डेवलपर कार्यक्रम की नीतियां

(31 अगस्त, 2024 से लागू, जब तक अलग से निर्देश न दिए जाएं)

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

आपके नए ऐप्लिकेशन, आपकी और हमारी सफलता को आगे बढ़ाते हैं. हालांकि, इसके साथ नई ज़िम्मेदारियां भी आती हैं. डेवलपर कार्यक्रम की इन नीतियों और डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट से यह पक्का होता है कि हम साथ मिलकर Google Play की मदद से, दुनिया के सबसे अनोखे और भरोसेमंद ऐप्लिकेशन करोड़ों लोगों तक पहुंचाते रहेंगे. 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

ऐसे ऐप्लिकेशन Google Play से हटा दिए जाएंगे जो बच्चों के शोषण या उनके साथ बुरे बर्ताव को बढ़ावा देने वाला कॉन्टेंट तैयार करने, अपलोड करने या बेचने से उपयोगकर्ताओं को नहीं रोकते. इसमें बच्चों का यौन शोषण दिखाने वाला सभी तरह का कॉन्टेंट शामिल है. किसी भी Google प्रॉडक्ट पर मौजूद ऐसा कॉन्टेंट जो बच्चों के शोषण से जुड़ा हो सकता है, उसकी शिकायत करने के लिए, **बुरे बर्ताव की शिकायत करें** पर क्लिक करें. अगर आपको इंटरनेट पर कहीं भी ऐसा कॉन्टेंट मिलता है, तो कृपया अपने देश में मौजूद ऐसे मामलों से जुड़ी एजेंसी से सीधे संपर्क करें.

हम ऐप्लिकेशन के ऐसे इस्तेमाल पर पाबंदी लगाते हैं जिनसे बच्चों को खतरा हो सकता है. इसमें बच्चों के शोषण को बढ़ावा देने के लिए ऐप्लिकेशन का इस्तेमाल करने के अलावा, और भी चीज़ें शामिल हो सकती हैं, जैसे कि:

- किसी बच्चे से गलत व्यवहार करना. उदाहरण के लिए, गलत ढंग से छूना या सहलाना.
- यौन शोषण से पहले बच्चों को बहलाना-फुसलाना - उदाहरण के लिए, बच्चे के साथ ऑनलाइन दोस्ती करके, उनके साथ ऑनलाइन या ऑफ़लाइन यौन संबंध बनाने और/या उनके साथ अश्लील तस्वीरों का लेन-देन करना.
- नाबालिगों को अश्लील तरीके से दिखाने वाला कॉन्टेंट - उदाहरण के लिए, ऐसी तस्वीरें जो बच्चों का यौन शोषण दिखाती हों, उसे बढ़ावा देती हों या उसका प्रचार करती हों या बच्चों को इस तरह दिखाती हों जिससे उनका यौन शोषण हो सकता है.
- यौन शोषण की धमकी. उदाहरण के लिए, किसी बच्चे को धमकाने या ब्लैकमेल करने के लिए, अपने पास बच्चे की आपत्तिजनक तस्वीरें होने का दावा करना या ऐसी असली तस्वीरों का इस्तेमाल करना.
- बच्चे की तस्करी से जुड़ा कॉन्टेंट (जैसे कि व्यावसायिक तौर पर यौन शोषण के लिए, किसी बच्चे का विज्ञापन करना या लालच देना).

अगर हमें बच्चों का यौन शोषण दिखाने वाले कॉन्टेंट के बारे में पता चलता है, तो हम उचित कार्रवाई करेंगे. नैशनल सेंटर फ़ॉर मिसिंग ऐंड एक्स्प्लॉइटेड चिल्ड्रन को इसकी शिकायत भी की जा सकती है. अगर आपको लगता है कि कोई बच्चा खतरे में है या वह यौन शोषण, बुरे बर्ताव या तस्करी का शिकार हुआ है, तो स्थानीय पुलिस से संपर्क करें. इसके अलावा, बच्चों की सुरक्षा से जुड़े किसी संगठन से संपर्क करें जिनकी सूची यहां दी गई है.

