डेवलपर कार्यक्रम की नीति (12 अगस्त, 2020 से लागू)

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

आप जो नए और अनोखे ऐप्लिकेशन और गेम बनाते हैं उनसे हम और आप कामयाबी की नई ऊंचाइयां छूते हैं. हालांकि, इसके साथ नई ज़िम्मेदारियां भी आती हैं. डेवलपर कार्यक्रम की ये नीतियां और डेवलपर वितरण अनुबंध, यह पक्का करते हैं कि हम साथ मिलकर Google Play की मदद से करोड़ों लोगों तक दुनिया के सबसे अनोखे और भरोसेमंद ऐप्लिकेशन पहुंचाते रहें. नीचे दी गई हमारी नीतियों के बारे में जानें.

पाबंदी वाला कॉन्टेंट

दुनिया भर के लोग हर दिन ऐप्लिकेशन और गेम ऐक्सेस करने के लिए, Google Play का इस्तेमाल करते हैं. ऐप्लिकेशन सबमिट करने से पहले, पक्का करें कि आपका ऐप्लिकेशन Google Play के लिए सही हो और स्थानीय कानूनों का पालन करता हो.

बच्चों के लिए खतरनाक कॉन्टेंट

हम 'Play स्टोर' से ऐसे ऐप्लिकेशन तुरंत हटा देते हैं जिनमें नाबालिगों को यौन नज़रिए से दिखाने वाला कॉन्टेंट शामिल होता है-, इनमें ऐसे ऐप्लिकेशन शामिल हैं जो बच्चों के यौन शोषण या नाबालिगों के साथ गलत व्यवहार को बढ़ावा देते हैं, जैसे उन्हें गलत तरह से छूना या उनके शरीर पर गलत तरह से हाथ फिराना वगैरह.

इसके अलावा, बच्चों की पसंद वाले ऐसे ऐप्लिकेशन को अनुमति नहीं दी जाती जिनकी थीम वयस्कों के हिसाब से हो. इसमें ऐसे ऐप्लिकेशन शामिल हैं जो बहुत ज़्यादा हिंसा, खून-खराबा, और मार-काट जैसी नुकसानदायक और खतरनाक गतिविधियों को दिखाते हैं या उन्हें बढ़ावा देते हैं. हम ऐसे ऐप्लिकेशन को भी अनुमति नहीं देते जिनमें शरीर और व्यक्तित्व से जुड़ी नकारात्मक बातों को बढ़ावा दिया जाता है. इनमें मनोरंजन के मकसद से प्लास्टिक सर्जरी, वज़न घटाने, और किसी व्यक्ति के शरीर को आकर्षक दिखाने के लिए उसमें किए गए कॉस्मेटिक बदलाव को दिखाने वाले ऐप्लिकेशन शामिल हैं.

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.

आपत्तिजनक कॉन्टेंट

यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित करने और उस पर पाबंदी लगाने के मानक बनाए हैं जो हमारे ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए नुकसानदायक या गलत हो.

यौन सामग्री और धर्म का अपमान करने वाली सामग्री

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो यौन सामग्री या धर्म का अपमान करने वाली सामग्री को बढ़ावा देते हैं. इनमें पोर्नोग्राफ़ी या यौन रूप से संतुष्टि देने वाला कोई कॉन्टेंट या सेवाएं भी शामिल हैं. नग्नता वाले कॉन्टेंट 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.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- यौन नग्नता या यौन रूप से अश्लील मुद्राएं, जिसमें व्यक्ति नग्न हो, धुंधला हो या उसने कम से कम कपड़े पहने हों और/या किसी सार्वजनिक जगह के हिसाब से ऐसे कपड़े सही न हों.
- ऐनिमेशन या चित्रों में यौन गतिविधियों को दिखाना. साथ ही, अश्लील मुद्राएं या शरीर के अंगों को यौन रूप से दिखाना.
- ऐसा कॉन्टेंट जिसमें सेक्स को ज़्यादा मज़ेदार बनाने या कामुकता जगाने के बारे में बताया जाता है. साथ ही, जिसमें सेक्स गाइड, गैरकानूनी यौन थीम, और यौन गतिविधियां दिखाई गई हों.
- ऐसा कॉन्टेंट जो कामुक हो या धर्म का अपमान करता हो. इसका उदाहरण ऐप्लिकेशन के भीतर या स्टोर पेज में धर्म का अपमान करने वाली बातें, किसी व्यक्ति का अपमान करने वाली बातें, अश्लील मैसेज, वयस्क/यौन कीवर्ड शामिल होना है.
- पशुओं के साथ यौन गतिविधि दिखाने, इसके बारे में जानकारी देने या इसे बढ़ावा देने वाला कॉन्टेंट.
- ऐसे ऐप्लिकेशन जो सेक्स से जुड़े मनोरंजन, एस्कॉर्ट सेवाओं या ऐसी दूसरी सेवाओं का प्रचार करते हों जिन्हें पैसे के बदले में यौन क्रियाएं देने वाली सेवा समझा जा सकता है.
- ऐसे ऐप्लिकेशन जो लोगों को नीचा दिखाते हों या उनका अपमान करते हों.

नफ़रत फैलाने वाली भाषा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी व्यक्ति या समूह के ख़िलाफ़ 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 हिंसा को बढ़ावा देते हैं.

जिन ऐप्लिकेशन में नाज़ियों से जुड़ा ईडीएसए कॉन्टेंट (शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला) शामिल है उन्हें स्थानीय कानूनों और नियमों के हिसाब से कुछ देशों में ब्लॉक किया जा सकता है.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- ऐसा कॉन्टेंट या भाषण जो दावा करे कि कोई सुरक्षित ग्रुप अमानवीय, सामाजिक तौर पर कमतर या नफ़रत के लायक है.
- ऐसे ऐप्लिकेशन जिनमें नफ़रत फैलाने वाली टिप्पणियां, रूढ़िवादी या किसी सुरक्षित समूह के बारे में नकारात्मक बातें (जैसे कि नुकसान पहुंचाने वाला, भ्रष्ट, बुरा वगैरह) कही गई हैं. इसके अलावा, साफ़ तौर पर या किसी दूसरे तरीके से यह दावा किया गया है कि कोई 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 सुरक्षित ग्रुप के सदस्य हैं.
- ऐसा कॉन्टेंट जो नफरत फैलाने वाले प्रतीकों को बढ़ावा देता है, जैसे कि झंडे, प्रतीक, प्रतीक चिह्न या नफ़रत फैलाने वाले समूहों से जुड़ा व्यवहार.

हिंसा

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें ग़ैर-ज़रूरी हिंसा या दूसरी खतरनाक गतिविधियों को दिखाया जाता है या जो ऐसा करने को बढ़ावा देते हैं. आम तौर पर, ऐसे ऐप्लिकेशन को अनुमति दी जाती है जो किसी गेम के हिसाब से काल्पनिक हिंसा को दिखाते हैं, जैसे कि शिकार या फ़िशिंग करते हुए कार्टून.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- किसी भी व्यक्ति या पशु के ख़िलाफ़ असली दिखने वाली हिंसा या हिंसा के खतरे को ग्राफ़िक की मदद से दिखाना या उनके बारे में जानकारी देना.
- ऐसे ऐप्लिकेशन जो खुद को नुकसान पहुंचाने, खुदकुशी करने, धमकाने, उत्पीड़न 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 लोग यह समझ सकें कि किस बारे में बात हो रही है.

संवेदनशील घटनाएं

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 लेने की कोशिश करते हैं. आम तौर पर, ऐसे ऐप्लिकेशन को अनुमति दी जाती है जिनमें संवेदनशील घटना से जुड़ा ऐसा कॉन्टेंट होता है जिसे ईडीएसए (शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला) के नज़रिये से बनाया गया हो या जिसका इरादा ऐप्लिकेशन इस्तेमाल करने वाले लोगों को सतर्क करने या जागरूकता फैलाने का हो.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- आत्महत्या, दवा की ज़्यादा मात्रा, प्राकृतिक वजहों वगैरह 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 लेते दिखना जिसके पीड़ितों को कोई सीधा फ़ायदा न मिला हो.

धमकाना और उत्पीड़न करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें धमकियां देने, उत्पीड़न करने या प्रताड़ित करने जैसी बातें शामिल हों या जो ऐसी चीज़ों को बढ़ावा देते हों.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- अंतरराष्ट्रीय या धार्मिक टकरावों से पीड़ित लोगों को धमकाना.
- ऐसा कॉन्टेंट जो दूसरों का फ़ायदा उठाने की कोशिश करता है. इसमें जबरन वसूली, ब्लैकमेल करना वगैरह शामिल है.
- किसी व्यक्ति को सार्वजनिक रूप से अपमानित करने के लिए कॉन्टेंट पोस्ट करना.
- किसी दुखद घटना के पीड़ितों या उनके दोस्तों और परिवार के सदस्यों को परेशान करना.

ऐसे उत्पाद जिनसे किसी भी तरह का खतरा हो

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें विस्फोटकों, बंदूकों, गोला बारूद या बंदूकों से जुड़ी चीज़ों 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 जिन पर 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.

गांजा

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.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- इस्तेमाल करने वालों को ऐप्लिकेशन में मौजूद खरीदारी कार्ट की मदद से गांजा मंगवाने की सुविधा देना.
- लोगों को गांजे की डिलीवरी करना या पिक अप की व्यवस्था करना.
- टीएचसी (टेट्राहाइड्रोकैनाबिनॉल) वाले उत्पादों को बेचने की सुविधा देना. इनमें सीबीडी तेल जैसे उत्पाद शामिल हैं जिनमें टीएचसी होता है.

तंबाकू और शराब

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो तंबाकू (इसमें ई-सिगरेट और वेप पेन भी शामिल हैं) बेचने की सुविधा देते हैं या जो तंबाकू या शराब के गैरकानूनी और गलत इस्तेमाल को बढ़ावा देते हैं.

यहां आम तौर पर होने वाले उल्लंघनों के उदाहरण दिए गए हैं:

- शराब या तंबाकू के इस्तेमाल को दिखाना या बढ़ावा देना. इसके अलावा, 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.

वित्तीय सेवाएं

हम ऐसे ऐप्लिकेशन को अनुमति 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 और इलाके के नियमों का पालन करना होगा. उदाहरण के लिए, आपको स्थानीय कानून के मुताबिक ज़रूरी जानकारी सार्वजनिक करनी होगी.

बाइनरी ऑप्शन

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

आभासी मुद्राएं

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

निजी क़र्ज़

निजी क़र्ज़ लेने वाले लोगों को इसकी क्वालिटी, सुविधाओं, शुल्क, पैसे लौटाने के शेड्यूल, जोखिमों, और इससे होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे क़र्ज़ के बारे में सोच-समझकर फ़ैसला ले सकें. निजी क़र्ज़ लेने वालों को क़र्ज़ की क्वॉलिटी, सुविधाओं, शुल्क, जोखिमों, और उस क़र्ज़ से होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे क़र्ज़ लेने या न लेने के बारे में फ़ैसला कर सकें.

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

ऐसे ऐप्लिकेशन जो निजी क़र्ज़ देते हैं उन्हें ऐप्लिकेशन के मेटाडेटा में नीचे दी गई जानकारी देनी होगी. इनमें वे ऐप्लिकेशन शामिल हैं जो सीधे तौर पर क़र्ज़ देते हैं, लीड बनाते हैं, और ग्राहकों को तीसरे पक्ष के क़र्ज़ देने वालों से मिलाते हैं. हालांकि, यह सिर्फ़ इन ही तक सीमित नहीं 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
- ऐसी निजता नीति जिसमें ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी और संवेदनशील डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने के बारे में पूरी तरह से बताया गया हो.

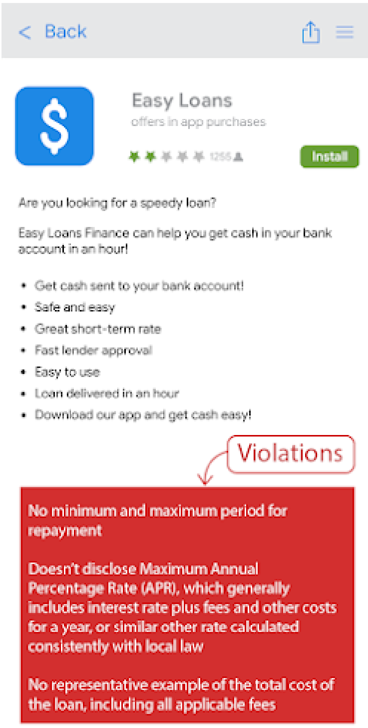
हम निजी क़र्ज़ का प्रचार करने वाले ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो क़र्ज़ की पूरी रकम लौटाने के लिए, 60 दिन या उससे कम समय की शर्त रखते हैं (इन्हें हम "कम अवधि वाले निजी क़र्ज़" कहते हैं).

ज़्यादा **APR** वाले निजी क़र्ज़

हम अमेरिका में ऐसे ऐप्लिकेशन को निजी क़र्ज़ देने की अनुमति 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.

यहां आम तौर पर होने वाले उल्लंघनों का एक उदाहरण दिया गया है:



असली पैसे दांव पर लगाकर खेले जाने वाला जुआ, गेम, और प्रतियोगिताएं

हम असली पैसे दांव पर लगाकर खेले जाने वाले जुए की सुविधा देने वाले ऐप्लिकेशन, उससे जुड़े विज्ञापनों, और रोज़ाना के फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन को तब ही अनुमति देते हैं, जब वे कुछ ज़रूरी शर्तों को पूरा करते हैं.

जुए वाले ऐप्लिकेशन

(इस समय सिर्फ़ यूके, आयरलैंड, और फ़्रांस में अनुमति दी गई है)
दूसरी सभी जगहों के लिए, हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें ऑनलाइन जुआ खेलने की सुविधा देने वाला कॉन्टेंट या सेवाएं होती हैं.

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

- Play पर अपने ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को ऐप्लिकेशन प्रोसेस सही तरीके से पूरा करनी होगी;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और उद्योग के मानकों का पालन करना चाहिए जहां उसे उपलब्ध कराया जाता है;
- डेवलपर के पास हर उस देश के लिए जुए का एक मान्य लाइसेंस होना चाहिए जहां ऐप्लिकेशन को उपलब्ध कराया जाता है;
- ऐप्लिकेशन को कम उम्र 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 पर, पैसे चुकाकर या Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करके ख़रीदे जाने वाले ऐप्लिकेशन के तौर पर मौजूद नहीं होना 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 इसकी ऐप्लिकेशन लिस्टिंग में, ज़िम्मेदारी से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

असली पैसे देकर खेले गए अन्य गेम, प्रतियोगिताएं, और टूर्नामेंट ऐप्लिकेशन

हम ऐसे कॉन्टेंट या सेवाओं को अनुमति नहीं देते जो ऐप्लिकेशन का इस्तेमाल करने वाले लोगों को दांव लगाने, हिस्सेदारी या असली पैसों के बदले में हिस्सा लेने (इसमें पैसों से ख़रीदे गए इन-ऐप्लिकेशन आइटम भी शामिल हैं) की सुविधा देते हैं, ताकि वे ऐसा पुरस्कार पा सकें जिसकी असल दुनिया में कोई कीमत होती है. इनमें ऑनलाइन कसीनो, खेलों पर सट्टा लगाना, और ऐसी लॉटरी शामिल हैं जो जुए वाले ऐप्लिकेशन के लिए ऊपर दी गई

ज़रूरी शर्तों को पूरा नहीं करती हैं. साथ ही, इनमें ऐसे गेम भी आते हैं जो नकद या असल दुनिया के दूसरे मूल्य के इनाम ऑफ़र करते हैं. हालांकि, यह इन ही तक सीमित नहीं है.

यहां उल्लंघनों के उदाहरण दिए गए हैं:

- ऐसे गेम जो कीमती चीज़ या नकद इनाम जीतने के मौके के बदले में पैसे लेते हैं
- "लॉयल्टी" पॉइंट (जैसे कि लोगों की दिलचस्पी बढ़ाना या गतिविधि) वाले ऐसे गेम (1) जिन्हें असली पैसों से किस्तों में या जल्दी से खरीदा गया है (2) जो असली दुनिया के पैसों की वस्तुओं या पुरस्कारों के लिए बदले जा सकते हैं
- ऐसे ऐप्लिकेशन जो किसी कीमती इनाम या असली पैसों के इनाम की योग्यता पाने या उसे बढ़ाने के लिए, जुआ खेलने वाले लोगों और हिस्सा लेने, जीतने या जमा करने के लिए ज़रूरी इन-ऐप्लिकेशन मुद्राओं को स्वीकार या प्रबंधित करते हैं.
- ऐसे ऐप्लिकेशन जो असली पैसों का इस्तेमाल करके, उनसे खेले जाने वाले गेम, प्रतियोगिताएं या टूर्नामेंट में दांव लगाने, हिस्सेदारी लेने या हिस्सा लेने के लिए "कॉल टू ऐक्शन" की सुविधा देते हैं. जैसे कि ऐसे नेविगेशनल एलिमेंट (मेन्यू आइटम, टैब, बटन वगैरह) जो लोगों को टूर्नामेंट में नकद इनाम जीतने का मौका देने के लिए "रजिस्टर करने" या "खेलने" के लिए न्योता भेजते हैं.

Play पर मौजूद ऐप्लिकेशन में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, प्रतियोगिताएं, और टूर्नामेंट से जुड़े विज्ञापन

जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, प्रतियोगिताएं, और टूर्नामेंट से जुड़े विज्ञापन दिखाने वाले ऐप्लिकशन को तब ही अनुमति दी जाती है, जब वे नीचे दी गई ज़रूरी शर्तों को पूरा करते हैं:

- किसी भी इलाके में विज्ञापन दिखाए जाने के लिए, ऐप्लिकेशन और विज्ञापन (इसमें विज्ञापन देने वाले लोग भी शामिल हैं) को उस इलाके के सभी लागू कानूनों और उद्योग मानकों का पालन करना चाहिए;
- विज्ञापन को जुए से जुड़े ऐसे सभी उत्पादों और सेवाओं के लाइसेंस के लिए ज़रूरी स्थानीय शर्तों को पूरा करना चाहिए जिनका प्रचार किया जा रहा हो;
- ऐप्लिकेशन में 18 साल से कम उम्र के लोगों के लिए जुए से जुड़ा कोई विज्ञापन नहीं दिखाना चाहिए:
- ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम का हिस्सा नहीं होना चाहिए;
- ऐप्लिकेशन को 18 साल से कम उम्र के लोगों को टारगेट नहीं करना चाहिए;
- अगर जुए से जुड़े ऐप्लिकेशन का प्रचार किया जा रहा है (जैसा कि ऊपर बताया गया है) ,तो विज्ञापन को अपने लैंडिंग पेज पर, विज्ञापन में दिखने वाली ऐप्लिकेशन लिस्ट में या ऐप्लिकेशन के अंदर, ज़िम्मेदारी से खेले जाने वाले जुए के बारे में साफ़ तौर पर जानकारी दिखानी चाहिए;-
- ऐप्लिकेशन में नकली जुए से जुड़ा कॉन्टेंट नहीं होना चाहिए. जैसे कि सोशल कसीनो ऐप्लिकेशन, वर्चुअल स्लॉट मशीन वाले ऐप्लिकेशन;
- ऐप्लिकेशन को जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट में मदद करने वाली सुविधाएं नहीं देनी चाहिए. जैसे कि खेलने, पैसे चुकाने, खेल के स्कोर/ऑड्स को ट्रैक करने या हिस्सा लेने के लिए दिए जाने वाले पैसों को प्रबंधित करने में मदद करने वाली सुविधा;
- ऐप्लिकेशन में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट से जुड़ी जिन सेवाओं का प्रचार किया जाता है उनमें आपको मालिकाना हक पाने की इच्छा नहीं होनी चाहिए;
- ऐप्लिकेशन के कॉन्टेंट को जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट की सेवाओं का प्रचार नहीं करना चाहिए और न ही लोगों को ऐसी सेवाएं देने वाले पेज पर ले जाना चाहिए

सिर्फ़ जुए से जुड़े ऐप्लिकेशन (जैसा कि ऊपर बताया गया है) या ऐसे ऐप्लिकेशन जो जुए से जुड़े विज्ञापनों की इन सभी ज़रूरी शर्तों को पूरा करते हैं उनमें असली पैसों को देकर खेले जाने वाले जुए के अलावा, असली पैसे देकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट का प्रचार करने वाले विज्ञापन शामिल हो सकते हैं.

