचाने वाली किसी और चीज़ के विज्ञापन.
जुआ: कृत्रिम जुआ, प्रतियोगिताओं या स्वीपस्टैक के प्रचारों के विज्ञापन, भले ही इनका इस्तेमाल मुफ़्त क्यों न हो.
वयस्क और अश्लील कॉन्टेंट: ऐसे विज्ञापन जिनमें यौन, यौन रूप से अश्लील, और परिपक्व सामग्री हो.
डेटिंग या संबंध: डेटिंग या वयस्क संबंध वाली वेबसाइट के विज्ञापन.
हिंसा से जुड़ा कॉन्टेंट: ऐसे विज्ञापन जिसमें हिंसा और ऐसा दिल दहलाने वाला कॉन्टेंट हो, जो बच्चों के लिए उचित न हो.

विज्ञापन SDK टूल

बच्चों को विज्ञापन दिखाने के लिए सिर्फ़ Google Play से प्रमाणित विज्ञापन SDK टूल का इस्तेमाल किया जा सकता है. 'परिवार के लिए बनाए गए' कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़ Google Play से प्रमाणित विज्ञापन SDK टूल का इस्तेमाल करें. ऐसे ऐप्लिकेशन जिनके उपयोगकर्ता वयस्क भी हैं, प्रमाणित न किए हुए विज्ञापन SDK टूल का इस्तेमाल कर सकते हैं. ऐसे ऐप्लिकेशन में न्यूट्रल एज स्क्रीन मौजूद होनी चाहिए. साथ ही, प्रमाणित न किए हुए विज्ञापन SDK टूल का इस्तेमाल सिर्फ़ जाने-पहचाने वयस्क उपयोगकर्ताओं को विज्ञापन दिखाने के लिए किया जाना चाहिए.

इन ज़रूरी शर्तों के बारे में जानने और मंज़ूरी पा चुके विज्ञापन SDK टूल की मौजूदा सूची देखने के लिए, कृपया परिवार के लिए विज्ञापन कार्यक्रम की नीति देखें.

अगर आप AdMob का इस्तेमाल करते हैं, तो उनके उत्पादों के बारे में ज़्यादा जानने के लिए AdMob के सहायता केंद्र पर जाएं.

यह पक्का करना आपकी ज़िम्मेदारी है कि आपका ऐप्लिकेशन विज्ञापनों, इन-ऐप्लिकेशन खरीदारी और व्यावसायिक कॉन्टेंट से जुड़ी सभी ज़रूरी शर्तों को पूरा करता हो. विज्ञापन SDK टूल देने वाले (वालों) की सामग्री नीतियों और विज्ञापन देने के तौर-तरीकों के बारे में ज़्यादा जानने के लिए, उनसे संपर्क करें.

इन-ऐप खरीदारी

Google Play 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा लेने वाले ऐप्लिकेशन में इन-ऐप्लिकेशन खरीदारी के लिए फिर से मंज़ूरी देगा. इस तरीके से यह पक्का करने में मदद मिलती है कि वित्तीय रूप से ज़िम्मेदार पक्ष ही खरीदारी को मंज़ूरी दे रहे हैं, न कि बच्चे.

Avoiding a policy violation is always better than managing one, but when violations do occur, we're committed to ensuring developers understand how they can bring their app into compliance. Please let us know if you see any violations or have any questions about managing a violation.

पॉलिसी का कवरेज

आपके ऐप्लिकेशन में जो भी कॉन्टेंट दिखाया जाता है या जिससे वह जुड़ा हुआ है उस पर Google Play की नीतियां लागू होती हैं. इसमें, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को दिखाए जाने वाले विज्ञापन शामिल हैं. साथ ही, किसी भी तरह का यूज़र जनरेटेड कॉन्टेंट जिसे ऐप्लिकेशन होस्ट करता है या जिससे यह जुड़ा हुआ है उस पर भी ये नीतियां लागू होती हैं. इसके अलावा, आपके डेवलपर खाते का वह सारा कॉन्टेंट जो Google Play में सार्वजनिक रूप से दिखाया जाता है उस पर ये नीतियां लागू होती हैं. इसमें आपके डेवलपर का नाम और सूची में दिया गया डेवलपर वेबसाइट का लैंडिंग पेज भी शामिल है.

हम ऐसे किसी ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जो इस्तेमाल करने वाले लोगों को उनके डिवाइस पर दूसरे ऐप्लिकेशन इंस्टॉल करने की अनुमति देते हैं. ऐसे ऐप्लिकेशन जो इंस्टॉल किए बिना दूसरे ऐप्लिकेशन, गेम या सॉफ़्टवेयर का ऐक्सेस देते हैं उन्हें यह पक्का करना चाहिए कि वह सारा कॉन्टेंट Google Play की नीतियों का पालन करता है. साथ ही, उस पर नीति की अन्य समीक्षाएं लागू हो सकती हैं. इसमें तीसरे पक्ष की दी हुई सुविधाएं और अनुभव भी शामिल हैं.