इसके अलावा, उन ऐप्लिकेशन को अनुमति नहीं दी जाती जो बच्चों को पसंद आते हैं, लेकिन उनकी थीम वयस्कों वाली होती है. साथ ही, इसमें नीचे बताए गए ऐप्लिकेशन के अलावा और भी ऐप्लिकेशन शामिल हो सकते हैं:

- ऐसे ऐप्लिकेशन जिनमें बहुत ज़्यादा हिंसा, मारपीट, और खून-खराबा वाला कॉन्टेंट हो.
- ऐसे ऐप्लिकेशन जो नुकसानदायक और खतरनाक गतिविधियों को दिखाते हैं या उन्हें बढ़ावा देते हैं.

हम ऐसे ऐप्लिकेशन को भी अनुमति नहीं देते जिनमें शरीर या छवि को लेकर गलत चीज़ों 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.

गलत कॉन्टेंट

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

सेक्शुअल और अपशब्दों के इस्तेमाल वाला कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें सेक्शुअल कॉन्टेंट या गाली-गलौज हो या वे इस तरह के कॉन्टेंट को बढ़ावा देते हों. इनमें पोर्नोग्राफ़ी या यौन संतुष्टि देने वाला कॉन्टेंट या सेवाएं शामिल हैं. हम ऐसे ऐप्लिकेशन या ऐप्लिकेशन के कॉन्टेंट को अनुमति नहीं देते हैं जिसमें सेक्शुअल ऐक्ट का प्रमोशन किया जाता है या फिर पैसे या दूसरे किसी फ़ायदे के बदले में उपयोगकर्ताओं से कोई सेक्शुअल ऐक्ट करने को कहा जाता है. हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें खुद से कम उम्र के लोगों के यौन शोषण से जुड़ा या बिना सहमति के पोस्ट किया गया सेक्शुअल कॉन्टेंट शामिल हो या जिसमें ऐसे कॉन्टेंट का प्रमोशन किया जाता हो. नग्नता वाले कॉन्टेंट को तब ही अनुमति दी जा सकती है, जब उसका मुख्य मकसद शिक्षा देना, डॉक्यूमेंट्री, वैज्ञानिक या कलात्मक हो. इसके अलावा, ऐसा कॉन्टेंट ऐप्लिकेशन में बेवजह शामिल नहीं होना चाहिए.

कैटलॉग ऐप्लिकेशन—ऐसे ऐप्लिकेशन जिनमें ज़्यादा कॉन्टेंट कैटलॉग के तौर पर किताब/वीडियो के टाइटल दिखते हैं—ये ऐप्लिकेशन उन किताबों (ई-बुक और ऑडियो बुक दोनों) या वीडियो के टाइटल को डिस्ट्रिब्यूट कर सकते हैं जिनमें सेक्शुअल कॉन्टेंट शामिल होता है. हालांकि, इसके लिए ज़रूरी है कि ये ऐप्लिकेशन यहां दी गई शर्तें पूरी करें:

- किताब/वीडियो के टाइटल में मौजूद सेक्शुअल कॉन्टेंट, ऐप्लिकेशन के पूरे कैटलॉग का एक छोटा-सा हिस्सा हो
- ऐप्लिकेशन किसी ऐसी किताब/वीडियो का प्रमोशन न करता हो जिसमें इंसिडेंटल सेक्शुअल कॉन्टेंट हो. हालांकि, ये टाइटल उपयोगकर्ता के इतिहास के आधार पर या कीमत के सामान्य प्रमोशन के दौरान, सुझाव के तौर पर दिख सकते हैं.
- ऐप्लिकेशन, किसी किताब/वीडियो के ऐसे टाइटल डिस्ट्रिब्यूट न करता हो जिसमें बच्चों के लिए खतरनाक कॉन्टेंट, पॉर्न या लागू कानून के मुताबिक गैर-कानूनी माना जाने वाला अन्य सेक्शुअल कॉन्टेंट शामिल हो
- नाबालिगों की सुरक्षा के लिए ऐप्लिकेशन, किताब/वीडियो के ऐसे टाइटल का ऐक्सेस नाबालिगों के लिए प्रतिबंधित करता हो जिनमें सेक्शुअल कॉन्टेंट शामिल होता है

अगर आपके ऐप्लिकेशन में ऐसा कॉन्टेंट है जो इस नीति का उल्लंघन करता है, लेकिन किसी खास इलाके में उस कॉन्टेंट को कानूनी रूप से सही समझा जाता है, तो ऐप्लिकेशन उस खास इलाके के उपयोगकर्ताओं के लिए उपलब्ध हो सकता है. हालांकि, यह ऐप्लिकेशन अन्य सभी इलाके के उपयोगकर्ताओं के लिए उपलब्ध नहीं होगा.