यहां उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसा ऐप्लिकेशन जो कम उम्र के लोगों के लिए डिज़ाइन किया गया है और उसमें जुए की सेवाओं का प्रचार करने वाला विज्ञापन दिखाया जाता है
- ऐसा नकली कसीनो गेम जो असली पैसे देकर खेले जाने वाले कसीनो का प्रचार करता है या लोगों को इस तरह के पेज पर ले जाता है
- खेल के ऑड्स को ट्रैक करने वाला ऐसा ऐप्लिकेशन जिसमें जुए से जुड़े ऐसे विज्ञापन दिखाए जाते हैं जो बेटिंग साइट पर ले जाते हैं
- जुए से जुड़ी सेवा के विज्ञापन दिखाने वाला ऐसा समाचार ऐप्लिकेशन जिसका मालिक या चलाने वाला व्यक्ति खुद ऐप्लिकेशन का डेवलपर है
- जिन ऐप्लिकेशन में जुए से जुड़े ऐसे विज्ञापन दिखाए जाते हैं जो धोखाधड़ी वाले विज्ञापन की हमारी नीति का उल्लंघन करते हैं. उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को बटन, आइकॉन या ऐप्लिकेशन के दूसरे इंटरैक्टिव एलिमेंट के तौर पर दिखाए जाने वाले विज्ञापन

रोज़ाना के फ़ैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन

हम रोज़ाना के फ़ैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन को अनुमति तब ही देते हैं, जब वे स्थानीय कानूनों के मुताबिक नीचे दी गई ज़रूरी शर्तों को पूरा करते हैं:

- ऐप्लिकेशन या तो 1)-सिर्फ़ अमेरिका में उपलब्ध कराया जाता हो या 2) उसे जुए से जुड़े ऐप्लिकेशन की ऊपर बताई गई ज़रूरी शर्तों के तहत मंज़ूरी दी जाए;
- Play पर ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को DFS ऐप्लिकेशन प्रोसेस सही तरीके से पूरी करनी होगी;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और उद्योग मानकों का पालन करना होगा जहां उसे उपलब्ध किया जाता है;
- ऐप्लिकेशन को कम उम्र के लोगों को ऐप्लिकेशन में जुआ खेलने या पैसों का लेन-देन करने से रोकना चाहिए;
- ऐप्लिकेशन को Google Play पर, पैसे चुकाकर या Google Play इन-ऐप्लिकेशन बिलिंग का इस्तेमाल करके खरीदे जाने वाले ऐप्लिकेशन के तौर पर मौजूद नहीं होना 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 इसकी ऐप्लिकेशन लिस्टिंग में, ज़िम्मेदारी से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

अगर ऐप्लिकेशन को अमेरिका में उपलब्ध कराया जाता है, तो नीचे दी गई अन्य ज़रूरी शर्तों का पालन करना होगा;

- ऐप्लिकेशन को अमेरिका के हर उस राज्य या इलाके में लागू सभी कानूनों और उद्योग मानकों का पालन करना होगा जहां उसे उपलब्ध कराया जाता है;
- डेवलपर के पास अमेरिका के हर उस राज्य या इलाके के लिए मान्य लाइसेंस होना चाहिए जहां रोज़ाना के फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन के लिए लाइसेंस की ज़रूरत होती है;
- ऐप्लिकेशन के इस्तेमाल को अमेरिका के उन राज्यों या इलाकों में रोक देना चाहिए जहां डेवलपर के पास रोज़ाना के फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन के लिए ज़रूरी लाइसेंस नहीं है; और
- ऐप्लिकेशन के इस्तेमाल को अमेरिका के उन राज्यों और इलाकों में रोक देना चाहिए जहां रोज़ाना के फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन गैरकानूनी है.

गैरकानूनी गतिविधियां

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो गैरकानूनी गतिविधियों की सुविधा देते हैं या उनका प्रचार करते हैं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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 (यूजीसी)

यूज़र जनरेटेड कॉन्टेंट (यूजीसी) ऐसा कॉन्टेंट है जिसे लोग किसी ऐप्लिकेशन में जोड़ते हैं. साथ ही, जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों के कम से कम एक समूह को दिखता है या वे उसे ऐक्सेस कर सकते हैं.

ऐसे ऐप्लिकेशन जिनमें यूजीसी (लोगों का बनाया कॉन्टेंट) होता है या जो इसकी सुविधा देते हैं उनके लिए ज़रूरी है कि:

- ऐप्लिकेशन इस्तेमाल करने वाले लोग यूजीसी (लोगों का बनाया कॉन्टेंट) बनाने या अपलोड करने से पहले ऐप्लिकेशन को इस्तेमाल करने की शर्तों और/या उपयोगकर्ता नीति को स्वीकार करें;
- आपत्तिजनक कॉन्टेंट और व्यवहार को तय करें (Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक) और ऐप्लिकेशन के इस्तेमाल की शर्तों और उपयोगकर्ता नीतियों के तहत उन पर पाबंदी लगाई जाए;
- बेहतरीन, असरदार, और लगातार होने वाला यूजीसी (लोगों का बनाया कॉन्टेंट) मॉडरेशन लागू किया जाए. ऐप्लिकेशन पर होस्ट किया गया इस तरह का यूजीसी (लोगों का बनाया कॉन्टेंट) उचित और अनुकूल होता है
  - लाइव स्ट्रीमिंग ऐप्लिकेशन के मामले में, आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) को रीयल-टाइम में जितना जल्दी हो सके उतना जल्दी हटा देना चाहिए;
  - ऑगमेंटेड रिएलिटी ऐप्लिकेशन के मामले में, यूजीसी (लोगों का बनाया कॉन्टेंट) मॉडरेशन (जिसमें इन-ऐप्लिकेशन रिपोर्टिंग सिस्टम शामिल है) को, आपत्तिजनक एआर यूजीसी (उदाहरण के लिए, अश्लील यौन एआर इमेज) और संवेदनशील एआर एंकरिंग की जगह दोनों के लिए ज़िम्मेदार होना चाहिए. उदाहरण के लिए, संवेदनशील एआर एंकर का पाबंदी वाला क्षेत्र, जैसे कि सेना का बेस या निजी संपत्ति जहां एआर एंकरिंग से प्रॉपर्टी के मालिक को समस्या हो सकती है;
- ऐसा इन-ऐप्लिकेशन सिस्टम उपलब्ध कराया जाए जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए आसान हो. साथ ही, यूजीसी (लोगों का बनाया कॉन्टेंट) सही न होने पर इस सिस्टम की मदद से, ऐप्लिकेशन इस्तेमाल करने वाले लोग इसकी शिकायत कर सकें और कोई कार्रवाई कर सकें;
- ऐप्लिकेशन इस्तेमाल करने वाले उन लोगों को हटाया या ब्लॉक किया जाए जो बुरा बर्ताव करते हैं और ऐप्लिकेशन के इस्तेमाल की शर्तों और/या उपयोगकर्ता नीति का उल्लंघन करते हैं;
- 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, उन ऐप्लिकेशन को भी Google Play से हटा दिया जाएगा जो मुख्य रूप से आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) होस्ट करने के लिए इस्तेमाल किए जाते हैं या ऐप्लिकेशन इस्तेमाल करने वाले लोगों के बीच आपत्तिजनक यूजीसी (लोगों का बनाया कॉन्टेंट) दिखाने वाले ऐप्लिकेशन की छवि बनाते हैं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- यौन रूप से अश्लीलता फैलाने वाले ऐसे यूज़र जनरेटेड कॉन्टेंट को बढ़ावा देना जिसमें मुख्य रूप से पैसे लेकर आपत्तिजनक कॉन्टेंट को बढ़ावा या अनुमति देने वाली सुविधाएं शामिल हैं.
- यूज़र जनरेटेड कॉन्टेंट (यूजीसी) वाले ऐसे ऐप्लिकेशन जिनमें डराने, उत्पीड़न करने या धमकियां देने 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 ऐप्लिकेशन इस्तेमाल करने वाले लोगों की शिकायतों को हल करने में लगातार नाकामयाब होते हैं.

ऐसी चीज़ें जिन्हें बिक्री या प्रचार की अनुमति नहीं मिली है

Google Play कानूनी दावे के बावजूद भी, ऐसे ऐप्लिकेशन को अनुमति नहीं देता जो ऐसी चीज़ों की बिक्री या प्रचार करते हैं जिनकी अनुमति नहीं है. उदाहरण:

- पाबंदी वाली दवाओं और सप्लीमेंट की ऐसी सूची के सभी आइटम जिसमें पूरी जानकारी नहीं है.
- 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 ख़ास 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 बिना मंज़ूरी वाली या गुमराह करने वाली जिन दवाओं और सप्लीमेंट पर नज़र रखते हैं उनके बारे में ज़्यादा जानकारी के लिए, कृपया www.legitscript.com पर जाएं.

बौद्धिक संपत्ति

जब डेवलपर किसी और के काम की नकल करते हैं या बिना किसी ज़रूरी अनुमति के उसका इस्तेमाल करते हैं, तो इससे उस काम के मालिक को नुकसान पहुंच सकता है. दूसरे लोगों के काम का इस तरह से इस्तेमाल न करें कि वह गलत हो.

बौद्धिक संपत्ति

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते जो दूसरे लोगों के बौद्धिक संपत्ति के अधिकारों का उल्लंघन करते हैं. इनमें ट्रेडमार्क, कॉपीराइट, पेटेंट, कारोबार से जुड़ी गोपनीय जानकारी, और अन्य 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 डीएमसीए (DMCA) अनुरोध दर्ज करने के लिए, हमारी कॉपीराइट से जुड़ी प्रक्रियाओं वाले पेज पर जाएं.

किसी ऐप्लिकेशन में हो रही नकली उत्पादों की बिक्री या 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 हमारा सुझाव है कि अपनी समस्या हल करने के लिए सीधे डेवलपर से संपर्क करें. अगर आपकी समस्या फिर भी हल नहीं होती है, तो कृपया इस फ़ॉर्म को भरकर ट्रेडमार्क के बारे में शिकायत दर्ज करें.

अगर आपके पास यह बताने वाला दस्तावेज़ है कि आपके पास अपने ऐप्लिकेशन या स्टोर पेज में किसी तीसरे पक्ष की बौद्धिक संपत्ति (जैसे कि ब्रांड का नाम, लोगो, और ग्राफ़िक रचना) का इस्तेमाल करने की अनुमति है, तो आप सबमिट करने से पहले ही Google Play की 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 अनुमति के इस्तेमाल करना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते 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 के बारे में बता 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.

यहां कॉपीराइट किए गए ऐसे कॉन्टेंट के कुछ उदाहरण दिए गए हैं जिसका इस्तेमाल आम तौर पर अनुमति के बिना या कानूनी रूप से मान्य वजह के बिना किया जाता है:

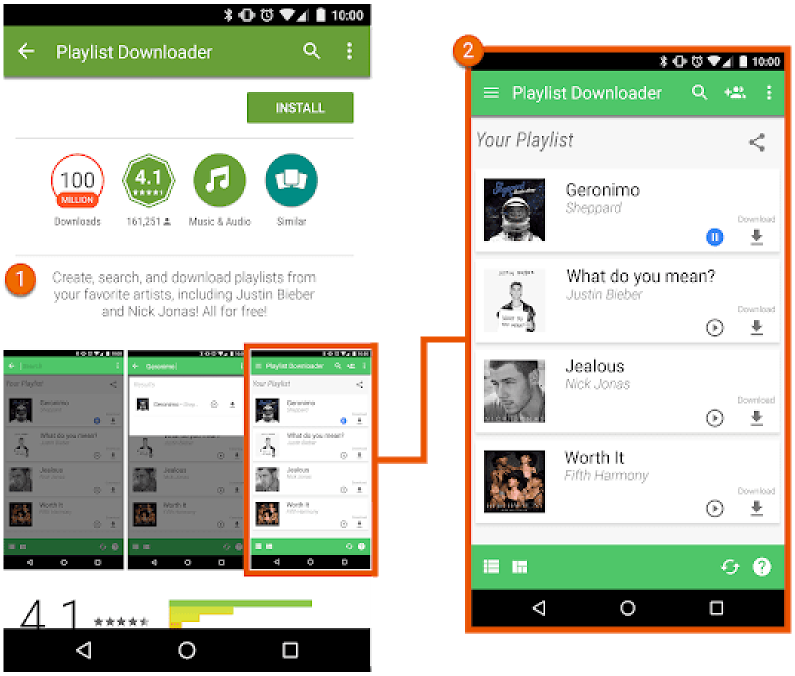
- म्यूज़िक एल्बम, वीडियो गेम, और किताबों के लिए कवर आर्ट.
- फ़िल्मों, टेलीविज़न या वीडियो गेम की मार्केटिंग इमेज.
- कॉमिक बुक, कार्टून, फ़िल्मों, संगीत वीडियो या टेलीविज़न के आर्टवर्क या इमेज.
- कॉलेज और पेशेवर खेल टीम के लोगो.
- किसी लोकप्रिय हस्ती के सोशल मीडिया खाते से ली गई फ़ोटो.
- लोकप्रिय हस्तियों 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 पूरा रिप्रोडक्शन या अनुवाद जो सार्वजनिक डोमेन में मौजूद नहीं है.

कॉपीराइट के उल्लंघन को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो कॉपीराइट के उल्लंघन को बढ़ावा देते हैं या उसके लिए उकसाते हैं. अपना ऐप्लिकेशन प्रकाशित करने से पहले, पता लगाएं कि आपका ऐप्लिकेशन कॉपीराइट उल्लंघन को बढ़ावा तो नहीं दे रहा. साथ ही, अगर ज़रूरी हो, तो कानूनी सलाह लें.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

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



① इस ऐप्लिकेशन लिस्टिंग में दी गई जानकारी, लोगों को कॉपीराइट वाले कॉन्टेंट को बिना अनुमति के डाउनलोड करने के लिए बढ़ावा देती है.
② इस ऐप्लिकेशन लिस्टिंग में दिया गया स्क्रीनशॉट, लोगों 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 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 अपने ऐप्लिकेशन के लिए किसी दूसरे पक्ष के ट्रेडमार्क का इस्तेमाल इस तरीके से करते हैं जिससे भ्रम की स्थिति पैदा हो सकती है, तो आपका ऐप्लिकेशन निलंबित किया जा सकता है.

नकली सामान बेचना या उसे बढ़ावा देना

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो नकली सामान की बिक्री 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 सुविधाओं) की नकल करके खुद को ब्रैंड मालिक के असली उत्पाद की तरह पेश करते हैं.

निजता, धोखाधड़ी, और डिवाइस का गलत इस्तेमाल

हम ऐप्लिकेशन इस्तेमाल करने वाले लोगों की निजता की सुरक्षा करने और उन्हें पूरी तरह सुरक्षित माहौल देने का वादा करते हैं. ऐसे ऐप्लिकेशन पर सख्त पाबंदी है जो धोखाधड़ी करते हैं, नुकसान पहुंचाते हैं या जिनका इरादा किसी नेटवर्क, डिवाइस या निजी डेटा से छेड़छाड़ करना या उसका गलत इस्तेमाल करना है.

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का डेटा

आप ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को कैसे प्रबंधित करते हैं, इस बारे में आपको साफ़ तौर पर जानकारी देनी चाहिए. इसमें ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति 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 ज़रूरी शर्तें, निजता और डेटा सुरक्षा के लागू कानूनों में बताई गई ज़रूरी शर्तों के अलावा 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 की जानकारी, मैसेज (एसएमएस) और फ़ोन से जुड़ा 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 इन बातों का ध्यान रखना चाहिए:

- ऐप्लिकेशन से मिले निजी और संवेदनशील डेटा के ऐक्सेस, संग्रह, इस्तेमाल, और इसे शेयर करने को उन मकसदों तक सीमित करना जो ऐप्लिकेशन की सुविधाएं देने और उन्हें बेहतर बनाने के लिए सीधे तौर पर जुड़े हैं. उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की उम्मीद के मुताबिक काम करने का तरीका, जिसे दस्तावेज़ में बताया गया है और 'Play स्टोर' में ऐप्लिकेशन की जानकारी में जिसका प्रचार किया गया है. विज्ञापन दिखाने के लिए इस डेटा का इस्तेमाल करने वाले ऐप्लिकेशन को हमारी विज्ञापन नीति का पालन करना होगा.
- Play Console 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.

खास जानकारी देने और सहमति की ज़रूरत

उन मामलों में जहां हो सकता है कि ऐप्लिकेशन इस्तेमाल करने वाले लोगों को इस बात की उम्मीद न हो 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, जैसे कि डेटा संग्रह आपके ऐप्लिकेशन के बैकग्राउंड में होता है. इसके अलावा, आपको नीचे बताई गई ज़रूरी शर्तों को भी पूरा करना होगा:

आपको डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, 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;
- इसमें ऐक्सेस या इकट्ठा किए जा रहे डेटा के बारे में बताया जाना चाहिए;
- में 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
- इसको ऐसी दूसरी जानकारी में शामिल नहीं किया जा सकता जो निजी या संवेदनशील डेटा इकट्ठा करने से जुड़ी नहीं है.

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 मौजूद 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 लेने के लिए ऐप्लिकेशन का अनुरोध:

- सहमति संवाद साफ़ और सही 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 सहमति नहीं समझा जाना चाहिए. इसमें टैप करके बाहर जाने या वापस जाने के लिए बैक या होम बटन दबाना शामिल है; और
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति लेने के लिए, अपने-आप खारिज या खत्म होने वाले मैसेज का इस्तेमाल नहीं किया जाना चाहिए.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति के इंस्टॉल किए गए ऐप्लिकेशन की इन्वेंट्री ऐक्सेस करता है और इस डेटा को ऊपर बताई गई निजता नीति, डेटा प्रबंधन, और खास तौर पर सहमति से जानकारी देने की ज़रूरी शर्तों के तहत आने वाले निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति के फ़ोन या संपर्क सूची के डेटा को ऐक्सेस करता है और इस डेटा को ऊपर बताई गई निजता नीति, डेटा प्रबंधन, और खास तौर पर सहमति से जानकारी देने की ज़रूरी शर्तों के तहत आने वाले निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की स्क्रीन रिकॉर्ड करता है और इस नीति के मुताबिक डेटा को निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन जो डिवाइस की जगह की जानकारी इकट्ठा करता है और इसके इस्तेमाल के बारे में पूरी जानकारी नहीं देता है. साथ ही, ऊपर बताई गई ज़रूरी शर्तों के मुताबिक इस पर सहमति भी नहीं लेता है
- ऐसा ऐप्लिकेशन जो ट्रैकिंग, रिसर्च या मार्केटिंग के मकसद से ऐप्लिकेशन के बैकग्राउंड में पाबंदी वाली अनुमतियों को इकट्ठा करता है और पूरी तरह से इसके इस्तेमाल की जानकारी नहीं देता है. साथ ही, ऊपर दी गई ज़रूरी शर्तों के मुताबिक सहमति लेता है.

संवेदनशील डेटा के ऐक्सेस पर ख़ास पाबंदियां

ऊपर दी गई शर्तों के अलावा, नीचे दिए गए टेबल में ख़ास गतिविधियों के लिए ज़रूरी शर्तों के बारे में बताया गया है.

गतिविधि	ज़रूरी शर्त
आपका ऐप्लिकेशन वित्तीय या पैसे चुकाने के बारे में जानकारी या सरकारी पहचान की संख्याओं का प्रबंधन करता है	आपके ऐप्लिकेशन को 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 ज़ाहिर 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 जिसमें ऐप्लिकेशन में दी गई किसी जानकारी के साथ यह भी बताया जाए कि आपका ऐप्लिकेशन, इस्तेमाल करने वाले व्यक्ति का कौनसा डेटा इकट्ठा करता है और दूसरों तक पहुंचाता है. साथ ही, नीति में यह भी बताया जाए कि उस डेटा का इस्तेमाल किस तरह से किया जाता है. इसके अलावा, निजता नीति में उन समूहों की जानकारी भी शामिल होनी चाहिए जिनके साथ डेटा शेयर किया जाता है.

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

Privacy Shield

अगर आप Google की दी हुई ऐसी निजी जानकारी को ऐक्सेस, 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:

- लागू होने वाले सभी निजता, डेटा सुरक्षा, और डेटा संरक्षण कानूनों, निर्देशों, विनियमों, और नियमों का पालन करना;
- ईयू (यूरोपीय संघ) की निजी जानकारी को सिर्फ़ ऐसे मकसद से ऐक्सेस, इस्तेमाल 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 बिना अनुमति के या गैरकानूनी तरीके से ऐक्सेस करने, जानकारी देने, बदलाव करने, और खत्म होने से बचाने के लिए, संगठन और तकनीकी स्तर पर सही कदम लागू करना; और
- उसी स्तर की सुरक्षा मुहैया कराना जैसी Privacy Shield के सिद्धांतों के मुताबिक ज़रूरी है.

आपको समय-समय पर देखना चाहिए कि इन शर्तों का पालन ठीक तरीके से हो रहा है या नहीं. अगर आप किसी भी समय 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 भेज कर तुरंत बताना चाहिए. साथ ही, आपको ईयू (यूरोपीय संघ) की निजी जानकारी से जुड़े काम तुरंत रोक देने चाहिए या सुरक्षा के स्तर को पहले जैसा बनाए रखने के लिए ज़रूरी कदम उठाने चाहिए.

अनुमतियां

उन ही अनुमतियों का अनुरोध करना चाहिए जो इस्तेमाल करने वाले लोगों के लिए काम की हों. 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 ऐक्सेस किया गया निजी या संवेदनशील डेटा कभी भी बेचा नहीं जा सकता.