इन नीतियों में बताई गई शर्तों का वही मतलब है जैसा डेवलपर वितरण अनुबंध (DDA) में बताया गया है. इन नीतियों और DDA का पालन करने के अलावा, आपके ऐप्लिकेशन का कॉन्टेंट, Google Play के कॉन्टेंट रेटिंग से जुड़े दिशा-निर्देश के मुताबिक रेट किया जाना चाहिए.

हो सकता है कि ऐसे ऐप्लिकेशन जो आम दर्शकों के लिए सही नहीं हैं या हमारे असली उपयोगकर्ताओं का अनुभव जिन पर खराब रहा हो उन्हें Google Play पर प्रचार करने की मंज़ूरी न दी जाए. हालांकि, ऐसे ऐप्लिकेशन तब तक Google Play पर मौजूद रहेंगे, जब तक वे इन नीतियों और DDA का पालन करेंगे.

Google, अपने विवेक से यह तय करता है कि Google Play में ऐप्लिकेशन शामिल करने हैं या हटाने हैं. हम हानिकारक व्यवहार या बुरे बर्ताव के ज़्यादा खतरे के पैटर्न सहित कई दूसरी वजहों के आधार पर कार्रवाई कर सकते हैं. हम पहले किए गए उल्लंघन की जानकारी, ऐप्लिकेशन इस्तेमाल करने वाले लोगों की शिकायत, और लोकप्रिय ब्रैंड की मदद से बुरा बर्ताव होने के खतरे की पहचान करते हैं. साथ ही, इसके लिए ऐप्लिकेशन की खास बातें और अन्य एसेट जैसी अलग-अलग चीज़ों का इस्तेमाल भी किया जाता है.

प्रवर्तन प्रक्रिया

अगर आपका ऐप्लिकेशन हमारी किसी भी नीति का उल्लंघन करता है, तो उसे Google Play से हटा दिया जाएगा और आपको हटाए जाने की प्रक्रिया की खास वजह के साथ एक ईमेल सूचना मिलेगी. इन नीतियों या डेवलपर वितरण अनुबंध (DDA) की वजह से बार-बार होने वाले या गंभीर उल्लंघनों (जैसे कि मैलवेयर, धोखाधड़ी, और उपयोगकर्ता या डिवाइस को नुकसान पहुंचाने वाले ऐप्लिकेशन) के नतीजे के बाद व्यक्तिगत या मिलते-जुलते खातों को खत्म कर दिया जाएगा.

कृपया ध्यान दें कि हो सकता है कि निकालने की प्रक्रिया या प्रशासनिक नोटिस, आपके ऐप्लिकेशन या व्यापक ऐप्लिकेशन कैटलॉग के हर नीति उल्लंघन को ना दिखाए. डेवलपर किसी भी फ़्लैग की गई नीति के मुद्दे को पता करने और उसे ठीक करने के लिए जिम्मेदार हैं और वह यह ध्यान से देख लें कि उनके ऐप्लिकेशन का बाकि बचा भाग पूरी तरह से नीति का अनुपालन करता हो. उल्लंघनों पर ध्यान न देने की वजह से नीति उल्लंघन ठीक करने के दूसरे तरीकों (एनफ़ोर्समेंट) के तहत कार्रवाई हो सकती है, जिनमें आपके ऐप्लिकेशन को हमेशा के लिए हटाया जाना या खाता बंद किया जाना भी शामिल है.

पॉलिसी संबंधी उल्लंघनों का प्रबंधन और रिपोर्टिंग

अगर किसी उपयोगकर्ता की रेटिंग/टिप्पणी या उसे हटाए जाने के बारे में आपके पास कोई सवाल या परेशानी है, तो आप नीचे दिए गए संसाधनों को देख सकते हैं या Google Play सहायता केंद्र पर जाकर हमसे संपर्क कर सकते हैं. हालांकि, हम आपको कानूनी सलाह नहीं दे सकते हैं. अगर आपको कानूनी सलाह चाहिए, तो कृपया कानूनी सलाहकार से संपर्क करें.

ऐप्लिकेशन की पुष्टि और अपील करना
नीति उल्लंघन की शिकायत करना
खाता बंद किए जाने या ऐप्लिकेशन हटाए जाने के बारे में Google Play से संपर्क करना
चेतावनी
आपत्तिजनक ऐप्लिकेशन और टिप्पणियों की शिकायत करना
मेरे ऐप्लिकेशन को Google Play से हटा दिया गया है
Google Play डेवलपर खाता बंद होने की वजह समझना

Developer Distribution Agreement