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

- यौन गतिविधि वाली नग्नता या ऐसी अश्लील मुद्राएं दिखाना जिसमें व्यक्ति नग्न हो, धुंधला किया गया हो या उसने बहुत कम कपड़े पहने हों और/या ऐसे कपड़े पहने हों, जो सार्वजनिक जगह के लिहाज़ से सही न हों.
- ऐनिमेशन, तस्वीरों या किसी और तरह से यौन गतिविधियों को दिखाना या अश्लील मुद्राएं या शरीर के अंगों को यौन गतिविधि वाली स्थिति में 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 गतिविधियों वाली थीम, और यौन गतिविधियां दिखाई जाती हों.
- इसमें ऐसा कॉन्टेंट शामिल है जो ऐप्लिकेशन या स्टोर पेज पर शामिल होता है. साथ ही, जो कामुक हो या धर्म का अपमान करता हो. इस कॉन्टेंट में धर्म का अपमान करने वाली बातें, किसी व्यक्ति का अपमान करने वाली बातें, अश्लील मैसेज, और वयस्क/यौन कीवर्ड शामिल हो सकते हैं. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.
- जानवरों के साथ यौन गतिविधि दिखाने, इसके बारे में जानकारी देने या इसे बढ़ावा देने वाला कॉन्टेंट.
- वे ऐप्लिकेशन जो सेक्स से जुड़े मनोरंजन या एस्कॉर्ट सेवाओं का प्रमोशन करते हैं. इसके अलावा, ऐसी अन्य सेवाओं का प्रमोशन करते हैं जो हो सकता है कि पैसे देकर की जाने वाली यौन गतिविधियों की सुविधा उपलब्ध कराती हैं. इस तरह की सुविधा में, पैसे/गिफ़्ट देकर की जाने वाली डेटिंग या ऐसे सेक्शुअल अरेंजमेंट के अलावा, और भी चीज़ें शामिल हो सकती हैं, जिनमें एक पार्टनर से दूसरे पार्टनर को पैसे, गिफ़्ट या आर्थिक सहायता देने की उम्मीद की जाती है या ऐसा किया जाता है ("शुगर डेटिंग").
- ऐसे ऐप्लिकेशन जो लोगों को नीचा दिखाते हैं या उनका अपमान करते हैं, जैसे कि ऐसे ऐप्लिकेशन जो लोगों के कपड़े उतरते हुए दिखाने या उन्हें पारदर्शी कपड़ों में दिखाने का दावा करते हैं, भले ही इन्हें जान-बूझकर शरारत करने या मनोरंजन के लिए बने ऐप्लिकेशन के तौर पर लेबल किया गया हो.
- लोगों को धमकाने या उनसे यौन गतिविधि कराने के मकसद से बनाया गया कॉन्टेंट या व्यवहार. जैसे - बिना सहमति के तस्वीरें लेना, छुपाए गए कैमरे का इस्तेमाल करना, डीपफ़ेक या मिलती-जुलती टेक्नोलॉजी की मदद से सेक्शुअल कॉन्टेंट बनाकर उसे बिना सहमति के पोस्ट करना या यौन हिंसा वाला कॉन्टेंट पोस्ट करना.

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, जाति, प्रवास की स्थिति, 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.

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

- ऐसा कॉन्टेंट या भाषण जो दावा करे कि कोई सुरक्षित समूह 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 किसी समूह से 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 समूह के सदस्य हैं.
- ऐसा कॉन्टेंट जो नफ़रत 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 कार्टून, शिकार या फ़िशिंग करते हुए.