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

पाबंदी वाली अनुमतियां

ऊपर बताई गई अनुमतियों के अलावा, पाबंदी वाली अनुमतियां वे होती हैं जिन्हें हमारे डेवलपर दस्तावेज़ में, खतरनाक, विशेष या हस्ताक्षर 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 की मदद से, ऐक्सेस किए जाने वाले उपयोगकर्ता या डिवाइस के संवेदनशील डेटा को तीसरे पक्ष को ट्रांसफ़र तब ही किया जा सकता है, जब यह उस ऐप्लिकेशन की 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 दिए गए अपवादों का आकलन, ऐप्लिकेशन इस्तेमाल करने वाले लोगों की निजता या सुरक्षा पर पड़ने वाले असर के मुताबिक 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 व्यक्ति का संवेदनशील और निजी डेटा माना जाता है:

पाबंदी वाली अनुमति	ज़रूरी शर्त
अगर आपका ऐप्लिकेशन मेनिफ़ेस्ट कॉल लॉग की अनुमति समूह का अनुरोध करता है (जैसे कि **READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)**, तो	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमए) या Assistant हैंडलर के रूप में चालू तौर पर रजिस्टर किया जाना चाहिए.
अगर आपका ऐप्लिकेशन मेनिफ़ेस्ट मैसेज (एसएमएस) अनुमति समूह का अनुरोध करता है (जैसे कि **READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)**, तो	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमए) या सहायक हैंडलर के रूप में चालू तौर पर 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, उपयोगकर्ताओं 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 स्वीकार की हुई मुख्य सुविधाएं देने के लिए अनुमति (और अनुमति से मिलने वाले किसी भी डेटा) का इस्तेमाल कर सकते हैं. मुख्य सुविधा, किसी ऐप्लिकेशन का मुख्य मकसद होती हैं. इसमें ऐसी 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 के बिना, ऐप्लिकेशन "अधूरा" रहता है या किसी काम का नहीं रहता. इस डेटा का ट्रांसफ़र, शेयर या लाइसेंस के ज़रिए इस्तेमाल, सिर्फ़ ऐप्लिकेशन के अंदर मुख्य सुविधाओं या सेवाओं को देने के लिए होना चाहिए. इसका इस्तेमाल किसी और मकसद (जैसे कि दूसरे ऐप्लिकेशन या सेवाओं को बेहतर बनाने, विज्ञापन या मार्केटिंग) के लिए नहीं किया जा सकता है. कॉल लॉग या मैसेज (एसएमएस) से जुड़ी अनुमति से मिलने वाले डेटा के लिए, आप दूसरे तरीकों का इस्तेमाल नहीं कर सकते हैं. इन तरीकों में दूसरी अनुमतियां, एपीआई या तीसरे-पक्ष के स्रोत शामिल हैं.

जगह की जानकारी की अनुमतियां

डिवाइस की जगह की जानकारी को निजी और संवेदनशील जानकारी नीति और नीचे दी गई ज़रूरी शर्तों के तहत, इस्तेमाल करने वाले का निजी और संवेदनशील डेटा माना जाता है:

- ऐप्लिकेशन, जगह की जानकारी की अनुमति की मदद से सुरक्षित डेटा को ऐक्सेस तब नहीं कर सकते (उदाहरण के लिए, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION), जब मौजूदा सुविधाओं या सेवाओं को डिलीवर करने के लिए इसकी ज़रूरत न हो.
- सिर्फ़ विज्ञापन दिखाने या आंकड़े पाने के लिए, आपको कभी भी ऐप्लिकेशन इस्तेमाल करने वाले लोगों से, जगह की जानकारी इस्तेमाल करने की अनुमति का अनुरोध नहीं करना चाहिए. विज्ञापन दिखाने के लिए, इस डेटा के इस्तेमाल की अनुमति देने वाले ऐप्लिकेशन को हमारी विज्ञापन नीति का पालन करना होगा.
- ऐप्लिकेशन को मौजूदा सुविधा या सेवा देने के लिए उतने ही दायरे का अनुरोध करना चाहिए जो ज़रूरी है. उदाहरण के लिए, अच्छे की बजाय ठीक और बैकग्राउंड की बजाय फ़ोरग्राउंड. साथ ही, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को यह उम्मीद करनी चाहिए कि सुविधा या सेवा को जगह की उतनी जानकारी की ज़रूरत है जितनी के लिए 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.

फ़ोरग्राउंड 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 वाले व्यक्ति की शुरू की गई कार्रवाई पूरी होने के तुरंत बाद, इसे 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.

सभी फ़ाइलों को ऐक्सेस करने की अनुमति

ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति के डिवाइस पर मौजूद फ़ाइलें और डायरेक्ट्री की विशेषताएं, निजी और संवेदनशील डेटा नीति और नीचे दी गई ज़रूरी शर्तों के तहत ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की निजी और संवेदनशील जानकारी मानी जाती है:

- ऐप्लिकेशन को डिवाइस की सिर्फ़ उस मेमोरी के ऐक्सेस का अनुरोध करना चाहिए जो ऐप्लिकेशन के काम करने के लिए ज़रूरी है. साथ ही, ऐप्लिकेशन को किसी तीसरे पक्ष के लिए डिवाइस की उस मेमोरी के ऐक्सेस का अनुरोध नहीं करना चाहिए जो लोगों के इस्तेमाल किए जाने वाली सुविधाओं से जुड़ी नहीं है.
- जो Android डिवाइस, R (Android 11, एपीआई लेवल 30) या उसके आगे के वर्शन पर काम कर रहे हैं उन्हें डिवाइस की शेयर की गई मेमोरी का ऐक्सेस प्रबंधित करने के लिए, MANAGE_EXTERNAL_STORAGE की अनुमति की ज़रूरत होगी. वे सभी ऐप्लिकेशन जो R वर्शन को टारगेट करते हैं और डिवाइस की शेयर की गई मेमोरी ("सभी फ़ाइलों का ऐक्सेस") के लिए ऐक्सेस का दायरा बढ़ाने का अनुरोध करते हैं उन्हें प्रकाशित किए जाने से पहले एक समीक्षा होगी उनके लिए ज़रूरी है कि वे इस समीक्षा में फ़ैसला लें कि उन्हें इस ऐक्सेस की सच में ज़रूरत है या नहीं. ऐसे ऐप्लिकेशन जो इस अनुमति का इस्तेमाल करते हैं उन्हें "खास ऐप्लिकेशन के ऐक्सेस" की सेटिंग में अपने ऐप्लिकेशन के "सभी फ़ाइलों के ऐक्सेस" को चालू करने के लिए उपयोगकर्ता को साफ़ तौर पर जानकारी देनी चाहिए. R वर्शन की शर्तों के बारे में ज़्यादा जानकारी के लिए, इस सहायता लेख को पढ़ें.

डिवाइस और नेटवर्क का गलत इस्तेमाल

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो उपयोगकर्ता के डिवाइस, किसी दूसरे डिवाइस या कंप्यूटर, सर्वर, नेटवर्क, ऐप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई) या सेवाओं में दखल देते हैं. इसके अलावा, 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 ही तक सीमित नहीं है.

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

Google Play से इंस्टॉल होने वाले ऐप्लिकेशन में फ़ेरबदल करने, अपडेट करने या ऐप्लिकेशन बदलने के लिए, सिर्फ़ Google Play के अपडेट का तरीका इस्तेमाल किया जा सकता है. किसी और तरीके से शायद आप ऐसा न कर पाएं. इसी तरह, कोई ऐप्लिकेशन Google Play के अलावा किसी दूसरे स्रोत से एक्ज़ीक्यूटेबल कोड (उदा. dex, JAR, .so फ़ाइलें) डाउनलोड नहीं कर सकता. यह पाबंदी ऐसे कोड पर लागू नहीं होती जो किसी वर्चुअल मशीन पर काम करता है और जिसके पास Android एपीआई का सीमित ऐक्सेस होता है. जैसे कि वेबव्यू या ब्राउज़र में JavaScript.

हम ऐसे कोड को अनुमति नहीं देते जो सुरक्षा में जोखिम की संभावना पैदा करते हैं या उनका फ़ायदा लेते हैं. डेवलपर के लिए हाल ही में फ़्लैग की गई सुरक्षा की समस्याओं के बारे में जानने के लिए, ऐप्लिकेशन की सुरक्षा को बेहतर बनाने वाला प्रोग्राम देखें.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने पर दूसरे ऐप्लिकेशन को ब्लॉक कर देते हैं या फिर उनमें रुकावट डालते हैं.
- गेम में धोखाधड़ी करने वाले ऐप्लिकेशन जो दूसरे ऐप्लिकेशन के गेमप्ले पर असर डालते हैं.
- ऐसे ऐप्लिकेशन जो सेवाओं, सॉफ़्टवेयर या हार्डवेयर को हैक करने का तरीका बताते हैं या उसकी सुविधा देते हैं. साथ ही, सुरक्षा उपायों को खराब करने में भी मदद करते हैं.
- ऐसे ऐप्लिकेशन जो किसी सेवा या एपीआई का इस्तेमाल या ऐक्सेस इस तरह करते हैं जिससे उसकी सेवा की शर्तों का उल्लंघन होता है.
- ऐसे ऐप्लिकेशन जिन्हें वाइट लिस्ट करने की मंज़ूरी नहीं हैं और जो सिस्टम पावर प्रबंधन को अनदेखा करने की कोशिश करते हैं.
- ऐसे ऐप्लिकेशन जो तीसरे पक्ष को प्रॉक्सी सेवा देते हैं, वे ऐसा सिर्फ़ उन ऐप्लिकेशन में कर सकते हैं जिनका मुख्य मकसद ही प्रॉक्सी सेवा देना है.
- ऐप्लिकेशन या तीसरे पक्ष के कोड (जैसे कि SDK टूल) जो Google Play के अलावा, किसी दूसरे स्रोत से इस्तेमाल किया जा सकने वाला कोड डाउनलोड करते हैं. इस तरह के कोड में dex फ़ाइलें और स्थानीय कोड शामिल हैं.
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना दूसरे ऐप्लिकेशन को डिवाइस में इंस्टॉल करते हैं.
- ऐसे ऐप्लिकेशन जो नुकसान पहुंचाने वाले सॉफ़्टवेयर से जुड़े होते हैं या लोगों तक उन्हें पहुंचाने या इंस्टॉल करने की सुविधा देते हैं.

धोखाधड़ी वाला व्यवहार

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों के साथ धोखाधड़ी करने की कोशिश करते हैं या बेईमानी करते हैं. इनमें वे ऐप्लिकेशन भी शामिल हैं जो ऐसी सुविधाएं देने का दावा करते हैं जिन्हें पूरा नहीं किया जा सकता. ऐप्लिकेशन के लिए ज़रूरी है कि वे पूरे मेटाडेटा में अपनी सुविधाओं के बारे में सही जानकारी, विवरण, और फ़ोटो/वीडियो दें. ऐप्लिकेशन को ऑपरेटिंग सिस्टम या दूसरे ऐप्लिकेशन की सुविधाओं या चेतावनियों की नकल करने की कोशिश नहीं करनी चाहिए. डिवाइस की सेटिंग में किए जाने वाले किसी भी तरह के बदलाव, डिवाइस इस्तेमाल करने वाले व्यक्ति की जानकारी और सहमति से किए जाने चाहिए. ये बदलाव ऐसे हों जिन्हें उपयोगकर्ता पहले जैसा कर सके.

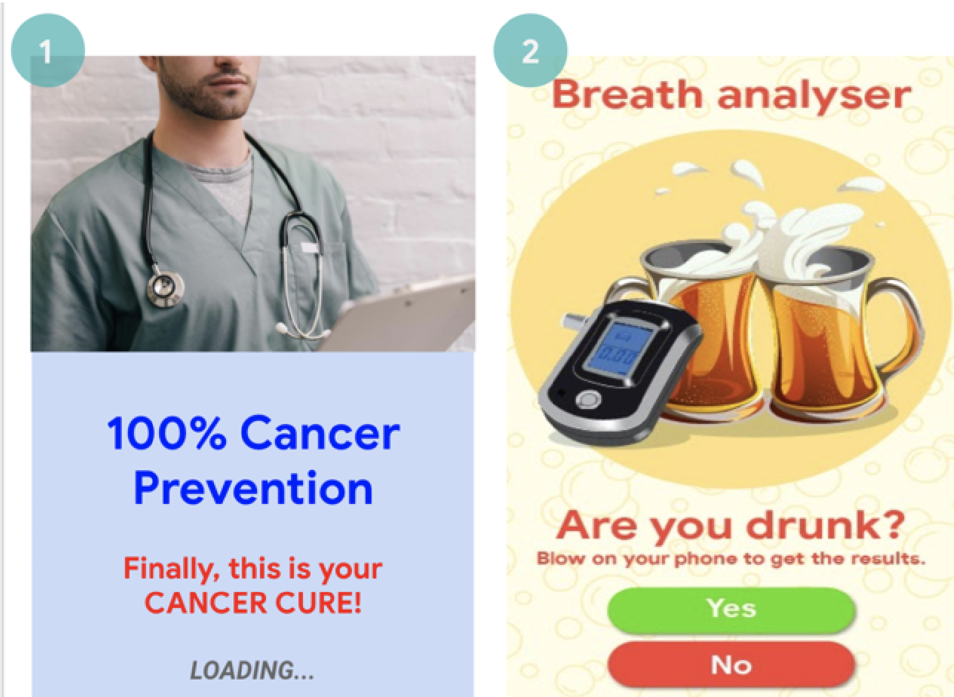
गुमराह करने वाले दावे

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें झूठी या गुमराह करने वाली जानकारी या दावे शामिल होते हैं. इस जानकारी में, विवरण, शीर्षक, आइकॉन, और स्क्रीनशॉट शामिल हैं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो अपनी सुविधाओं को गलत तरीके से पेश करते हैं या सही 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").
- ऐसे ऐप्लिकेशन जिनमें दवाई या स्वास्थ्य से जुड़ा ऐसा कॉन्टेंट शामिल है जो गुमराह कर सकता है या संभावित रूप से नुकसान पहुंचा सकता है.
- ऐसे ऐप्लिकेशन जो ऐसी सुविधाएं देने का दावा करते हैं जो दी नहीं जा सकती, जैसे कि कीड़े भगाने वाले ऐप्लिकेशन. भले ही, इसे शरारत, नकली, मज़ाक़ वगैरह के रूप में पेश किया जाए.
- ऐसे ऐप्लिकेशन जिन्हें गलत तरह के ऐप्लिकेशन के साथ रखा गया हो जिनमें ऐप्लिकेशन की रेटिंग या ऐप्लिकेशन की कैटगरी शामिल है. हालांकि, यह इन ही तक सीमित नहीं है.
- गुमराह करने वाला ऐसा कॉन्टेंट जिसका इस्तेमाल मतदान की प्रक्रिया में दखल देने के लिए हो सकता है.
- ऐसे ऐप्लिकेशन जो सरकार की किसी इकाई से जुड़े होने का झूठा दावा करते हैं या ऐसी सरकारी सेवाएं देने का दावा करते हैं जिनकी उन्हें अनुमति नहीं है.
- ऐसे ऐप्लिकेशन जो पहले से मौजूद किसी जानी-मानी इकाई का आधिकारिक ऐप्लिकेशन होने का झूठा दावा करते हैं. ज़रूरी अनुमतियों या अधिकारों के बिना "जस्टिन बीबर ऑफ़िशियल" जैसे शीर्षकों का इस्तेमाल करने की अनुमति नहीं है.



(1) यह ऐप्लिकेशन, दवाई और स्वास्थ्य से जुड़ी गुमराह करने वाली सुविधाएं (कैंसर का इलाज) देने का दावा करता है
(2) यह ऐप्लिकेशन ऐसी सुविधाएं देने का दावा करता है जो दी नहीं जा सकती (अपने फ़ोन को सांस जांचने वाले डिवाइस के रूप में इस्तेमाल करना)

डिवाइस की सेटिंग में गुमराह करने वाले बदलाव

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो इस्तेमाल करने वाले व्यक्ति की जानकारी और सहमति के बिना, उनके डिवाइस की सेटिंग या सुविधाओं में बदलाव करते 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:

- ऐसे 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.
- ऐसे 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.
- ऐसे 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.
- ऐसे ऐप्लिकेशन जो लोगों को तीसरे पक्ष के ऐप्लिकेशन हटाने या बंद करने या डिवाइस की सेटिंग और सुविधाओं में बदलाव करने को 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 जो दूसरे लोगों को गुमराह करने में उपयोगकर्ताओं की मदद करते हैं या जिनका मकसद किसी भी तरीके की धोखाधड़ी करना हो. ऐसे ही कुछ ऐप्लिकेशन के उदाहरण हैं: आईडी कार्ड, सोशल सिक्योरिटी नंबर, पासपोर्ट, डिप्लोमा, क्रेडिट कार्ड, और ड्राइविंग लाइसेंस. हालांकि, ये इन तक ही सीमित नहीं है. ऐप्लिकेशन के कॉन्टेंट और उसके इस्तेमाल के बारे में सही जानकारी देनी होगी. जैसे कि ऐप्लिकेशन का शीर्षक, उसका विवरण, और इमेज/वीडियो वगैरह. साथ ही, ऐप्लिकेशन को इस्तेमाल करने का अनुभव बिल्कुल वैसा ही होना चाहिए जैसा ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति ने उम्मीद की थी.

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

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 मिलती.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो दूसरे ऐप्लिकेशन या वेबसाइट की नकल करते हैं और इस्तेमाल करने वाले लोगों को धोखे से अपनी निजी जानकारी या पुष्टि करने से जुड़ी जानकारी देने के लिए कहते हैं.
- ऐसे ऐप्लिकेशन जो बिना पुष्टि वाले या असली फ़ोन नंबर, संपर्क, पते को दिखाते हैं या किसी कंपनी या व्यक्ति की सहमति के बिना निजी रूप से पहचान करने वाली जानकारी दिखाते हैं.
- ऐसे ऐप्लिकेशन जिनकी मुख्य सुविधाएं, इस्तेमाल करने वाले व्यक्ति के इलाके, डिवाइस पैरामीटर या इस्तेमाल करने वाले लोगों से मिलने वाले अन्य डेटा पर निर्भर हो और इनकी वजह से आने वाले बदलाव के बारे में स्टोर पेज में साफ़ तौर पर नहीं बताया गया हो.
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को बिना सूचना दिए वर्शन में ज़रूरी बदलाव करते हैं (उदाहरण के लिए, 'नया क्या है' सेक्शन) और स्टोर पेज अपडेट करते हैं.
- ऐसे ऐप्लिकेशन जो समीक्षा के दौरान व्यवहार में बदलाव करते हैं या उलझाने की कोशिश करते हैं.
- कॉन्टेंट डिलीवरी नेटवर्क (सीडीएन) वाले ऐसे ऐप्लिकेशन जो डाउनलोड करने की सुविधा देते हैं और डाउनलोड करने से पहले ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को डाउनलोड साइज़ के बारे में सही जानकारी नहीं देते हैं.

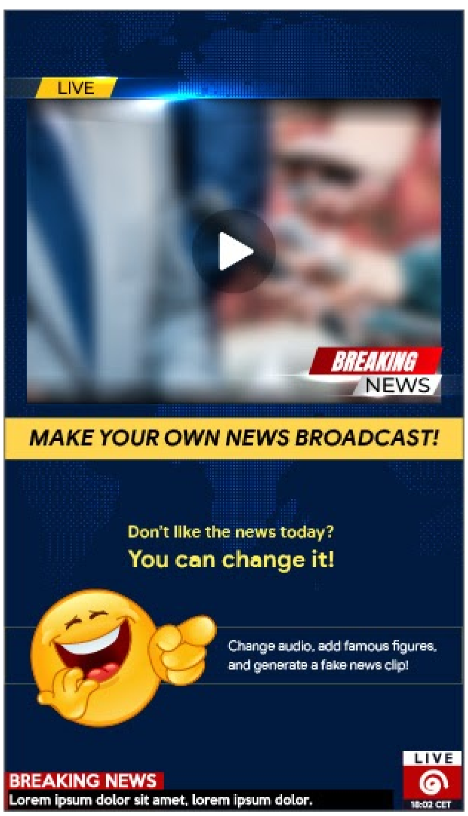
ऐसा कॉन्टेंट जिसमें छेड़छाड़ की गई हो

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो तस्वीरों, वीडियो, और/या टेक्स्ट की मदद से गलत या गुमराह करने वाली जानकारी या दावे करने का प्रचार करते हैं या उन्हें बनाने में मदद 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. हालांकि, लोगों की पसंद, व्यंग्य या पैरोडी वाले कॉन्टेंट के लिए छूट मिल सकती है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो किसी जानी-मानी हस्ती को राजनीतिक रूप से संवेदनशील कार्यक्रम के विरोध-प्रदर्शनों से जोड़कर दिखाते हैं.
- ऐसे 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 हस्तियों के फ़ुटेज का इस्तेमाल करते हैं.
- ऐसे ऐप्लिकेशन जो मीडिया क्लिप में बदलाव करके, किसी न्यूज़ ब्रॉडकास्ट की नकल करते हैं.



(1) यह ऐप्लिकेशन न्यूज़ ब्रॉडकास्ट की नकल करने के लिए, मीडिया क्लिप में बदलाव करते हैं और वॉटरमार्क के बिना क्लिप में मशहूर और जानी-मानी हस्तियों को जोड़ने की सुविधा देता है.

गलत तरीके से पेश करना

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते जो किसी दूसरे व्यक्ति या संगठन के नाम पर काम करते हों. इसके अलावा, हम उन्हें भी अनुमति नहीं देते जो ऐप्लिकेशन या डेवलपर खाते किसी दूसरे व्यक्ति या संगठन के मालिकाना हक या असली 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 गलत जानकारी देते हैं या अपने मूल देश के बारे में छिपाते हैं या किसी दूसरे देश के लोगों को टारगेट करते हैं. हालांकि, यह इन ही तक सीमित नहीं है.

मैलवेयर

मैलवेयर एक ऐसा कोड है जो किसी भी उपयोगकर्ता, उसके 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 कैटगरी शामिल हैं जिसमें हम लगातार नई कैटगरी को अपडेट कर रहे हैं और जोड़ रहे हैं.

मैलवेयर

हमारी मैलवेयर नीति बहुत आसान है. 'Google Play स्टोर' और ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डिवाइस के साथ Android का नेटवर्क, नुकसान पहुंचाने वाली गतिविधियों से दूर रहना चाहिए. अपने इस बुनियादी सिद्धांत से, हम अपने ऐप्लिकेशन इस्तेमाल करने वाले लोगों और उनके Android डिवाइस को एक सुरक्षित Android नेटवर्क देने की कोशिश कर रहे हैं.

हालांकि, मैलवेयर कई तरह के होते हैं और उनके 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

ऐसा कोड जो डिवाइस पर अनचाही, नुकसान पहुंचाने वाली, और कहीं से भी कंट्रोल की जाने वाली कार्रवाइयों की अनुमति देता है.

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 के तहत जोखिम से भरा माना जाता है.

बिलिंग से जुड़ी धोखाधड़ी

ऐसा कोड जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों से जान-बूझकर और धोखाधड़ी करके, अपने-आप शुल्क लेता है.

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

मैसेज (एसएमएस) से जुड़ी धोखाधड़ी

ऐसा कोड जो लोगों से बिना उनकी अनुमति के प्रीमियम मैसेज भेजने पर शुल्क लेता है. इसके अलावा, पहचान ज़ाहिर करने वाली जानकारी को छिपाते हुए, ऐसे मैसेज भेजता है जिससे उपयोगकर्ता को अनजाने में पैसे चुकाने पड़ते हैं. इतना ही नहीं, धोखाधड़ी करने वाला, लोगों 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 की जानकारी के हिस्से को 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 पैसे चुकाने या सदस्यता लेने की पुष्टि करने की जानकारी देते हैं.

कॉल से जुड़ी धोखाधड़ी

ऐसा कोड जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों से बिना उनकी अनुमति के प्रीमियम नंबर पर कॉल करके शुल्क लेता है.

टोल नंबर से जुड़ी धोखाधड़ी

ऐसा कोड जिससे ऐप्लिकेशन इस्तेमाल करने वाले लोग अनजाने में अपने मोबाइल फ़ोन के बिल से कॉन्टेंट खरीदते या सदस्यता लेते हैं.

टोल नंबर से होने वाली धोखाधड़ी में प्रीमियम मैसेज और प्रीमियम कॉल के अलावा, 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.

स्टालकरवेयर

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.

स्टालकरवेयर ऐप्लिकेशन, पीएचए की सेवा देने वालों के अलावा, किसी दूसरे पक्ष को डेटा उपलब्ध कराते हैं. इन मान्य स्टालकरवेयर ऐप्लिकेशन का इस्तेमाल करके, अभिभावक अपने बच्चों की गतिविधियों पर नज़र नहीं रख सकते. हालांकि, इन ऐप्लिकेशन का इस्तेमाल करके किसी व्यक्ति (उदाहरण के लिए, पति या पत्नी) की जानकारी के बिना या अनुमति लिए बिना, उनकी गतिविधियों पर नज़र रखी जा सकती है. ऐसा तब हो सकता है, जब डेटा शेयर होने की सूचना लगातार दिखाई न दे रही हो.

'Play स्टोर' पर सिर्फ़ उन ही ऐप्लिकेशन की अनुमति है जो नीति का पालन करते हैं, जिन्हें खास तौर पर अभिभावक (परिवार समेत) की निगरानी या एंटरप्राइज़ प्रबंधन के लिए बनाया गया है और उनका प्रचार किया गया है. उनमें निगरानी करने और रिपोर्ट करने की सुविधा होनी चाहिए. भले ही, नीचे दी गई शर्तों का पूरी तरह से पालन करते हों.

'Play स्टोर' पर मौजूद ऐसे ऐप्लिकेशन जो किसी डिवाइस को इस्तेमाल करने वाले व्यक्ति के व्यवहार को मॉनिटर करते हैं या निगरानी करते हैं, उनके लिए इन शर्तों का पालन करना 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 के लिए आपने ऐप्लिकेशन प्रकाशित किया है, अगर वहां उसे गैरकानूनी बताया जाता है, तो उस ऐप्लिकेशन को हटा दिया जाएगा.

सेवा में रुकावट (DoS)

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

उदाहरण के लिए, रिमोट सर्वर पर लोड बढ़ाने के लिए, भारी संख्या में एचटीटीपी अनुरोध भेजकर ऐसा किया जा सकता है.

गलत तरीके से डाउनलोड करने वाले मैलवेयर

ऐसा कोड जो डिवाइस को नुकसान नहीं पहुंचाता, 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
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों की अनुमति मिलने पर ही सभी पीएचए डाउनलोड होते हैं.

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

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

ये ऐप्लिकेशन Android इस्तेमाल करने वाले व्यक्ति 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, ऐप्लिकेशन का इस्तेमाल करने वाले व्यक्ति की पुष्टि करने वाले क्रेडेंशियल या बिलिंग की 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 है या उसे ऐक्सेस करने से रोकता है. ऐसा करके, यह कोड ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति 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.

ऐसे प्रिविलेज एस्केलेशन ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना डिवाइस को रूट करते हैं. वे डिवाइस को रूट करने वाले ऐप्लिकेशन की कैटगरी में आते हैं.

रैंसमवेयर

ऐसा कोड जो डिवाइस या उसमें मौजूद डेटा पर कुछ या पूरा कंट्रोल अपने पास रखता है. साथ ही, इस्तेमाल करने वाले व्यक्ति से पैसे चुकाने या डिवाइस पर ऐसी कार्रवाई करने की मांग करता है जिससे इस्तेमाल करने वाला व्यक्ति 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 कैटगरी से बाहर रखा जा सकता है. इसका मुख्य काम डिवाइस के प्रबंधन को सब्सिडाइज़ करना है. यह कोड, सुरक्षित लॉक और प्रबंधन के लिए ज़रूरी शर्तें पूरी करता है. साथ ही, लोगों को पूरी जानकारी देता है और उनसे सहमति लेने की ज़रूरी शर्तें पूरी करता है.

रूट करना

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 ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को बिना जानकारी दिए डिवाइस रूट कर देते हैं. यह इस्तेमाल करने वाले व्यक्ति को रूट करने की जानकारी पहले देते हैं, लेकिन ये दूसरी ऐसी कार्रवाइयां करते हैं जो डिवाइस की दूसरी पीएचए कैटगरी पर लागू होती हैं.

स्पैम

ऐसा कोड जो इस्तेमाल करने वाले व्यक्ति 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 इस तरह से शेयर करता है जिसकी उम्मीद इस्तेमाल करने वाला व्यक्ति 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 या ऐप्लिकेशन की जानकारी 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 वह ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना कार्रवाइयां करता है.

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 कैटगरी में रखा जाएगा. इसका मतलब यह नहीं है कि वह ऐप्लिकेशन नुकसान पहुंचाने वाला है, लेकिन बिना समीक्षा किए इसे सुरक्षित भी नहीं कहा जा सकता.

बैकडोर कैटगरी वाले मैलवेयर पर नोट

कोड की कार्रवाइयों के आधार पर बैकडोर मैलवेयर की कैटगरी 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.

मोबाइल का अनचाहा सॉफ़्टवेयर

यह नीति, Android नेटवर्क और Google Play Store के सिद्धांतों के आधार पर Google की अनचाही सॉफ़्टवेयर नीति से बनती है. इन सिद्धांतों का उल्लंघन करने वाला सॉफ़्टवेयर संभावित रूप से ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के अनुभव को नुकसान पहुंचा सकता है और हम इस्तेमाल करने वाले व्यक्ति को इससे बचाने के लिए कदम उठाएंगे.

मोबाइल का अनचाहा सॉफ्टवेयर

Google का मानना है कि अगर हम ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति पर ध्यान देंगे, तो बाकी सब अपने-आप ठीक होगा. हम अपने सॉफ़्टवेयर सिद्धांत और अनचाही सॉफ़्टवेटर नीति में सॉफ़्टवेयर के लिए ऐसे सामान्य सुझाव देते हैं जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को बेहतरीन अनुभव देता है. यह नीति, Android नेटवर्क और Google Play Store के सिद्धांतों के आधार पर Google की अनचाही सॉफ़्टवेयर नीति से बनती है. इन सिद्धांतों का उल्लंघन करने वाला सॉफ़्टवेयर संभावित रूप से ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के अनुभव को नुकसान पहुंचा सकता है और हम इस्तेमाल करने वाले व्यक्ति को इससे बचाने के लिए कदम उठाएंगे.

अनचाही सॉफ़्टवेयर नीति के आधार पर, हमें पता चला है कि ज़्यादातर अनचाहे सॉफ़्टवेयर एक या उससे ज़्यादा विशेषताएं दिखाते हैं:

- अनचाहा सॉफ़्टवेयर ऐसी फ़ाइल या ऐसा मोबाइल ऐप्लिकेशन होता है जिससे लोगों के साथ धोखाधड़ी की जाती है. यह ऐसी खास बात का वादा करता है जिसे पूरा नहीं किया सकता.
- यह सॉफ़्टवेयर को इंस्टॉल किए जाने के लिए लोगों को चकमा देने की कोशिश करता है या फिर वह किसी दूसरे प्रोग्राम के साथ जुड़कर इंस्टॉल हो जाता है.
- यह सॉफ़्टवेयर इस्तेमाल करने वाले व्यक्ति को अपने सिद्धांतो और ज़रूरी सुविधाओं के बारे में नहीं बताता है.
- यह इस्तेमाल करने वाले व्यक्ति के सिस्टम पर गलत असर डालते हैं.
- यह सॉफ़्टवेयर लोगों को बिना बताए, उनकी निजी जानकारी को इकट्ठा करता है या उसे दूसरों तक पहुंचाता है.
- यह सॉफ़्टवेयर सुरक्षा इंतजाम के बिना ही निजी जानकारी को इकट्ठा करता है या उसे दूसरों तक पहुंचाता है (उदाहरण के लिए, एचटीटीपीएस पर शेयर करना)

- यह सॉफ़्टवेयर दूसरे सॉफ़्टवेयर के साथ शामिल होता है और इसकी मौजूदगी का पता नहीं चलता.

मोबाइल डिवाइस पर सॉफ़्टवेयर, ऐप्लिकेशन, बाइनरी, फ़्रेमवर्क में बदलाव वगैरह एक कोड के रूप में होता है. ऐसे सॉफ़्टवेयर को रोकने के लिए जो सॉफ़्टवेयर नेटवर्क को नुकसान पहुंचाते हैं या उपयोगकर्ता के अनुभव में रुकावट डालते हैं, इन सिद्धांतों का उल्लंघन करने वाले कोड पर कार्रवाई की जाएगी.

नीचे दी गई नीति को हमने अनचाहे सॉफ़्टवेयर के आधार पर बनाया है, ताकि इसे मोबाइल सॉफ़्टवेयर पर लागू किया जा सके. नीचे दी गई नीति के मुताबिक, हम मोबाइल के अनचाहे सॉफ़्टवेयर के नए तरह के गलत इस्तेमाल को रोकने के लिए नीति को बेहतर बनाना जारी रखेंगे.

पारदर्शिता वाला व्यवहार और साफ़ जानकारी

सभी कोड को इस्तेमाल करने वाले व्यक्ति से किए गए वादों को पूरा करना चाहिए. ऐप्लिकेशन को सुविधाओं की सभी जानकारी देनी चाहिए. ऐप्लिकेशन को लोगों को भ्रमित नहीं करना चाहिए.

- ऐप्लिकेशन को सुविधाओं और इरादों के बारे में साफ़ तौर पर बताना चाहिए.
- कृपया, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को साफ़ और सही जानकारी दें कि ऐप्लिकेशन, सिस्टम में किस तरह के बदलाव करेगा. साथ ही, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को सभी ज़रूरी इंस्टॉल करने के विकल्पों और बदलावों की समीक्षा करने और उन्हें मंज़ूरी देने की अनुमति दें.
- सॉफ़्टवेयर को डिवाइस की स्थिति को इस्तेमाल करने वाले व्यक्ति के लिए गलत तरीके से पेश नहीं करना चाहिए. उदाहरण के लिए, दावा करना कि सिस्टम की सुरक्षा से गंभीर खतरा है या सिस्टम में वायरस है.
- विज्ञापन ट्रैफ़िक और/या ऐप्लिकेशन इंस्टॉल करने वाले लोगों की संख्या बढ़ाने के लिए डिज़ाइन की गई गलत गतिविधि की मदद न लें.
- हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी दूसरे व्यक्ति या ऐप्लिकेशन की पहचान चुराकर लोगों को गुमराह करते हैं. जैसे कि दूसरे डेवलपर, कंपनी, इकाई. अगर आपके ऐप्लिकेशन को किसी व्यक्ति से अनुमति नहीं मिली है और न ही यह किसी व्यक्ति से जुड़ा है, तो इसका झूठा दावा न करें.

उल्लंघनों के उदाहरण:

- विज्ञापन से होने वाली धोखाधड़ी
- पहचान चुराना

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा की सुरक्षा करना

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी और संवेदनशील डेटा को ऐक्सेस करने, इस्तेमाल करने, इकट्ठा करने, और शेयर किए जाने के बारे में साफ़ और सही जानकारी दें. जहां भी लागू हो, वहां ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को इस्तेमाल करने के लिए सभी ज़रूरी नीतियों का पालन करना चाहिए. साथ ही, डेटा की सुरक्षा के लिए सभी सावधानियां रखें.

- लोगों के डिवाइस से डेटा भेजने और इकट्ठा करने से पहले, उनसे डेटा को इकट्ठा करने की सहमति लें. इसमें तीसरे पक्ष के खाते, ईमेल, फ़ोन नंबर, इंस्टॉल किए गए ऐप्लिकेशन, फ़ाइलें, जगह की जानकारी, और किसी भी तरह का ऐसा दूसरा निजी और संवेदनशील डेटा शामिल हैं जिसे इस्तेमाल करने वाले व्यक्ति को इकट्ठा किए जाने की उम्मीद नहीं होगी.
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के इकट्ठा किए गए निजी और संवेदनशील डेटा को सुरक्षित तरीके से प्रबंधित किया जाना चाहिए, जिसमें आधुनिक क्रिप्टोग्राफ़ी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करना भी शामिल है.
- मोबाइल ऐप्लिकेशन समेत सॉफ़्टवेयर को उपयोगकर्ता के निजी और संवेदनशील डेटा को सिर्फ़ सर्वर पर भेजना चाहिए, क्योंकि यह ऐप्लिकेशन की सुविधाओं से जुड़ा हुआ है.

उल्लंघनों के उदाहरण:

- डेटा इकट्ठा करना (cf स्पायवेयर)
- पाबंदी वाली अनुमतियों का गलत इस्तेमाल

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के लिए डेटा की नीतियों का उदाहरण:

- *Google Play का इस्तेमाल करने वाले लोगों के लिए डेटा नीति*
- *Google मोबाइल सेवाओं (GMS) का इस्तेमाल करने वाले व्यक्ति के लिए डेटा की नीति से जुड़ी ज़रूरी शर्तें*
- *Google API की सेवा का इस्तेमाल करने वाले व्यक्ति के लिए डेटा नीति*

मोबाइल पर इस्तेमाल के अनुभव को नुकसान न पहुंचाएं

इस्तेमाल करने वाले व्यक्ति का अनुभव साफ़, समझने में आसान, और उस पसंद पर आधारित होना चाहिए जो उसने चुनी है. इसे इस्तेमाल करने वाले व्यक्ति को इसकी खास बातें साफ़ तौर पर बतानी चाहिए और विज्ञापन में बताए गए या उपयोगकर्ता के मनमुताबिक अनुभव में बदलाव नहीं होना चाहिए.

- उन विज्ञापनों को न दिखाएं जो अनचाहे तरीके से लोगों को दिखते हैं. इन तरीकों में डिवाइस की सुविधाओं के इस्तेमाल में रुकावट डालना या हस्तक्षेप करना शामिल है. इसके अलावा, ट्रिगर करने वाले ऐप्लिकेशन के बाहर दिखाई देने या उन्हें आसानी से खारिज किए बिना और विशेषता के साथ नहीं दिखाते हैं.
- ऐप्लिकेशन को दूसरे ऐप्लिकेशन या डिवाइस के इस्तेमाल में रुकावट नहीं डालनी चाहिए
- यह साफ़ हो कि जहां भी लागू हो उसे अनइंस्टॉल करना चाहिए.
- मोबाइल सॉफ़्टवेयर को डिवाइस के OS या दूसरे ऐप्लिकेशन से मिलने वाली सूचनाओं की नकल नहीं करनी चाहिए. उपयोगकर्ता को दूसरे ऐप्लिकेशन या ऑपरेटिंग सिस्टम की चेतावनियां न दिखाएं. खास तौर पर ऐसी चेतावनियां जो OS में होने वाले बदलावों की सूचना इस्तेमाल करने वाले व्यक्ति को देते हैं.

उल्लंघनों के उदाहरण:

- परेशान करने वाले विज्ञापन
- सिस्टम की सुविधाओं का गलत या गैरकानूनी इस्तेमाल

विज्ञापन से होने वाली धोखाधड़ी

विज्ञापन से जुड़ी धोखाधड़ी पर पूरी तरह से पाबंदी है. ऐसे उपयोगकर्ता की पसंद जिनकी पहचान की पुष्टि हो चुकी है उनसे किसी विज्ञापन नेटवर्क को भरोसे में लेकर ट्रैफ़िक पाने के गलत इरादे से बनाए गए विज्ञापन इंटरैक्शन, विज्ञापन से जुड़ी धोखाधड़ी हैं. यह अमान्य ट्रैफ़िक का एक रूप है. डेवलपर के सह-उत्पाद को बिना अनुमति से विज्ञापनों को दिखाना विज्ञापन से जुड़ी धोखाधड़ी है, जैसे कि छिपे हुए विज्ञापनों को दिखाना, विज्ञापनों पर अपने-आप क्लिक करना, जानकारी को बदलना या गैर मानवीय कार्रवाइयों (स्पाइडर्स, बॉट वगैरह) का फ़ायदा लेना या मानव गतिविधि को अमान्य विज्ञापन ट्रैफ़िक बनाने के लिए डिज़ाइन करना. अमान्य ट्रैफ़िक और विज्ञापन से होने वाली धोखाधड़ी विज्ञापन देने वालों, डेवलपर, और लोगों को नुकसान पहुंचाती है. यह मोबाइल विज्ञापन नेटवर्क के भरोसे को भी लंबे समय तक नुकसान पहुंचा सकती है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

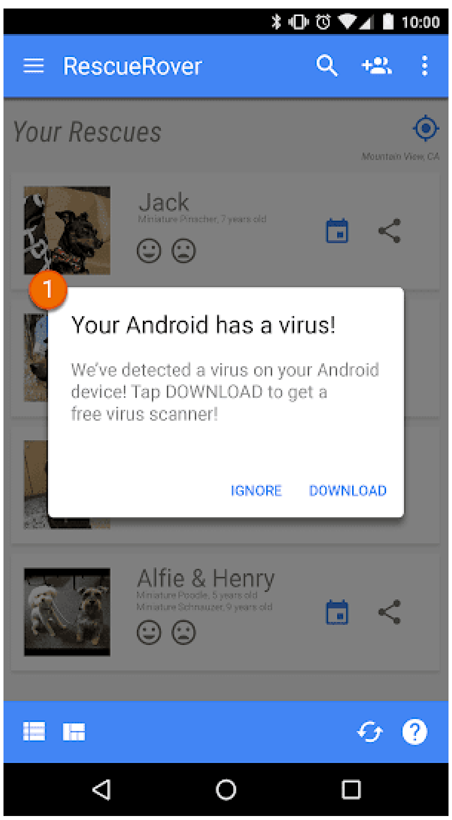
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को दिखाई न देने वाले विज्ञापन देता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की इच्छा के बिना अपने-आप विज्ञापनों पर क्लिक करता है या धोखाधड़ी से विज्ञापनों पर क्लिक का क्रेडिट उपयोगकर्ता को देने के लिए, ऐसे किसी नेटवर्क का इस्तेमाल करता है.
- ऐसा ऐप्लिकेशन जो इंस्टॉल करने के पैसे पाने के लिए इंस्टॉल करने के नकली एट्रिब्यूशन क्लिक भेजता है और यह भेजने वाले के नेटवर्क से जनरेट नहीं किया गया होता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति के ऐप्लिकेशन इंटरफ़ेस में न होने पर भी पॉप-अप विज्ञापन दिखाता है.
- ऐसा ऐप्लिकेशन जो विज्ञापन इन्वेंट्री को गलत तरीके से दिखाता है. उदाहरण के लिए, वह ऐप्लिकेशन जो विज्ञापन नेटवर्क को बताता है कि यह iOS डिवाइस पर चल रहा है जबकि वह वास्तव में Android डिवाइस पर चल रहा होता है, वह ऐप्लिकेशन जो कमाई करने वाले पैकेज के नाम की गलत जानकारी देता है.