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

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

हिंसात्मक चरमपंथ

हम ऐसे आतंकवादी संगठनों, अन्य खतरनाक संगठनों या आंदोलनों के लिए, Google Play पर ऐप्लिकेशन पब्लिश करने की अनुमति नहीं देते जो नागरिकों के ख़िलाफ़ हिंसा की कार्रवाइयों में शामिल हैं, ऐसा करने की तैयारी कर रहे हैं या जिन्होंने इस तरह की कार्रवाइयों की ज़िम्मेदारी ली है. इसमें, ऐसे कामों के लिए भर्ती करना भी शामिल है.

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जिनमें हिंसक चरमपंथ या नागरिकों के ख़िलाफ़ हिंसा की योजना बनाने या उसकी तैयारी करने या हिंसा की तारीफ़ से जुड़ा कॉन्टेंट शामिल हो. जैसे, आतंकवादी गतिविधियों को बढ़ावा देने, हिंसा करने के लिए उकसाने या आतंकी हमलों का जश्न मनाने वाला कॉन्टेंट. अगर शिक्षा, डॉक्यूमेंट्री, विज्ञान या कला को ध्यान में रखकर हिंसक चरमपंथ से जुड़ा कॉन्टेंट पोस्ट किया जा रहा है, तो उस ईडीएसए कॉन्टेंट का संदर्भ देना न भूलें.

संवेदनशील घटनाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो किसी संवेदनशील घटना का फ़ायदा उठाकर कमाई करते हैं या घटना पर संवेदना नहीं दिखाते. इनमें, ऐसी घटनाएं शामिल हैं जिनका सामाजिक, सांस्कृतिक या राजनैतिक तौर पर असर गंभीर हो सकता है. जैसे, नागरिक आपातकाल, प्राकृतिक आपदाएं, सार्वजनिक स्वास्थ्य से जुड़े आपातकाल, झगड़ा, मौत या कोई अन्य दुखद घटना. आम तौर पर, संवेदनशील घटना से जुड़े ऐसे कॉन्टेंट वाले ऐप्लिकेशन को अनुमति दी जाती है जिसमें ईडीएसए (शिक्षा, डॉक्यूमेंटरी, विज्ञान या कला) वैल्यू हो या जिसका मकसद उपयोगकर्ताओं को सतर्क करना या जागरूकता फैलाना हो.

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

- प्राकृतिक वजहों, आत्महत्या, दवा की ज़्यादा मात्रा वगैरह से किसी व्यक्ति या एक से ज़्यादा लोगों की मौत होने जैसी घटनाओं पर संवेदनशीलता न दिखाना.
- ऐसी दुर्घटना के होने से इनकार करना जिसका पूरा सबूत हो.
- किसी ऐसी संवेदनशील घटना से फ़ायदा लेना जिसके पीड़ितों को सीधे तौर पर कोई राहत या मदद न मिली हो.

धमकाना और उत्पीड़न करना

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

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

- अंतरराष्ट्रीय या धार्मिक टकरावों से पीड़ित लोगों को धमकाना

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

खतरनाक उत्पाद

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

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

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें विस्फोटक, बंदूक, गोला-बारूद, दूसरे हथियार या बंदूक से जुड़ी ऐसी चीज़ों को बनाने के निर्देश होते हैं 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.

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

- इस्तेमाल करने वालों को ऐप्लिकेशन में मौजूद खरीदारी कार्ट की सुविधा की मदद से गांजा मंगवाने देना.
- गांजे की डिलीवरी या पिक अप में इसका इस्तेमाल करने वालों की मदद 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 या निकोटीन संबंधी प्रॉडक्ट (जैसे, ई-सिगरेट, वेप पेन, और निकोटीन पाउच) बेचने की सुविधा देते हैं या जो तंबाकू, शराब या निकोटीन के गैरकानूनी और गलत इस्तेमाल को बढ़ावा देते हैं.

ज़्यादा जानकारी

- नाबालिगों को शराब या तंबाकू का इस्तेमाल करते या बेचते हुए दिखाने या फिर ऐसा करने के लिए बढ़ावा देने की अनुमति नहीं है.
- ऐसे विज्ञापन भी दिखाने की अनुमति नहीं है जिनसे यह मैसेज जाता हो कि तंबाकू के सेवन से सामाजिक या पेशेवर स्थिति, बौद्धिक, खेल-कूद या यौन क्षमता बेहतर हो सकती है.
- बहुत ज़्यादा शराब पीने को अच्छाई के तौर पर दिखाने की अनुमति नहीं है. जैसे, लगातार पीते रहने या आपस में मुकाबले के तौर पर शराब पीते हुए दिखाना.
- तंबाकू से बनी चीज़ों के विज्ञापन, प्रमोशन या उन्हें प्रमुखता से दिखाने की अनुमति नहीं है. इसमें, तंबाकू से बने प्रॉडक्ट बेचने वाली साइटों के लिंक, विज्ञापन, बैनर, और कैटगरी दिखाना शामिल है.
- हम कुछ देशों/इलाकों में, खाने-पीने की चीज़ों/राशन की डिलीवरी की सुविधा देने वाले ऐप्लिकेशन में तंबाकू से बने चुनिंदा प्रॉडक्ट को बेचने की अनुमति दे सकते हैं. इसके लिए, उम्र से जुड़ी पाबंदी का पालन करना और सुरक्षा के तरीकों का इस्तेमाल करना ज़रूरी होगा. जैसे, डिलीवरी के समय आईडी देखना.
- हम ऐसे प्रॉडक्ट बेचने की अनुमति दे सकते हैं जिन्हें निकोटिन की लत छुड़ाने वाले प्रॉडक्ट के तौर पर प्रमोट किया जाता है. इसके लिए, उम्र से जुड़ी पाबंदी का पालन करना ज़रूरी है.

वित्तीय सेवाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो धोखा देने वाले या नुकसान पहुंचाने वाले फ़ाइनेंशियल प्रॉडक्ट और सेवाएं मुहैया कराते हैं.

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

अगर आपके ऐप्लिकेशन में फ़ाइनेंशियल प्रॉडक्ट और सेवाएं शामिल हैं या ऐप्लिकेशन से इनका प्रमोशन किया जाता है, तो आपका ऐप्लिकेशन जिस इलाके या देश के लोगों को टारगेट कर रहा है उस इलाके या देश के स्थानीय कानूनों का आपको पालन करना होगा.

उदाहरण के लिए, आपको स्थानीय कानून के मुताबिक ज़रूरी जानकारी ज़ाहिर करनी होगी.

अगर किसी ऐप्लिकेशन में फ़ाइनेंशियल फ़ीचर शामिल हैं, तो आपको Play Console में फ़ाइनेंशियल फ़ीचर के बारे में एलान वाला फ़ॉर्म भरना ज़रूरी है.

बाइनरी विकल्प

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

निजी क़र्ज़

हमारे हिसाब से, किसी व्यक्ति का किसी दूसरे व्यक्ति, संगठन या इकाई से पैसा उधार लेना निजी क़र्ज़ है. यह एक बार में लिया जाता है और इसका इस्तेमाल अचल संपत्ति खरीदने या पढ़ाई करने के लिए नहीं किया जाता. निजी क़र्ज़ लेने वालों को क़र्ज़ की क्वॉलिटी, सुविधाओं, शुल्क, पैसे लौटाने का शेड्यूल, जोखिमों, और उस क़र्ज़ से होने वाले फ़ायदों की जानकारी होनी चाहिए, ताकि वे क़र्ज़ लेने या न लेने के बारे में फ़ैसला ले सकें.

- निजी क़र्ज़ के उदाहरण: निजी क़र्ज़, दिन के हिसाब से मिलने वाले क़र्ज़ (पेडे क़र्ज़), आपस में सीधे एक-दूसरे को दिए जाने वाले क़र्ज़ (पीयर-टू-पीयर लोन), गाड़ी को गिरवी रखकर मिलने वाले क़र्ज़ (टाइटल लोन)
- ये निजी क़र्ज़ नहीं हैं: संपत्ति या घर गिरवी रखकर लिया जाने वाला क़र्ज़, कार के लिए लिया जाने वाला क़र्ज़, बैंक या वित्तीय संस्थानों की तय की गई सीमा के अंदर लिया जाने वाला क़र्ज़ (जैसे कि क्रेडिट कार्ड या पर्सनल लाइन ऑफ़ क्रेडिट)