सिस्टम की सुविधाओं का गलत या गैरकानूनी इस्तेमाल

हम ऐसे ऐप्लिकेशन या विज्ञापनों को अनुमति नहीं देते जो सूचना या चेतावनी जैसे सिस्टम की सुविधा की नकल करते हैं या उसमें दखल देते हैं. सिस्टम के लेवल से मिलने वाली सूचनाओं का इस्तेमाल सिर्फ़ किसी ऐप्लिकेशन की आंतरिक सुविधाओं के लिए किया जा सकता है, जैसे कि कोई ऐसा एयरलाइन ऐप्लिकेशन जो लोगों को खास ऑफ़र के बारे में सूचना देता है या ऐसा गेम जो लोगों को गेम में प्रचारों के बारे में सूचना देता है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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.

पहचान चुराना

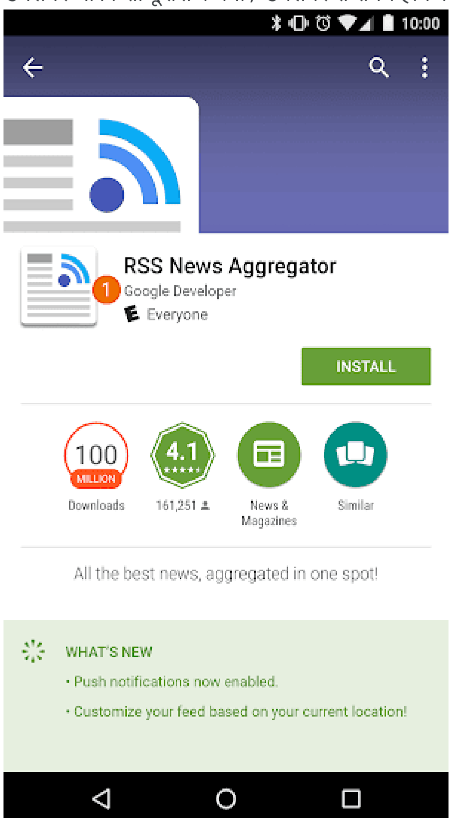
जब डेवलपर दूसरे लोगों या उनके ऐप्लिकेशन की पहचान चुराते हैं, तो इससे लोग गुमराह होते हैं. साथ ही, इससे डेवलपर समुदाय को नुकसान पहुंचता है. हम ऐसे ऐप्लिकेशन पर पाबंदी लगाते हैं जो किसी दूसरे की पहचान चुराकर लोगों को गुमराह करते हैं.

पहचान चुराना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी दूसरे व्यक्ति (जैसे कि दूसरे डेवलपर, कंपनी, इकाई) या ऐप्लिकेशन की पहचान चुराकर लोगों को गुमराह करते हैं. अगर आपके ऐप्लिकेशन को किसी व्यक्ति से अनुमति नहीं मिली है और न ही ये किसी व्यक्ति से जुड़ा है, तो इसका झूठा दावा न करें. इस बात का ध्यान रखें कि आप अपने ऐप्लिकेशन में आइकॉन, जानकारी, शीर्षक या ऐप्लिकेशन के अंदर मौजूद ऐसी चीज़ों का इस्तेमाल न करें जो लोगों को किसी और या किसी दूसरे ऐप्लिकेशन से आपके ऐप्लिकेशन के संबंध के बारे में गुमराह कर सकता है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- डेवलपर जो किसी दूसरी कंपनी / डेवलपर से संबंध होने का झूठा दावा करते हैं:



① इस ऐप्लिकेशन के डेवलपर के नाम से इसके Google से आधिकारिक रूप से जुड़े होने का पता चलता है, जबकि दोनों के बीच ऐसा कोई संबंध नहीं है.

- ऐसे ऐप्लिकेशन जिनके शीर्षक और आइकॉन पहले से मौजूद ऐसे उत्पादों या सेवाओं से मिलते-जुलते हैं जिससे इस्तेमाल करने वाले लोग गुमराह हो सकते हैं:

कमाई करना और विज्ञापन

Google Play, डेवलपर और लोगों के फ़ायदे के लिए कमाई करने के कई तरीके देता है. इनमें पैसे चुकाकर लोगों तक ऐप्लिकेशन पहुंचाना, ऐप्लिकेशन के अंदर उत्पाद, सदस्यताएं, और अलग-अलग तरह के विज्ञापन मॉडल के हिसाब से ऐप्लिकेशन तैयार करने जैसे तरीके शामिल हैं. लोगों को सुविधाओं का 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.

यहां ऐसे उत्पादों के कुछ उदाहरण दिए गए हैं जो हाल ही में Google Play इन-ऐप्लिकेशन बिलिंग से जुड़े नहीं हैं:

- वर्चुअल गेम वाले उत्पाद, इनमें सिक्के, रत्न, हारने के बाद एक और लाइफ़ या मौका, खास आइटम या उपकरण, पात्र या अवतार या किसी अन्य लेवल या खेलने का समय शामिल है.
- ऐप्लिकेशन फ़ंक्शन या सामग्री, जैसे कि किसी ऐप्लिकेशन का बिना विज्ञापन वाला वर्शन या नई सुविधाएं जो मुफ़्त वर्शन में उपलब्ध नहीं हैं.
- सदस्यता सेवाएं, जैसे कि म्यूज़िक की स्ट्रीमिंग, वीडियो, किताब या दूसरी मीडिया सेवाएं; असल वर्शन के साथ जुड़े डिजिटल प्रकाशन; और सोशल नेटवर्किंग सेवाएं.
- क्लाउड सॉफ़्टवेयर वाले उत्पाद, इनमें डेटा स्टोर करने वाली सेवाएं, कारोबार की उत्पादकता बढ़ाने वाले सॉफ़्टवेयर, और वित्तीय प्रबंधन वाले सॉफ़्टवेयर शामिल हैं.

यहां ऐसे उत्पादों के कुछ उदाहरण दिए गए हैं जो हाल ही में Google Play इन-ऐप्लिकेशन बिलिंग से जुड़े नहीं है:

- खुदरा कारोबार के लिए बेची जाने वाली चीज़ें, जैसे कि किराना का सामान, कपड़े, घरेलू सामान, और इलेक्ट्रॉनिक का सामान.
- सेवा शुल्क, इनमें टैक्सी और परिवहन सेवाएं, सफ़ाई सेवाएं, खाने की डिलीवरी, हवाई किराया, और इवेंट के टिकट शामिल हैं.
- सदस्यता के लिए एक-बार में दिया जाने वाला शुल्क या बार-बार दी जाने वाली रकम, इनमें जिम की सदस्यता, लॉयल्टी कार्यक्रम या ऐक्सेसरीज़, कपड़े या दूसरे असल उत्पाद ऑफ़र करने वाले क्लब शामिल हैं.
- एकमुश्त भुगतान, इनमें एक सहयोगी का दूसरे सहयोगी को पैसे चुकाना, ऑनलाइन नीलामी, और दान शामिल हैं.
- बिल चुकाने का इलेक्ट्रॉनिक तरीका , इनमें क्रेडिट कार्ड के बिल, सुविधाएं, और केबल या दूरसंचार सेवाएं शामिल हैं.

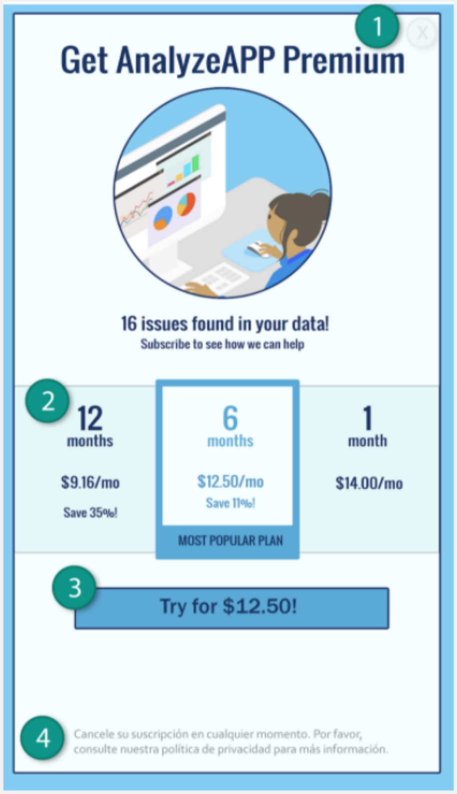
ध्यान रखें कि हम असल उत्पाद और सेवाएं बेचने वाले ऐप्लिकेशन के लिए, **Google Pay** एपीआई की सुविधा ऑफ़र करते हैं. ज़्यादा जानकारी के लिए, कृपया हमारे **Google Pay** डेवलपर पेज पर जाएं.

सदस्यताएं

डेवलपर के तौर पर, आपको अपने ऐप्लिकेशन में दी जाने वाली किसी सदस्यता सेवा या कॉन्टेंट के बारे में लोगों को गुमराह नहीं करना चाहिए. किसी भी स्प्लैश स्क्रीन या ऐप्लिकेशन के अंदर किए जाने वाले प्रचार में अपने सभी ऑफ़र से जुड़ी सही जानकारी देना ज़रूरी है.

अपने ऐप्लिकेशन में आपको अपने ऑफ़र के बारे में साफ़ तौर पर बताना चाहिए. आपको अपने ऑफ़र की शर्तों के बारे में भी साफ़ तौर पर बताना चाहिए, जैसे कि सदस्यता शुल्क कितना होगा, बिलिंग साइकल कितने दिन का होगा, और ऐप्लिकेशन इस्तेमाल करने के लिए सदस्यता ज़रूरी है या नहीं. लोगों को जानकारी की समीक्षा करने के लिए कोई और कार्रवाई करने की ज़रूरत नहीं होनी चाहिए.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:



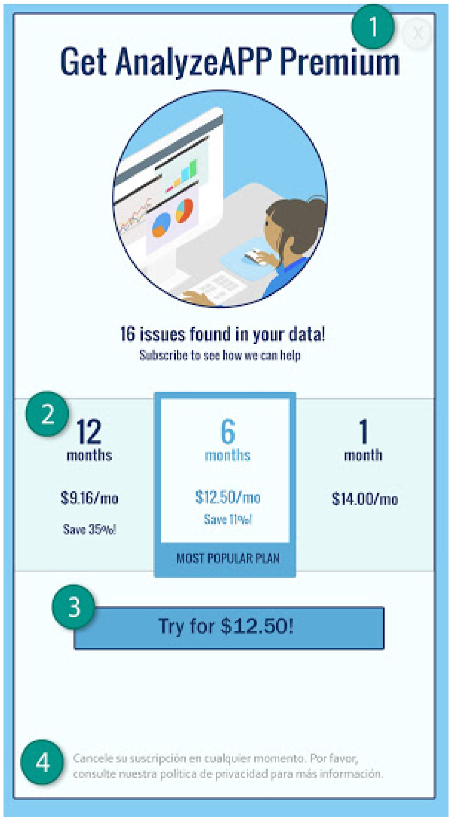
① Dismiss button is not clearly visible and users may not understand that they can access functionality without accepting the subscription offer.

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.

- 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.

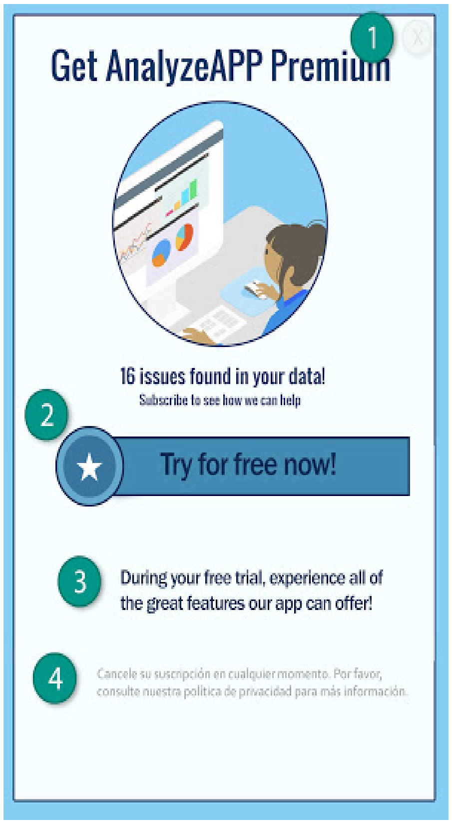
④ Offer should be localized in the same language as the terms and conditions so that users can understand the entire offer.

मुफ़्त में आज़माने की सुविधा और शुरुआती ऑफ़र

किसी उपयोगकर्ता को आपके ऐप्लिकेशन की सदस्यता लेने से पहले: आपको ऑफ़र से जुड़ी शर्तों के बारे में लोगों को साफ़ और सही तरीके से बताना चाहिए. इन शर्तों में ऑफ़र की अवधि, किराया, और कॉन्टेंट या सेवाओं को ऐक्सेस करने की जानकारी शामिल है. लोगों को यह बताना न भूलें कि मुफ़्त में आज़माने की सुविधा वाली सदस्यता कब और कैसे, पैसे देकर ली जाने वाली सदस्यता में बदलेगी. इसके अलावा, पैसे देकर ली जाने वाली सदस्यता की कीमत के बारे में बताएं और अगर वे इसे नहीं लेना चाहते, तो उन्हें सदस्यता रद्द करने का तरीका भी बताएं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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.

सदस्यताओं को प्रबंधित करना और उन्हें रद्द करना

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

यह आपकी ज़िम्मेदारी है कि आप सदस्यता लेने, उसे रद्द कराने, और रिफ़ंड पाने की नीतियों में होने वाले किसी भी बदलाव के बारे में लोगों को जानकारी दें. साथ ही, यह पक्का करें कि नीतियां लागू कानून का पालन करती हों.

विज्ञापन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह या परेशान करने वाले विज्ञापन शामिल होते हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं. हम आपके ऐप्लिकेशन में दिए गए विज्ञापनों को आपके 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 बारे में जानने के लिए, कृपया यहां क्लिक करें.

विज्ञापनों के लिए जगह के डेटा की जानकारी का इस्तेमाल

ऐसे ऐप्लिकेशन जो अनुमति मांगकर लिए गए, डिवाइस की जगह की जानकारी के डेटा का इस्तेमाल विज्ञापन दिखाने के लिए भी 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 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.

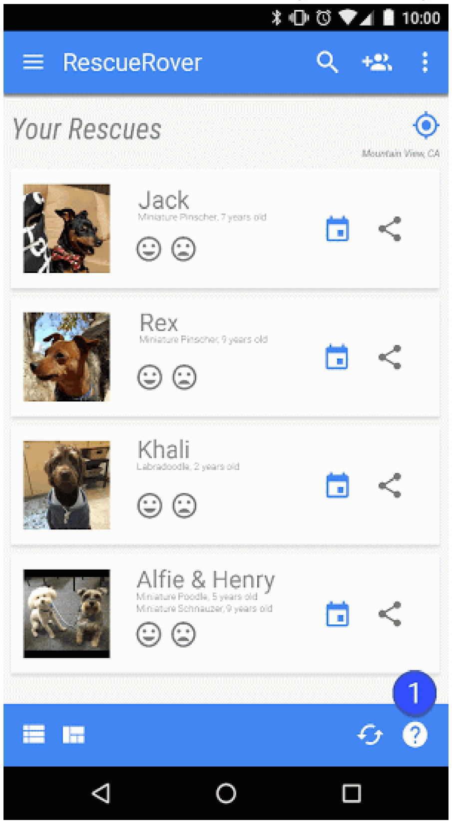
- [जगह की जानकारी की अनुमति](#) की शर्तों के मुताबिक, जगह की जानकारी के ऐक्सेस का अनुरोध ऐप्लिकेशन में पहले से मौजूद सुविधाओं और सेवाओं को लागू करने के लिए ही किया जा सकता है, लेकिन सिर्फ़ विज्ञापन दिखाने के लिए नहीं.

धोखाधड़ी करने वाले विज्ञापन

विज्ञापनों को किसी भी ऐप्लिकेशन के यूज़र इंटरफ़ेस या किसी ऑपरेटिंग सिस्टम की सूचना या चेतावनी देने के तरीकों की नकल या उनकी पहचान नहीं चुरानी चाहिए. ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को यह साफ़ तौर पर बताया जाना चाहिए कि हर एक विज्ञापन किस ऐप्लिकेशन की तरफ़ से उपलब्ध कराया जा रहा है.

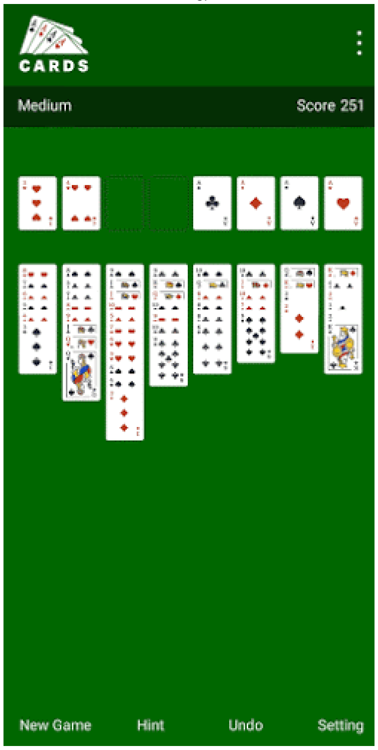
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

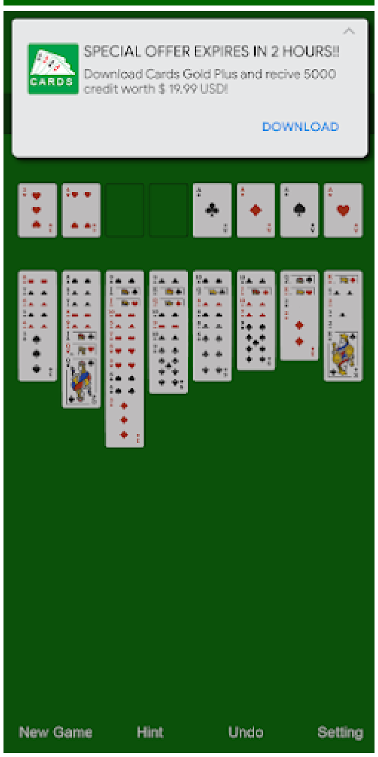
- ऐसे विज्ञापन जो किसी ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) की नकल करते हैं:



① इस ऐप्लिकेशन में दिया गया सवाल वाला 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:



- 

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

लॉकस्क्रीन पर कमाई करने की सुविधा

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

परेशान करने वाले विज्ञापन

परेशान करने वाले विज्ञापन ऐसे विज्ञापन होते हैं जो लोगों को अचानक दिखाए जाते हैं. ऐसे विज्ञापनों पर ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति गलती से किसी जगह क्लिक कर सकता है. साथ ही, इनसे डिवाइस की सुविधाओं के इस्तेमाल में रूकावट या खराबी भी आ सकती है.

आपका ऐप्लिकेशन, विज्ञापन के मकसद से उपयोगकर्ता को तब तक किसी विज्ञापन पर क्लिक करने या अपनी निजी जानकारी देने के लिए मजबूर नहीं कर सकता, जब तक वह ऐप्लिकेशन को पूरी तरह से इस्तेमाल नहीं करता है. साथ ही, पेज पर अचानक दिखने वाले विज्ञापन सिर्फ़ उसी

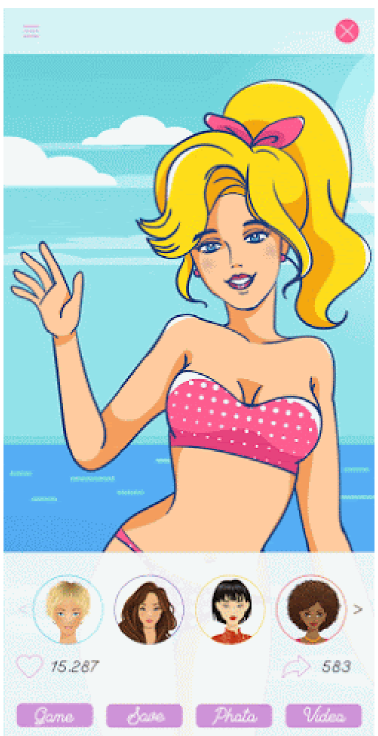
ऐप्लिकेशन में दिखाए जा सकते हैं जिसमें उन्हें उपलब्ध कराया गया है. अगर आपका ऐप्लिकेशन पेज पर अचानक दिखने वाले विज्ञापन या ऐसे दूसरे विज्ञापन दिखाता है जो सामान्य इस्तेमाल में रुकावट डालते हैं, तो उन्हें ऐसा होना चाहिए कि पेनल्टी के बिना आसानी से खारिज किया जा सके.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

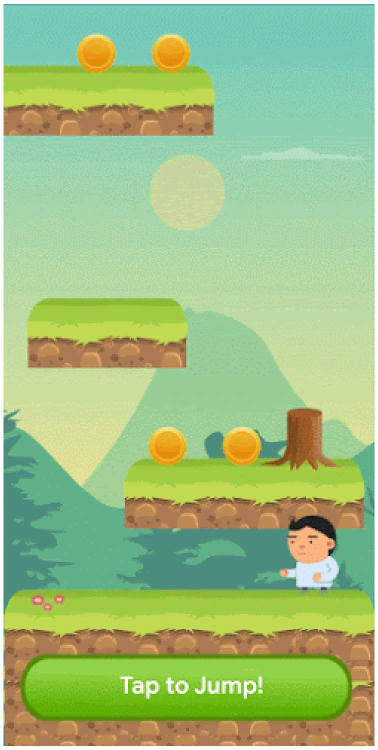
- ऐसे विज्ञापन जो पूरी स्क्रीन को घेर लेते हैं या सामान्य इस्तेमाल में रूकावट डालते हैं और विज्ञापन हटाने का सही तरीका नहीं बताते:

① इस विज्ञापन में 'खारिज करें' बटन नहीं है.

- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति को खारिज करने के गलत बटन पर क्लिक करने के लिए मजबूर करते हैं या ऐसी जगहों पर अचानक विज्ञापन दिखाते हैं जहां इस्तेमाल करने वाला व्यक्ति आम तौर पर दूसरी सुविधा के लिए टैप करता है.



ऐसा विज्ञापन जो खारिज करने के गलत बटन का इस्तेमाल करता है



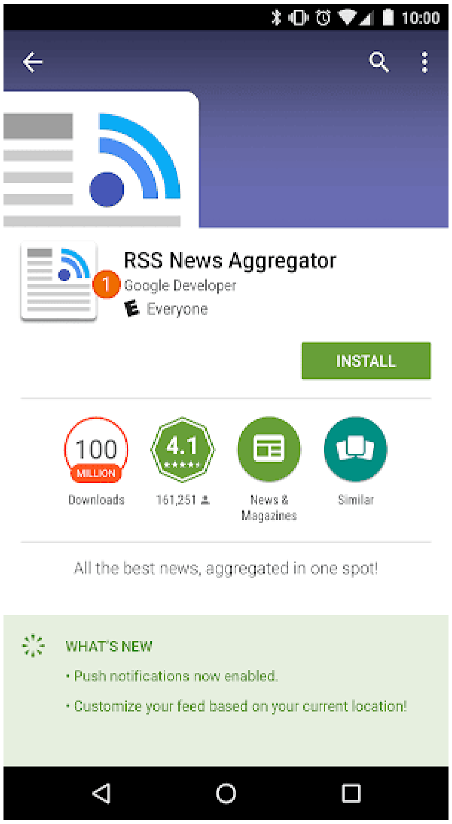
ऐसा विज्ञापन जो उस जगह पर अचानक दिखता है जहां ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति ऐप्लिकेशन की सुविधाओं के लिए आम तौर पर टैप करता है

ऐप्लिकेशन, तीसरे पक्ष के विज्ञापन या डिवाइस के काम करने के तरीके में दखल देना

आपके ऐप्लिकेशन के विज्ञापनों को दूसरे 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.

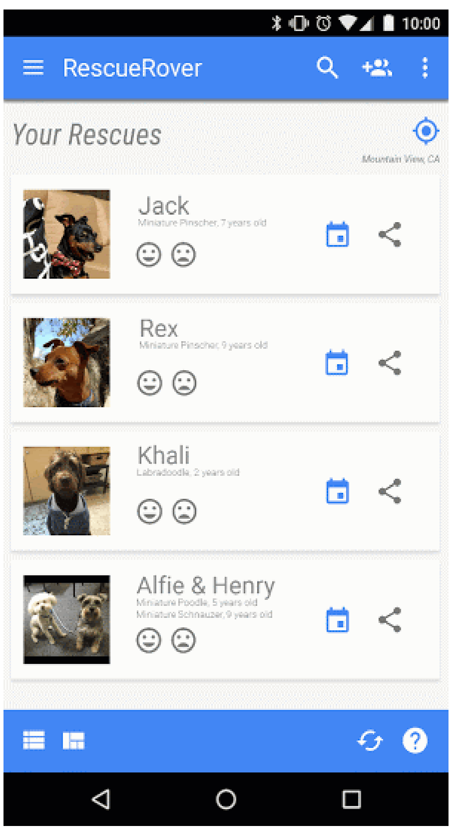
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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:

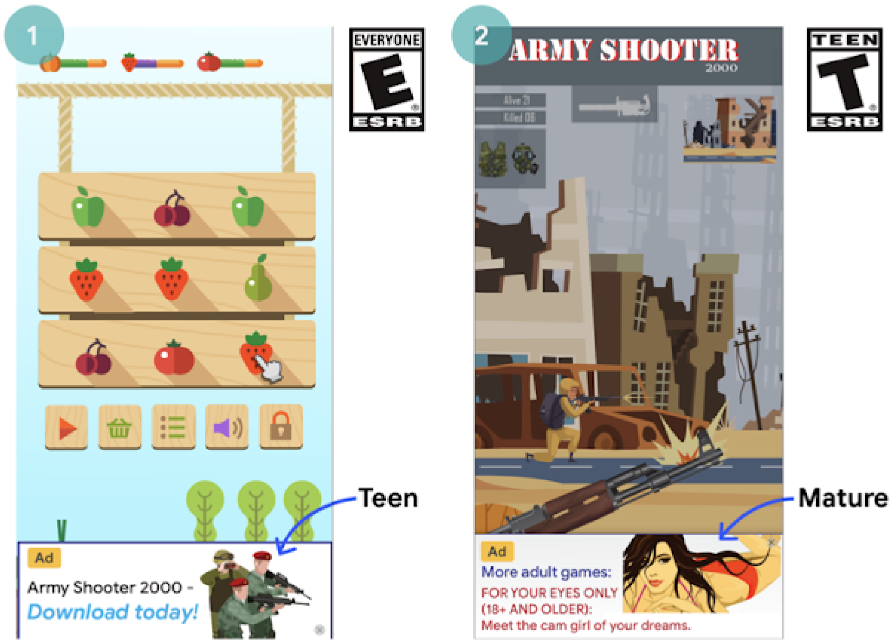


ब्यौरा: उपयोगकर्ता ऐप्लिकेशन से बाहर निकलने और होम स्क्रीन पर जाने की कोशिश करता है, लेकिन इसके बजाय, किसी विज्ञापन की वजह से ऐसा करने में रुकावट आ जाती है.

ऐसे विज्ञापन जो सही नहीं हैं

आपके ऐप्लिकेशन में दिखाए गए विज्ञापन उन दर्शकों के लिए सही होने चाहिए जिनके लिए यह ऐप्लिकेशन बनाया गया है. भले ही, कॉन्टेंट हमारी नीतियों का पालन करता हो.

यहां आम तौर पर होने वाले उल्लंघन का उदाहरण दिए गया हैं:



① यह विज्ञापन, ऐप्लिकेशन के टारगेट दर्शकों (किशोरों) के लिए सही नहीं है (7+)
② यह विज्ञापन, ऐप्लिकेशन के टारगेट दर्शकों (वयस्कों) के लिए सही नहीं है (12+)

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 आंकड़ों के लिए किया जाना चाहिए. हर बार आईडी ऐक्सेस करने पर, "पसंद के हिसाब से विज्ञापन से ऑप्ट-आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन से ऑप्ट-आउट करने" की सेटिंग की स्थिति की पुष्टि की जानी चाहिए.
- निजी रूप से पहचान करने लायक जानकारी या दूसरे पहचानकर्ता से जुड़ना
  - विज्ञापन का इस्तेमाल: विज्ञापन पहचानकर्ता, विज्ञापन के मकसद के लिए डिवाइस पहचानकर्ता से लगातार नहीं जुड़ सकता. उदाहरण के लिए: SSAID, MAC का पता, IMEI वगैरह. विज्ञापन पहचानकर्ता, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की साफ़ तौर पर सहमति के बाद ही, निजी रूप से पहचान करने लायक जानकारी के साथ जुड़ सकता है.
  - आंकड़ों का इस्तेमाल: विज्ञापन पहचानकर्ता ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की साफ़ तौर पर सहमति के बाद ही, निजी रूप से पहचान करने लायक जानकारी या किसी डिवाइस पहचानकर्ता के साथ लगातार जुड़ सकता है. उदाहरण के लिए: SSAID, MAC का पता, IMEI वगैरह.
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों 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 टारगेट करने के लिए विज्ञापन पहचानकर्ता का इस्तेमाल नहीं कर सकते. जिन गतिविधियों की अनुमति दी गई है उनमें कॉन्टेंट के हिसाब से विज्ञापन, फ़्रीक्वेंसी कैपिंग, कन्वर्ज़न ट्रैकिंग, रिपोर्टिंग और सुरक्षा, और धोखाधड़ी की पहचान करना शामिल है.
- ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए साफ़ तौर पर जानकारी देनी चाहिए. विज्ञापन पहचानकर्ता का संग्रह, इस्तेमाल, और इन शर्तों को पूरा करने के वादे को ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के सामने कानूनी रूप से सही निजता नोटिस के रूप में ज़ाहिर किया जाना चाहिए. निजता मानकों के बारे में ज़्यादा जानकारी के लिए, कृपया हमारे ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा की नीति देखें.
- इस्तेमाल करने 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 मकसद के लिए, किसी दूसरे डिवाइस पहचानकर्ता के बदले विज्ञापन आईडी (डिवाइस पर उपलब्ध होने पर) का इस्तेमाल करना होगा.

परिवार के लिए विज्ञापन कार्यक्रम

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 आपको Google Play की नीतियों के हिसाब से खुद प्रमाणित किया हुआ विज्ञापन SDK टूल इस्तेमाल करना होगा. 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 विज्ञापन SDK टूल से ही मिले हों. '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 को खुद को 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 ऐप्लिकेशन इस्तेमाल करने वाले की डेटा नीति और परिवार नीति का पालन करते हों:

- इन-हाउस विज्ञापन से आप SDK टूल का इस्तेमाल करके, आप अपने ऐप्लिकेशन या दूसरी मालिकाना हक वाली मीडिया और प्रचार के लिए बेची जाने वाली चीज़ों को प्रबंधित करने के लिए SDK टूल का इस्तेमाल 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. परिभाषाओं को Play की डेवलपर कार्यक्रम की नीतियों का पालन करना चाहिए.
- अपने विज्ञापन क्रिएटिव को रेट करने का ऐसा तरीका बनाएं जो उम्र के हिसाब से बने समूहों के मुताबिक हो. उम्र के हिसाब से बने समूहों में कम से कम 'सभी के लिए' और 'वयस्क' समूह शामिल हों. रेटिंग का तरीका उसी तरीके के मुताबिक होना चाहिए जो Google, SDK टूल को तब देता है, जब वे अपनी पसंद 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 लागू कानूनों और नियमों, जैसे कि यूएस चिल्ड्रन ऑनलाइन प्राइवेसी एंड प्रोटेक्शन एक्ट (कोपा) और ईयू (यूरोपीय संघ)सामान्य डेटा से जुड़े सुरक्षा कानून (जनरल डेटा प्रोटेक्शन रेगुलेशन) (जीडीपीआर) के मुताबिक होना चाहिए. Google Play को दर्शकों की पसंद को ध्यान में रखकर बनाए गए विज्ञापन, पसंद के हिसाब से बनाए गए विज्ञापन, और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव के तौर पर फिर से मार्केटिंग को बंद करने के लिए SDK टूल की ज़रूरत होती है.
- प्रकाशकों को ऐसे विज्ञापन फ़ॉर्मैट चुनने की अनुमति दें जो Play की परिवार विज्ञापन और कमाई करने की नीति का पालन करते हों और शिक्षकों से मंज़ूरी मिले ऐप्लिकेशन वाले कार्यक्रम की शर्तें पूरी करते हों.
- 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 हो और निजता बनाए रखने के संकेत, बोली लगाने वालों को दिए जाते हों.
- 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, इस तरह की जानकारी नीचे दिए गए पसंद बताने वाले फ़ॉर्म में दी गई 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 होते हैं.

बच्चों के लिए विज्ञापन दिखाते समय, इसकी सुविधा देने वाले प्लैटफ़ॉर्म के लिए मीडिएशन (मध्यस्थता) 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; और
- विज्ञापन की रेटिंग और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव दिखाने के लिए मीडिएशन प्लैटफ़ॉर्म को ज़रूरी जानकारी दें.

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

इसके साथ ही, डेवलपर पसंद बताने वाला फ़ॉर्म भी उन विज्ञापन SDK टूल के साथ शेयर कर सकते हैं जो खुद को प्रमाणित करना 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, हल्की 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 को अनुमति नहीं देते जो सीधे तौर पर या किसी और तरीके से लोगों या डेवलपर के साथ धोखाधड़ी करते हैं या उन्हें नुकसान पहुंचाते हैं. इसके अलावा, फ़ायदा लेने 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 से अनचाहा प्रचार करना.

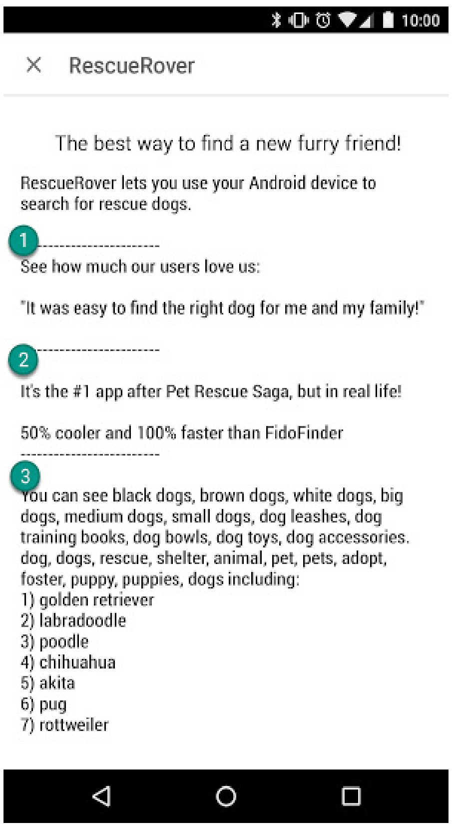
यह पक्का करना आपकी ज़िम्मेदारी है कि कोई भी विज्ञापन नेटवर्क कंपनी या आपके ऐप्लिकेशन के सहयोगी इन नीतियों का पालन करते हों. साथ ही, प्रचार करने के लिए किसी भी पाबंदी वाले तरीके का इस्तेमाल नहीं करते हों.

मेटाडेटा

हम उन ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह करने वाला, गलत तरीके से फ़ॉर्मैट किया गया, बिना किसी जानकारी वाला, ग़ैर-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 ही तक सीमित नहीं है. डेवलपर को अपने ऐप्लिकेशन के बारे में साफ़ और सही तरीके से जानकारी लिखनी चाहिए. हम ऐप्लिकेशन की जानकारी में बिना एट्रिब्यूशन वाले या पहचान छिपाने वाले उपयोगकर्ता टेस्टीमोनियल की अनुमति नहीं देते हैं.

यहां बताई गई ज़रूरी शर्तों के अलावा, Play की खास डेवलपर नीतियों के लिए आपको मेटाडेटा की और भी जानकारी देने की ज़रूरत हो सकती है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:



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 होता है. 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. भले ही, उसे चित्र या असल रूप में दिखाया गया हो.
- अपने ऐप्लिकेशन के स्टोर पेज में गलत, अश्लील या ऐसी किसी दूसरी भाषा का इस्तेमाल करना जो आम दर्शकों के लिए सही नहीं है.
- 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 ईडीएसए (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.

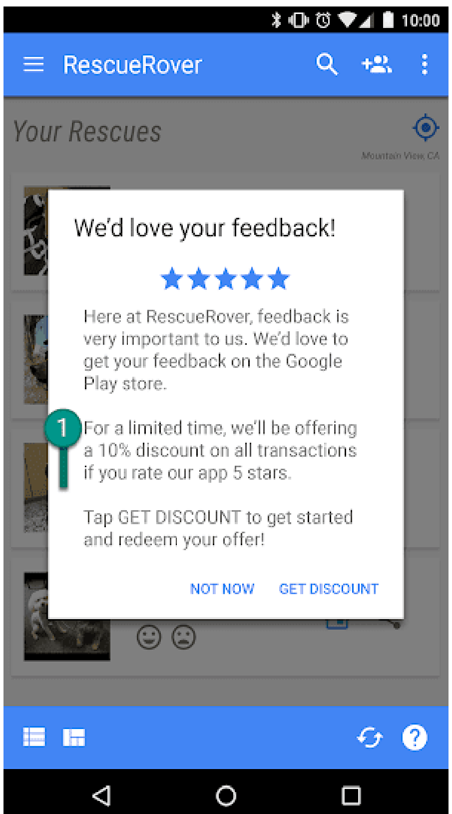
- अपने ऐप्लिकेशन की जानकारी कम और आसान शब्दों में दें. कम शब्दों में जानकारी का मकसद, खास तौर पर छोटे डिसप्ले वाले डिवाइस पर बेहतरीन उपयोगकर्ता अनुभव देना है. हद से ज़्यादा लंबे, विवरण, गलत फ़ॉर्मैट या दोहराई जाने वाली जानकारी से, इस नीति का उल्लंघन हो सकता है.
- ध्यान रखें कि आपका स्टोर पेज, आम दर्शक 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.

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की रेटिंग, समीक्षाएं, और इंस्टॉल की संख्या

डेवलपर को Google Play में किसी भी ऐप्लिकेशन के प्लेसमेंट में बदलाव 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. हालांकि, यह इन ही चीज़ों तक सीमित नहीं है.

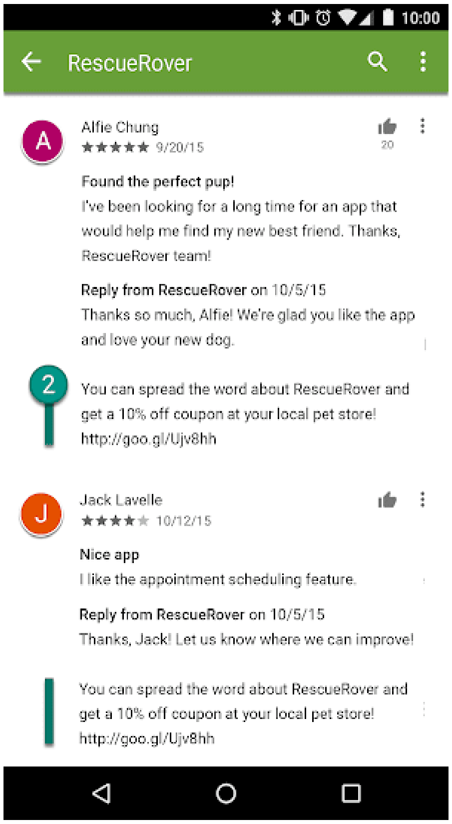
यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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.

कॉन्टेंट रेटिंग

Google Play पर कॉन्टेंट रेटिंग इंटरनैशनल एज रेटिंग कोअलिशन (आईएआरसी) देता है और इसे ऐप्लिकेशन इस्तेमाल करने वाले लोगों को स्थानीय रूप से सभी ज़रूरी कॉन्टेंट रेटिंग देने में डेवलपर की सहायता करने के लिए डिज़ाइन किया गया है. आधिकारिक क्षेत्रीय आईएआरसी ऐसे दिशा-निर्देश बनाए रखते हैं जिनका इस्तेमाल ऐप्लिकेशन में कॉन्टेंट के समझदारी स्तर को तय करने के लिए किया जाता है. हम Google Play पर बिना कॉन्टेंट रेटिंग वाले ऐप्लिकेशन को अनुमति नहीं देते हैं.

कॉन्टेंट रेटिंग का इस्तेमाल किस तरह 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 Console में रेटिंग से जुड़े सवालों की सूची भरनी होगी. इसमें यह पूछा जाता है कि आपके ऐप्लिकेशन का कॉन्टेंट कैसा है. सवालों की सूची में दिए गए जवाबों के मुताबिक, आपके ऐप्लिकेशन को अलग-अलग रेटिंग प्राधिकरणों की तरफ़ से कॉन्टेंट रेटिंग दी जाएगी. आपके ऐप्लिकेशन के कॉन्टेंट को गलत तरीके से पेश करने की वजह से ऐप्लिकेशन को हटाया जा सकता है या उस पर कुछ देर के लिए रोक लगाई जा सकती है. इसलिए, कॉन्टेंट रेटिंग से जुड़े सवालों की सूची में सही जवाब देना ज़रूरी है.

अपने ऐप्लिकेशन को "बगैर रेटिंग वाला" सूची में शामिल होने से रोकने के लिए, आपको Play Console 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 पर पहले से मौजूद सभी ऐप्लिकेशन के लिए भी ज़रूरी है.

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 Console में कॉन्टेंट रेटिंग से जुड़े सवालों की नई सूची सबमिट करनी होगी.

अलग-अलग रेटिंग प्राधिकरणों के बारे में ज़्यादा जानकारी पाने 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 आप अपने प्रमाणपत्र ईमेल में दिए गए लिंक का इस्तेमाल करके सीधे आईएआरसी रेटिंग प्राधिकरण में अपील कर सकते हैं.

समाचार

ऐसे ऐप्लिकेशन जो 'समाचार' कैटगरी चुनते हैं, लेकिन ऐसा कॉन्टेंट दिखाते हैं जो इन ज़रूरी शर्तों को पूरा नहीं करता उन्हें 'Play स्टोर' की समाचार कैटगरी में रखे जाने की अनुमति नहीं है. ऐसे समाचार ऐप्लिकेशन जिनका इस्तेमाल करने के लिए किसी व्यक्ति को सदस्यता खरीदने की ज़रूरत होती है उन्हें खरीदारी से पहले लोगों को कॉन्टेंट की एक झलक दिखानी चाहिए.

समाचार ऐप्लिकेशन के लिए ज़रूरी है कि वे:

- समाचार प्रकाशक और इसमें योगदान देने वालों के बारे में पूरी जानकारी दें. इसमें मालिकाना हक की जानकारी भी शामिल है और
- उनकी एक वेबसाइट या इन-ऐप्लिकेशन पेज हो, जिसमें समाचार प्रकाशकों की सही संपर्क जानकारी दी गई हो.

समाचार ऐप्लिकेशन में:

- स्पेलिंग और व्याकरण की मुख्य गड़बड़ियां नहीं होनी चाहिए,
- सिर्फ़ स्टैटिक कॉन्टेंट नहीं होना चाहिए, और
- इनका मुख्य मकसद अफ़िलिएट मार्केटिंग या विज्ञापन से पैसे कमाना नहीं होना चाहिए.

समाचार एग्रीगेटर ऐप्लिकेशन को प्रकाशित होने वाले कॉन्टेंट के स्रोत के बारे में साफ़ तौर पर जानकारी देनी चाहिए. साथ ही, हर एक स्रोत को समाचार नीति की ज़रूरी शर्तों को पूरा करना चाहिए.

स्पैम और कम से कम सुविधाएं

कम से कम, ऐप्लिकेशन के ज़रिए उपयोगकर्ताओं को बुनियादी सुविधाओं के साथ-साथ बेहतर अनुभव देना चाहिए. जिन ऐप्लिकेशन का मकसद लोगों या Google Play को सिर्फ़ स्पैम भेजना होता है उनका कैटलॉग सही तरीके से बड़ा नहीं होता. ऐसा उन ऐप्लिकेशन के साथ भी होता है जो अचानक बंद हो जाते हैं या इस तरह से काम करते हैं कि ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को अच्छा अनुभव नहीं मिल पाता.

स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते 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 हल्की होती है.

मैसेज स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो इस्तेमाल करने वाले व्यक्ति को कॉन्टेंट और चुने हुए लोगों की पुष्टि करने की सुविधा दिए बिना, उनकी तरफ़ से मैसेज (एसएमएस), ईमेल या अन्य मैसेज भेजते हैं.

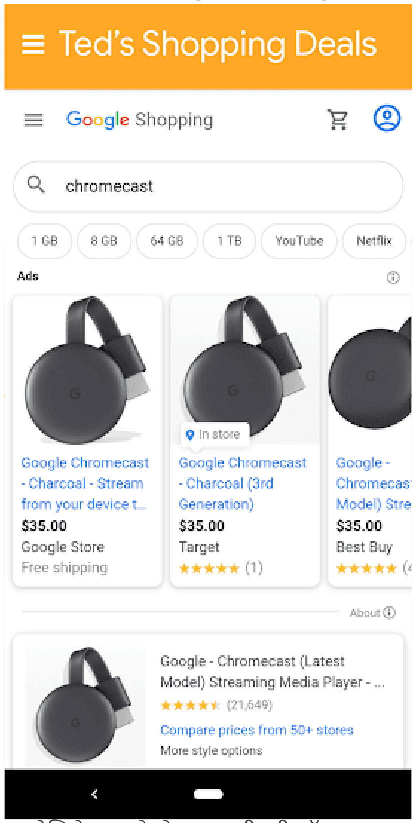
वेबव्यू और उससे जुड़े स्पैम

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनका मुख्य मकसद अफ़िलिएट ट्रैफ़िक को किसी वेबसाइट पर भेजना या किसी वेबसाइट का वेबव्यू उस वेबसाइट के मालिक या एडमिन की मंज़ूरी के बिना दिखाना हो.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसा ऐप्लिकेशन जिसका मुख्य मकसद रेफ़रल ट्रैफ़िक को किसी वेबसाइट पर भेजना होता है, ताकि उस वेबसाइट पर इस्तेमाल करने वाले व्यक्ति के साइन-अप या खरीदारी करने से क्रेडिट पा सके.

- ऐसे ऐप्लिकेशन जिनका मुख्य मकसद अनुमति के बिना किसी वेबसाइट का वेबव्यू दिखाना होता है:



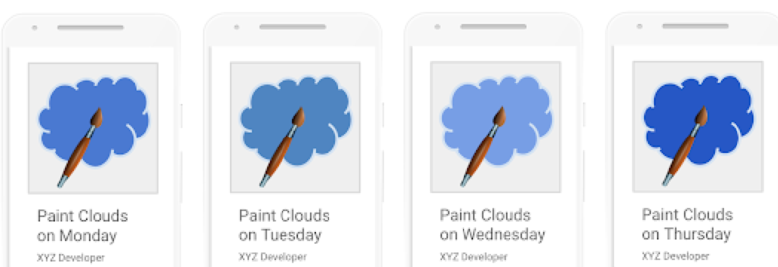
इस ऐप्लिकेशन को "टेड का खरीदारी ऑफ़र" कहा जाता है और यह Google Shopping का वेबव्यू दिखाता है.

बार-बार एक ही तरह का कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते 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.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- कोई मूल कॉन्टेंट या उसमें कुछ नया जोड़े बिना दूसरे ऐप्लिकेशन से कॉन्टेंट की नकल 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.



विज्ञापन के लिए बनाए गए ऐप्लिकेशन

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनका मुख्य मकसद विज्ञापन दिखाना है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जिन पर इस्तेमाल करने वाले व्यक्ति की हर कार्रवाई के बाद, पेज पर अचानक दिखने वाले विज्ञापन आ जाते हैं. इनमें क्लिक, स्वाइप वगैरह शामिल हैं. हालांकि, यह इन ही तक सीमित नहीं है.

कम से कम सुविधाएं

पक्का करें कि आपका ऐप्लिकेशन भरोसेमंद, दिलचस्प, और इस्तेमाल करने वाले व्यक्ति को बेहतर अनुभव देता हो.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

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

अधूरी सुविधाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो बीच में रुक जाते हैं, ज़बरदस्ती बंद हो जाते हैं, फ़्रीज़ हो जाते हैं या फिर असामान्य तरीके से काम करते हैं.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- 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

दूसरे प्रोग्राम

Android के दूसरे अनुभवों के लिए डिज़ाइन किए गए और Google Play उपलब्ध ऐप्लिकेशन को इस नीति केंद्र में कहीं और बताई गई सामग्री नीतियों का पालन करना होगा. इसके अलावा, उन पर प्रोग्राम के लिए खास तौर पर बनी ज़रूरी नीतियां भी लागू हो सकती हैं. यह तय करने के लिए नीचे दी गई सूची की समीक्षा करें कि क्या इनमें से कोई नीति आपके ऐप्लिकेशन पर लागू होती है.

Android Instant Apps

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 लोगों 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 लोगों को किसी झटपट ऐप्लिकेशन तक ले जा सकते हैं, तो डेवलपर को अपने ऐप्लिकेशन के वेबव्यू में दूसरे लिंक नहीं दिखाने चाहिए. डेवलपर के लिए ज़रूरी है कि वह ऐसे तरीके इस्तेमाल करने के बजाय, लोगों 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 इंस्टॉल करने लायक ऐप्लिकेशन ऑफ़र कर सकता है, लेकिन यह झटपट ऐप्लिकेशन का प्राथमिक उद्देश्य 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.
- लोगों को किसी ऐप्लिकेशन को इंस्टॉल करने का अनुरोध दिखाने के लिए, बैनर या विज्ञापन जैसी दूसरी तकनीक का इस्तेमाल नहीं करना चाहिए.

झटपट ऐप्लिकेशन के बारे में ज़्यादा जानकारी और UX से जुड़े दिशा-निर्देश ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को बेहतर अनुभव देने के सबसे सही तरीके पर जा कर देखे जा सकते हैं.

डिवाइस की स्थिति में बदलाव करना

Instant Apps 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, Instant apps उपयोगकर्ता का वॉलपेपर नहीं बदल सकते हैं या कोई होमस्क्रीन विजेट नहीं बना सकते हैं.

ऐप्लिकेशन की विज़िबिलिटी

डेवलपरों को यह पक्का करना चाहिए कि उपयोगकर्ताओं को instant apps इस तरह दिखाई दें, कि उपयोगकर्ता को हर समय यह पता रहे कि उसके डिवाइस पर झटपट ऐप्लिकेशन चल रहा है.

डिवाइस पहचानकर्ता

Instant Apps ऐसे डिवाइस पहचानकर्ता ऐक्सेस करने से प्रतिबंधित करते हैं जो (1) झटपट ऐप्लिकेशन चलना बंद होने के बाद भी बने रहते हैं और (2) जिन्हें उपयोगकर्ता फिर से सेट नहीं कर सकता है. नीचे इनके उदाहरण दिए जा रहे हैं, लेकिन ये इन ही तक सीमित नहीं हैं:

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

अगर फ़ोन नंबर रनटाइम अनुमति के दौरान मिला है, तो Instant Apps उसे ऐक्सेस कर सकते हैं. डेवलपर को इन पहचानकर्ताओं या दूसरे किसी भी तरीके का उपयोग 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.

परिवार

Google Play, डेवलपर के लिए ऐसा बेहतरीन प्लैटफ़ॉर्म मुहैया कराता है जहां वे अपना कॉन्टेंट दिखा कर बता सकें कि वह अच्छी क्वालिटी का, हर उम्र के मुताबिक, और पूरे परिवार के हिसाब से सही है. किसी ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम में सबमिट करने से पहले या फिर बच्चों को टारगेट करने वाला ऐप्लिकेशन 'Google Play स्टोर' में सबमिट करने से पहले, यह तय करना आपकी ज़िम्मेदारी है कि आपका ऐप्लिकेशन बच्चों के लिए सही है और सभी संबंधित कानूनों का पालन करता है.

Academy for App Success पर जाएं और परिवार से जुड़ी प्रोसेस के बारे में जानें. साथ ही, आप इसकी इंटरैक्टिव चेकलिस्ट भी देख सकते हैं.

बच्चों और परिवार के लिए ऐप्लिकेशन बनाना

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 का कॉन्टेंट खोज रहे हैं. हो सकता है कि आप ख़ास 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 जुड़ी पाबंदी लागू हो सकती है. 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 हों.

ख़ास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा लेना चाहिए. अगर आपका ऐप्लिकेशन बच्चों और बड़ों, दोनों तरह के दर्शकों को टारगेट करता है, तब भी आप 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा ले सकते हैं. 'परिवार के लिए बनाए गए' कार्यक्रम में ऑप्ट-इन करने वाले सभी लोगों को शिक्षकों से मंज़ूरी मिले ऐप्लिकेशन वाले कार्यक्रम के लिए रेट किया जा सकता है. हालांकि, हम गारंटी नहीं दे सकते कि आपका ऐप्लिकेशन शिक्षकों से मंज़ूरी मिले ऐप्लिकेशन वाले कार्यक्रम में शामिल हो होगा. अगर आप 'परिवार के लिए बनाए गए' कार्यक्रम में हिस्सा नहीं लेते हैं, तब भी आपको नीचे दी गई Google Play की परिवार के लिए बनाई गई नीति का पालन करना होगा. साथ ही, आपको Google Play डेवलपर कार्यक्रम की नीतियों और डेवलपर वितरण अनुबंध 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 को चुनना होगा. 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 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 शिशुओं, छोटे बच्चों, और प्री-स्कूल में पढ़ने वाले बच्चों के लिए है, तो उम्र समूह को टारगेट करते समय "पांच साल और उससे कम" उम्र का समूह ही चुनना चाहिए. अगर आपका ऐप्लिकेशन स्कूल के किसी ख़ास लेवल के लिए बनाया गया है, तो वह उम्र समूह चुनें जो उस स्कूल लेवल के लिए 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 को अपडेट कर सकते हैं. 'Google Play स्टोर' पर यह जानकारी दिखाने से पहले ऐप्लिकेशन अपडेट करना 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

'टारगेट ऑडियंस और सामग्री' सेक्शन के साथ ही, Play Console में आपके ऐप्लिकेशन के बारे में किसी जानकारी को गलत तरीके से पेश करने की वजह से आपका खाता हटाया या निलंबित किया जा सकता है. इसलिए, सही जानकारी देना ज़रूरी है.

परिवार नीति की ज़रूरतें

अगर आपके ऐप्लिकेशन के टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो आपको आगे दी गई ज़रूरतों का पालन करना चाहिए. इन शर्तों को पूरा नहीं करने पर ऐप्लिकेशन को हटाया या निलंबित किया जा सकता है.

1. ऐप्लिकेशन का कॉन्टेंट: आपके ऐप्लिकेशन का ऐसा 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:
    - ऐसे लोगों को विज्ञापन दिखाने के लिए, सिर्फ़Google Play से प्रमाणित किए गए विज्ञापन SDK टूल का इस्तेमाल करें;
    - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में, पसंद के हिसाब से विज्ञापन (ऑनलाइन ब्राउज़िंग व्यवहार के हिसाब से अलग-अलग लोगों को टारगेट करके दिखाए जाने वाले विज्ञापन) या रीमार्केटिंग (किसी ऐप्लिकेशन या वेबसाइट के साथ पिछले इंटरैक्शन के आधार पर अलग-अलग लोगों को टारगेट करने वाले विज्ञापन) शामिल नहीं हो;
    - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों का कान्टेंट बच्चों के लिए सही हो;
    - यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों में ऐसा कॉन्टेंट है जो परिवार के लिए बनाए गए विज्ञापन फ़ॉर्मेट की शर्तें पूरी करती है; और
    - यह भी पक्का करें कि बच्चों को विज्ञापन दिखाने से जुड़े सभी कानूनी नियमों और उद्योग मानकों का पालन हो.
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 की मदद से ली जाने वाले मिलने 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. हालांकि, ये इन ही तक सीमित नहीं है.
5. एपीआई और **SDK** टूल: आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन हर एपीआई और SDK टूल को सही तरीके से लागू करे.
    - सिर्फ़ बच्चों को टारगेट करने वाले ऐप्लिकेशन में ऐसा 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.
    - जिन ऐप्लिकेशन का टारगेट बच्चे और बड़े, दोनों तरह के दर्शक हैं उन्हें ऐसे एपीआई या SDK टूल लागू नहीं करने चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी नहीं मिली है. इन्हें तभी लागू किया जा सकता है, जब ये न्यूट्रल एज स्क्रीनके तहत इस्तेमाल किए जाते हों. इसके अलावा, इन्हें ऐसे तरीके से लागू न किया जाए जिससे बच्चों का डेटा इकट्ठा हो. जैसे कि Google साइन-इन की सुविधा को विकल्प को तौर पर देना. जिन ऐप्लिकेशन का टारगेट बच्चे और बड़े, दोनों तरह के दर्शक हैं उन्हें ऐसे एपीआई या SDK टूल से लोगों को साइन इन या कॉन्टेंट ऐक्सेस करने के लिए नहीं कहना चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी नहीं मिली है.
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 करने 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 होगी. 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. कानून का पालन: आपको यह पक्का करना होगा कि आपके ऐप्लिकेशन के साथ ही, ऐसे सभी एपीआई या SDK टूल जिनकी मांग या इस्तेमाल आपका ऐप्लिकेशन करता है, वह अमेरिका में लागू बच्चों की ऑनलाइन निजता और संरक्षण नियम (कोपा), ईयू (यूरोपीय संघ) में लागू सामान्य डेटा से जुड़े सुरक्षा कानून (जीडीपीआर), और किसी भी अन्य लागू कानून या नियम का पालन करता है.

यहां आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं:

- ऐसे ऐप्लिकेशन जो अपने स्टोर पेज में बच्चों के लिए खेल का प्रचार करते हैं, लेकिन ऐप्लिकेशन का कॉन्टेंट सिर्फ़ वयस्कों के लिए सही होता है.
- ऐसे ऐप्लिकेशन जो एपीआई को सेवा की ऐसी शर्तों के साथ लागू करते 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 जिन पर सरकार का कंट्रोल होता 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 यौन या शादीशुदा ज़िंदगी से जुड़ी सलाह देते हैं.
- ऐसे ऐप्लिकेशन जिनमें उन वेबसाइटों के लिंक होते हैं जो Google Play कीडेवलपर कार्यक्रम नीतियों का उल्लंघन करने वाले कॉन्टेंट को पेश करते हैं.
- ऐसे ऐप्लिकेशन जो बच्चों को बड़ों के लिए बनाए गए विज्ञापन दिखाते हैं. जैसे कि हिंसक कॉन्टेंट, यौन सामग्री, जुआ खेलने से जुड़ा कॉन्टेंट. बच्चों के लिए विज्ञापन, इन-ऐप्लिकेशन खरीदारी, और व्यावसायिक कॉन्टेंट पर Google Play की नीतियों के बारे में ज़्यादा जानकारी के लिए कृपया,परिवार के लिए विज्ञापन और कमाई करने की नीतियां देखें.

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 के साथ ही, सभी उम्र के लिए बनाया गया 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 वितरण अनुबंध 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 पालन करना होगा. Google Play किसी भी ऐप्लिकेशन को 'परिवार के लिए बनाए गए' कार्यक्रम के लिए गलत पाए जाने पर, उसे खारिज कर सकता है, हटा सकता है या निलंबित कर सकता 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 Speech API 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 का इस्तेमाल करना चाहिए.
5. खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन, जगह की जानकारी की अनुमतियां नहीं मांग सकते.
6. ब्लूटूथ कनेक्शन का अनुरोध करते समय ऐप्लिकेशन के लिए, 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.

यहां कुछ ऐसे सामान्य ऐप्लिकेशन के उदाहरण दिए गए हैं जिन्हें कार्यक्रम में हिस्सा लेने की अनुमति नहीं है:

- ऐसे ऐप्लिकेशन जिन्हें 'ईएसआरबी सभी' रेटिंग दी गई है, लेकिन उनमें जुए के कॉन्टेंट से जुड़े 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 डिवाइस प्रबंधन करने वाले ऐसे ऐप्लिकेशन जिनका इस्तेमाल सिर्फ़ माता-पिता या देखभाल करने वाले लोग ही कर सकते हैं
- ऐप्लिकेशन, जो ऐसे ऐप्लिकेशन आइकॉन और लॉन्चर आइकॉन का इस्तेमाल करते हैं जो बच्चों के लिए सही नहीं हैं

कैटगरी

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 वाले व्यक्ति 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.

क्रिएटिविटी: ऐसे ऐप्लिकेशन और गेम जो क्रिएटिविटी को बढ़ावा देते हैं. इनमें ड्रॉइंग, पेंटिंग, कोडिंग, और दूसरे 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 का बढ़ावा मिल सके. इनमें शैक्षणिक, सामाजिक-भावनात्मक, शारीरिक, और रचनात्मक तरीके से सीखना शामिल है. 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 व्यक्ति कोई किरदार निभा सकता है. जैसे कि शेफ़, देखभाल करने वाले, राजकुमार/राजकुमारी, फ़ायर फ़ाइटर, पुलिसकर्मी या किसी काल्पनिक किरदार की भूमिका निभाना.

विज्ञापन और कमाई करना

नीचे दी गई नीतियां किसी भी तरह के विज्ञापन (जिसमें आपके ऐप्लिकेशन और तीसरे पक्षों के लिए विज्ञापन शामिल हैं), इन-ऐप्लिकेशन ख़रीदारी के ऑफ़र या किसी भी दूसरे 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/या 'परिवार के लिए बनाए गए' कार्यक्रम की ज़रूरी शर्तें लागू होती हैं. इन ऐप्लिकेशन में दिखाए जाने वाले सभी तरह के विज्ञापन, इन-ऐप्लिकेशन ख़रीदारी के ऑफ़र, और व्यावसायिक कॉन्टेंट को इन पर लागू होने वाले सभी कानूनों और नियमों (इनमें खुद लागू किए गए नियम या उद्योग से जुड़े दिशा-निर्देश शामिल हैं) का पालन करना ज़रूरी है.

Google Play के पास व्यावसायिक फ़ायदे के लिए बहुत ज़्यादा आक्रामक विज्ञापन दिखाने वाले ऐप्लिकेशन को खारिज करने या हटाने का अधिकार होता है.

विज्ञापन फ़ॉर्मैट की शर्तें

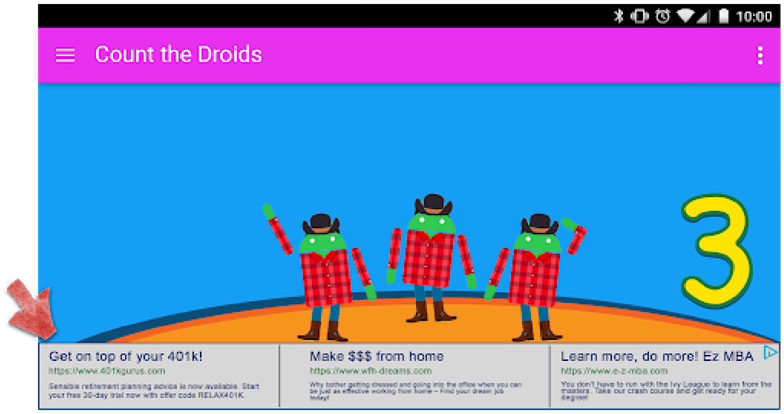
विज्ञापनों और इन-ऐप्लिकेशन ख़रीदारी के ऑफ़र देने वाले कॉन्टेंट को गुमराह करने वाला नहीं होना चाहिए. साथ ही, उन्हें इस तरह से डिज़ाइन किया जाए कि बच्चे अनजाने में क्लिक न करें. नीचे दी गई चीज़ों पर पाबंदी है:

- परेशान करने वाले विज्ञापन में ऐसे विज्ञापन शामिल हैं जो पूरी स्क्रीन को घेर लेते हैं या सामान्य इस्तेमाल में रूकावट डालते हैं और विज्ञापन हटाने का तरीका भी सही से नहीं बताते हैं. (उदाहरण के लिए, विज्ञापन वॉल)
- ऐसे विज्ञापन जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट डालते हैं और इन्हें पांच सेकंड के बाद बंद भी नहीं किया जा सकता. ऐसे विज्ञापन जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट नहीं डालते हैं, लेकिन ये पांच सेकंड के बाद भी चलते रहते हैं (जैसे कि विज्ञापन से जुड़ा हुआ वीडियो कॉन्टेंट).
- पेज पर अचानक दिखने वाले विज्ञापन या इन-ऐप्लिकेशन ख़रीदारी के ऐसे ऑफ़र जो ऐप्लिकेशन लॉन्च होते ही दिखते हैं
- पेज पर एक से ज़्यादा विज्ञापन प्लेसमेंट (उदाहरण के लिए, ऐसे बैनर विज्ञापन जो एक प्लेसमेंट में एक से ज़्यादा ऑफ़र दिखाते हैं या एक से ज़्यादा बैनर या वीडियो विज्ञापन दिखाते हैं, जिसकी अनुमति नहीं है).
- ऐसे विज्ञापन या इन-ऐप्लिकेशन ख़रीदारी 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 ख़रीदारी को बढ़ाने के लिए, भावनात्मक रूप से गुमराह करने या चौंकाने वाले तरीकों का इस्तेमाल करना
- इन-ऐप्लिकेशन ख़रीदारी करने के लिए, वर्चुअल गेम के सिक्कों और असली पैसों के बीच फ़र्क़ न दिखाना

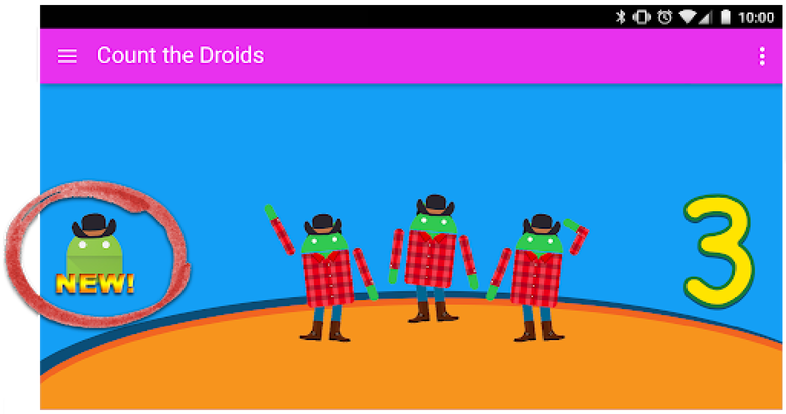
यहां विज्ञापन फ़ॉर्मैट के आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण दिए गए हैं

- 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:

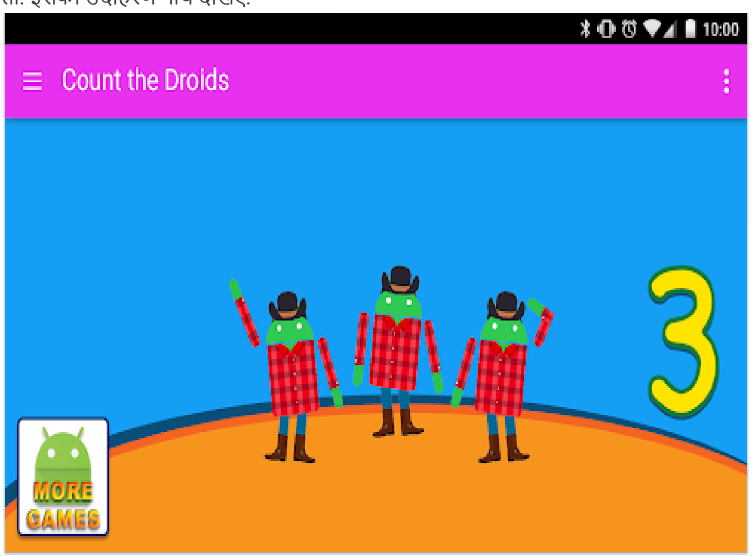
- ऐसे बैनर विज्ञापन जिनमें एक से ज़्यादा ऑफ़र दिखाए जा रहे हों. इसका उदाहरण नीचे देखिए:



- 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, फ़िल्मों, 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

अगर आप अपने ऐप्लिकेशन में विज्ञापन दिखाते हैं और आपकी टारगेट ऑडियंस में सिर्फ़ बच्चे शामिल हैं, तो आपको Google Play से प्रमाणित विज्ञापन SDK टूल का इस्तेमाल करना होगा. अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस बच्चे और वयस्क दोनों हैं, तो आपको स्क्रीन से जुड़े हुए मानकों का पालन करना चाहिए, जैसे कि न्यूट्रल एज स्क्रीन. साथ ही, यह पक्का करना चाहिए कि बच्चों को दिखाए जाने वाले विज्ञापनों में Google Play के प्रमाणित विज्ञापन SDK टूल का इस्तेमाल हो. '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.

ज़रूरी शर्तों के बारे में जानने और मंज़ूरी पा चुके 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 जानकारी के लिए AdMob सहायता केंद्र देखें.

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 कॉन्टेंट नीतियों और विज्ञापन देने के तौर-तरीकों के बारे में ज़्यादा जानने के लिए, उनसे संपर्क करें.

इन-ऐप्लिकेशन 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.

नीति उल्लंघन ठीक करने के तरीके

नीति उल्लंघन का प्रबंधन करने के बजाय, उससे बचना हमेशा बेहतर होता है. हालांकि, नीति का उल्लंघन होने पर, यह हमारी ज़िम्मेदारी होती है कि हम डेवलपर को यह बताएं कि वे अपने ऐप्लिकेशन को नीतियों के हिसाब से कैसे बना सकते हैं. अगर आपको कोई कोई उल्लंघन दिखता है या उल्लंघन को प्रबंधित करने के बारे में आपके सवाल हैं, तो कृपया हमें बताएं.

नीति 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 अनुमति नहीं देते जो लोगों को उनके डिवाइस पर दूसरे ऐप्लिकेशन इंस्टॉल करने की अनुमति देते हैं. ऐसे ऐप्लिकेशन जो इंस्टॉल किए बिना दूसरे ऐप्लिकेशन, गेम या सॉफ़्टवेयर को ऐक्सेस देते हैं उन्हें यह पक्का करना चाहिए कि पूरा कॉन्टेंट Google Play की नीतियों का पालन करता हो. साथ ही, उस पर नीति की अन्य समीक्षाएं लागू हो सकती हों. 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.

Google Play में किसी ऐप्लिकेशन को रखना है या हटाना है, इसके लिए हम गलत इस्तेमाल के ज़्यादा खतरे जैसी कई दूसरी वजहों के आधार पर कार्रवाई कर सकते हैं. हालांकि, ये इन ही तक सीमित नहीं है. हम पहले हुए उल्लंघन की जानकारी, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के शिकायत, सुझाव, और राय के साथ ही, लोकप्रिय ब्रैंड की मदद से बुरा बर्ताव होने के खतरे की पहचान करते हैं. इसके अलावा, ऐप्लिकेशन की खास बातें और अन्य एसेट जैसी अलग-अलग चीज़ों का इस्तेमाल भी किया जाता है. हालांकि, ये इन ही तक सीमित नहीं है.

Google Play Protect कैसे काम करता है

Google Play Protect, ऐप्लिकेशन डाउनलोड करने पर उनकी जांच करता है. यह समय-समय पर आपका डिवाइस भी स्कैन करता है. नुकसान पहुंचा सकने वाला कोई ऐप्लिकेशन मिलने पर, यह ये काम कर सकता है:

- आपको सूचना भेज सकता है. ऐप्लिकेशन हटाने के लिए सूचना और उसके बाद 'अनइंस्टॉल करें' पर टैप करें.
- ऐप्लिकेशन को तब तक के लिए बंद कर सकता है, जब तक कि आप इसे अनइंस्टॉल नहीं कर देते.
- ऐप्लिकेशन को अपने-आप हटा सकता है. ज़्यादातर मामलों में, अगर किसी नुकसान पहुंचाने वाले ऐप्लिकेशन के होने का पता चलता है, तो आपको सूचना मिलेगी कि ऐप्लिकेशन को हटा दिया गया है.

मैलवेयर सुरक्षा कैसे काम करती है

आपके डिवाइस को नुकसान पहुंचाने वाले तीसरे पक्ष के सॉफ़्टवेयर, यूआरएल, और सुरक्षा से जुड़ी दूसरी समस्याओं से बचाव करने के लिए Google को यह जानकारी मिल सकती है:

- आपके डिवाइस के नेटवर्क कनेक्शन की जानकारी
- ऐसे यूआरएल की जानकारी जो आपके डिवाइस को नुकसान पहुंचा सकते हैं

- आपके डिवाइस पर Google Play या दूसरे स्रोतों से इंस्टॉल किए गए ऐप्लिकेशन और ऑपरेटिंग सिस्टम.

आपको Google से, किसी ऐसे ऐप्लिकेशन या यूआरएल के बारे में चेतावनी मिल सकती है जो शायद सुरक्षित न हो. अगर Google को लगता है कि डिवाइस, डेटा या लोगों के लिए ऐप्लिकेशन या यूआरएल सुरक्षित नहीं है, तो वह उसे हटा सकता है या इंस्टॉल होने से रोक सकता है.

आप अपने डिवाइस की सेटिंग में जाकर इन सुरक्षाओं में से कुछ को बंद करना चुन सकते हैं. हालांकि, Google को Google Play से इंस्टॉल किए गए ऐप्लिकेशन के बारे में जानकारी मिलनी जारी रह सकती है. साथ ही, आपके डिवाइस पर दूसरे स्रोतों से इंस्टॉल किए गए ऐप्लिकेशन की सुरक्षा समस्याओं के लिए जांच करना जारी रह सकता है. इसकी जानकारी Google को नहीं भेजी जाएगी.

निजता से जुड़ी चेतावनियां आपको कैसे मिलती हैं

अगर 'Google Play स्टोर' से किसी ऐप्लिकेशन को हटा दिया जाता है, तो Google Play Protect आपको चेतावनी भेजेगा. ऐसा इसलिए, क्योंकि ऐप्लिकेशन आपकी निजी जानकारी को ऐक्सेस करने की कोशिश कर सकता है. हालांकि, आपके पास ऐप्लिकेशन को अनइंस्टॉल करने का विकल्प होगा.

नीति उल्लंघन ठीक करने की प्रक्रिया

अगर आपका ऐप्लिकेशन हमारी किसी नीति का उल्लंघन करता है, तो हम सही कार्रवाई करेंगे, जैसा कि नीचे बताया गया है. इसके अलावा, हम जो कार्रवाई करेंगे उसकी जानकारी आपको ईमेल से भेज देंगे. साथ ही, अगर आपको लगता है कि हमने गलत कार्रवाई की है, तो हम अपील करने का तरीका बताएंगे.

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 न दिखाए. डेवलपर किसी भी फ़्लैग की गई नीति के मुद्दे को पता करने और उसे ठीक करने के लिए ज़िम्मेदार हैं और वह यह ध्यान से देख ले कि उसके ऐप्लिकेशन का बाकि बचा हिस्सा पूरी तरह से नीति का पालन करता हो. आपके सभी ऐप्लिकेशन में नीति उल्लंघन को हल न कर पाने पर, नीति उल्लंघन के तरीके ठीक करने के तहत कार्रवाई हो सकती है.

इन नीतियों या डेवलपर वितरण अनुबंध (DDA) से बार-बार होने वाले या गंभीर उल्लंघनों के नतीजे के बाद व्यक्तिगत या मिलते-जुलते खातों को खत्म कर दिया जाएगा. जैसे कि मैलवेयर, धोखाधड़ी, और उपयोगकर्ता या डिवाइस को नुकसान पहुंचाने वाले ऐप्लिकेशन.

नीति उल्लंघन ठीक करने के लिए कार्रवाईयां

नीति उल्लंघन ठीक करने की अलग-अलग कार्रवाइयां, आपके ऐप्लिकेशन पर अलग-अलग असर डाल सकती हैं. नीचे दिए गए सेक्शन में उन कार्रवाइयों की जानकारी दी गई है जो Google Play कर सकता है. साथ ही, यह जानकारी भी दी गई है कि इन कार्रवाइयों का आपके ऐप्लिकेशन या Google Play डेवलपर खाते पर क्या असर पड़ेगा. इस वीडियो में पूरी जानकारी दी गई है.

खारिज करना

- समीक्षा के लिए सबमिट किया गया नया ऐप्लिकेशन या ऐप्लिकेशन अपडेट Google Play पर उपलब्ध नहीं होगा.
- अगर किसी मौजूदा ऐप्लिकेशन के अपडेट को खारिज किया गया था, तो अपडेट से पहले प्रकाशित किया गया वर्शन अब भी Google Play पर मौजूद रहेगा.
- खारिज होने का असर, खारिज हुए ऐप्लिकेशन के मौजूदा स्टोर पेज, उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग देखने की सुविधा पर नहीं पड़ता.
- खारिज होने से आपके Google Play डेवलपर खाते की स्थिति पर असर नहीं होता है.

ध्यान दें: खारिज किए गए ऐप्लिकेशन को तब तक दोबारा सबमिट करने की कोशिश न करें, जब तक आप नीतियों के उल्लंघन को ठीक नहीं कर लेते हैं.

हटाना

- ऐप्लिकेशन और उसके पहले का कोई भी ऐसा वर्शन जिसे Google Play से हटा दिया गया है, लोगों के डाउनलोड करने के लिए उपलब्ध नहीं होगा.
- ऐप्लिकेशन को हटा दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े और रेटिंग नहीं देख पाएंगे. हटाए गए ऐप्लिकेशन में नीति का पालन करने वाला अपडेट करने पर जानकारी वापस आ जाएगी.
- जब तक Google Play नीति का पालन करने वाले वर्शन को मंज़ूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले सकते.
- ऐप्लिकेशन को कई बार हटाने से उस पर रोक लगा सकते हैं, लेकिन इसका असर आपके Google Play डेवलपर खाते की स्थिति पर तुरंत नहीं पड़ता.

ध्यान दें: हटाए गए ऐप्लिकेशन को तब तक दोबारा प्रकाशित करने की कोशिश न करें, जब तक आप सभी नीतियों के उल्लंघन को ठीक नहीं कर लेते हैं.

निलंबन

- ऐप्लिकेशन और उसके पहले का कोई भी ऐसा वर्शन जिसे Google Play से हटा दिया गया है, लोगों के डाउनलोड करने के लिए उपलब्ध नहीं होगा.
- नीति के बहुत खराब या एक से ज़्यादा बार उल्लंघन होने के साथ ही, कई बार खारिज होने या हटाने से ऐप्लिकेशन निलंबित हो सकता है.

- [मेरा ऐप्लिकेशन Google Play से हटा दिया गया है]
- [Google Play डेवलपर खाता बंद होने की वजह समझना]

इस लेख के बारे में सुझाव दें

क्या यह उपयोगी था?

हां नहीं

और मदद चाहिए?

आगे दिए गए कदमों को आज़माएं:

हमसे संपर्क करें

हमें ज़्यादा जानकारी दें और हम आपकी पूरी मदद करेंगे

- ऐप्लिकेशन को निलंबित कर दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े और रेटिंग नहीं देख पाएंगे. निलंबित ऐप्लिकेशन के लिए नीति का पालन करने वाला अपडेट करने पर जानकारी वापस आ जाएगी.
- अब आप निलंबित ऐप्लिकेशन का APK या ऐप्लिकेशन बंडल का इस्तेमाल नहीं कर सकते.
- जब तक Google Play नीति का पालन करने वाले वर्शन को मंज़ूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले पाएंगे.
- निलंबन को आपके Google Play डेवलपर खाते की अच्छी स्थिति के ख़िलाफ़ हमला माना जाता है. एक से ज़्यादा बार निलंबित होने पर आपका Google Play डेवलपर खाता और उससे जुड़े खाते बंद किए जा सकते हैं.

ध्यान दें: किसी निलंबित ऐप्लिकेशन को तब तक दोबारा प्रकाशित करने की कोशिश न करें, जब तक Google Play आपसे ऐसा करने के लिए न कहे.

ऐप्लिकेशन किसको दिखेगा, यह सीमित करना

- Google Play पर आपके ऐप्लिकेशन को खोजे जाने पर पाबंदी लगा दी गई है. आपका ऐप्लिकेशन Google Play पर उपलब्ध रहेगा और ऐप्लिकेशन के 'Play स्टोर" में दिए सीधे लिंक के साथ लोग इसे ऐक्सेस कर सकते है.
- ऐप्लिकेशन किसको दिखेगा, यह सीमित करने से आपके Google Play डेवलपर खाते की स्थिति पर असर नहीं पड़ता.
- ऐप्लिकेशन किसको दिखेगा, यह सीमित करने से लोगों के ऐप्लिकेशन के मौजूदा स्टोर पेज, उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग देखने की सुविधा पर असर नहीं पड़ता.

खाता बंद कर देना

- जब आपका डेवलपर खाता बंद कर दिया जाता है, तो आपकी सूची के सभी ऐप्लिकेशन को Google Play से हटा दिए जाएगा और आप नए ऐप्लिकेशन प्रकाशित नहीं कर पाएंगे. इसका मतलब यह भी है कि सभी Google Play डेवलपर से जुड़े हुए सभी खातों को भी हमेशा के लिए निलंबित कर दिया जाएगा.
- अगर आपको नीति का कई बार निलंबन या गंभीर उल्लंघन करने की वजह से निलंबित किया जाता है, तो आपका Play Console खाता बंद किया जा सकता है.
- बंद किए गए खाते को ऐप्लिकेशन से हटा दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टेर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े, और रेटिंग नहीं देख पाएंगे.

ध्यान दें: आप जिस नए खाते को खोलने की कोशिश करेंगे उसे भी बंद कर दिया जाएगा (डेवलपर रजिस्ट्रेशन शुल्क रिफ़ंड किए बिना). इसलिए, जब आपका कोई दूसरा खाता बंद कर दिया गया हो, तो कृपया किसी नए Play Console खाते के लिए रजिस्ट्रेशन करने की कोशिश न करें.

नीति के उल्लंघनों का प्रबंधन और उनकी शिकायत करना

ऐप्लिकेशन पर नीति उल्लंघन ठीक करने के तरीके की कार्रवाई के ख़िलाफ़ अपील करना

अगर कोई गड़बड़ी हुई हो और हमें पता चले कि आपका ऐप्लिकेशन Google Play कार्यक्रम नीतियों और डेवलपर वितरण अनुबंध का उल्लंघन नहीं करता है, तो हम ऐप्लिकेशन बहाल करेंगे. अगर आपने नीतियों की ध्यान से समीक्षा की है और आपको लगता है कि हमारे फ़ैसले में गड़बड़ी हुई है, तो कृपया अपील करने के लिए नीति उल्लंघन ठीक करने के तरीके बताने वाले ईमेल में नीचे दिए गए निर्देशों का पालन करें.

दूसरे संसाधन

अगर आपको किसी उपयोगकर्ता पर लागू कार्रवाई या रेटिंग/टिप्पणी से जुड़ी ज़्यादा जानकारी चाहिए, तो आप नीचे दिए गए कुछ संसाधनों को देख सकते हैं या Google Play सहायता केंद्र पर 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
- साफ़ तौर पर चेतावनी
- आपत्तिजनक ऐप्लिकेशन और टिप्पणियों की शिकायत करना