निजी क़र्ज़ देने वाले ऐप्लिकेशन को Play Console में ऐप्लिकेशन कैटगरी के तौर पर “वित्तीय” सेट करना होगा. इनमें, वे ऐप्लिकेशन शामिल हैं जो सीधे तौर पर क़र्ज़ देते हैं, लीड जनरेट करते हैं, और ग्राहकों को क़र्ज़ देने वाले तीसरे पक्ष से मिलाते हैं. इनमें, ऊपर बताए गए उदाहरणों के अलावा, और अन्य तरह के ऐप्लिकेशन भी शामिल हो सकते हैं. इन ऐप्लिकेशन को मेटाडेटा में नीचे बताई गई जानकारी भी ज़ाहिर करनी होगी:

- पैसे लौटाने के लिए तय की गई कम से कम और ज़्यादा से ज़्यादा अवधि
- ब्याज की ज़्यादा से ज़्यादा सालाना दर (एपीआर), जिसमें आम तौर पर साल भर के लिए ब्याज की दर, शुल्क, और अन्य लागतें शामिल होती हैं या फिर जिसमें स्थानीय कानून के हिसाब से लगने वाली इसी तरह की अन्य दरें शामिल होती हैं
- क़र्ज़ की कुल लागत का एक उदाहरण, जिसमें क़र्ज़ पर ली गई रकम और लागू होने वाले सभी शुल्क शामिल होंगे
- ऐसी निजता नीति जिसमें वित्तीय सेवाओं से जुड़ी नीति में बताई गई पाबंदियों के हिसाब से, उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने से जुड़ी जानकारी ज़ाहिर की गई हो

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

इस नीति के अपवादों के तौर पर, उन देशों में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन को अपवाद माना जाएगा जहां कुछ नियमों के तहत कम समय के लिए ऐसे क़र्ज़ देने की अनुमति हो. ऐसे कुछ मामलों में, अपवादों का आकलन मौजूदा देश के स्थानीय नियम और कानून के दिशा-निर्देशों के मुताबिक किया जाएगा.

निजी क़र्ज़ की सेवा देने की आपकी क्षमता की पुष्टि करने के लिए, आपने जो लाइसेंस या दस्तावेज़ दिए हैं उनके और आपके डेवलपर खाते के बीच संबंध, साफ़ तौर पर दिखना चाहिए. हम पक्का करेंगे कि आपका खाता, सभी स्थानीय नियमों और कानूनों के हिसाब से है या नहीं. इसके लिए, आपसे ज़्यादा जानकारी या दस्तावेज़ मांगे जा सकते हैं.

निजी क़र्ज़ देने वाले या निजी क़र्ज़ दिलाने में मुख्य रूप से सहायता करने वाले ऐप्लिकेशन (जैसे, लीड जनरेट करने वाले या सहायता करने वाले ऐप्लिकेशन) या लोन से जुड़े ऐक्सेसरी ऐप्लिकेशन (लोन कैलकुलेटर, लोन गाइड वगैरह), और सैलरी पर क़र्ज़ देने वाले (ईडबल्यूए) ऐप्लिकेशन के लिए, फ़ोटो या संपर्क जैसी संवेदनशील जानकारी को ऐक्सेस करने पर पाबंदी लगी होती है. यहां दी गई अनुमतियों पर पाबंदी है:

- Read_external_storage
- Read_media_images
- Read_contacts
- Access_fine_location
- Read_phone_numbers
- Read_media_videos
- Query_all_packages
- Write_external_storage

संवेदनशील जानकारी या एपीआई का इस्तेमाल करने वाले ऐप्लिकेशन पर, अन्य ज़रूरी शर्तें और पाबंदियां लागू होती हैं. कृपया ज़्यादा जानकारी के लिए, अनुमतियों की नीति देखें.

ज़्यादा एपीआर वाले निजी क़र्ज़

हम अमेरिका में ऐसे ऐप्लिकेशन को निजी क़र्ज़ देने की मंज़ूरी नहीं देते जिनके ब्याज की सालाना दर (एपीआर) 36% या इससे ज़्यादा होती है. अमेरिका में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन को, ट्रूथ इन लेंडिंग ऐक्ट (TILA) के तहत मैक्सिमम एपीआर दिखाना ज़रूरी है.

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

देश के हिसाब से ज़रूरी शर्तें

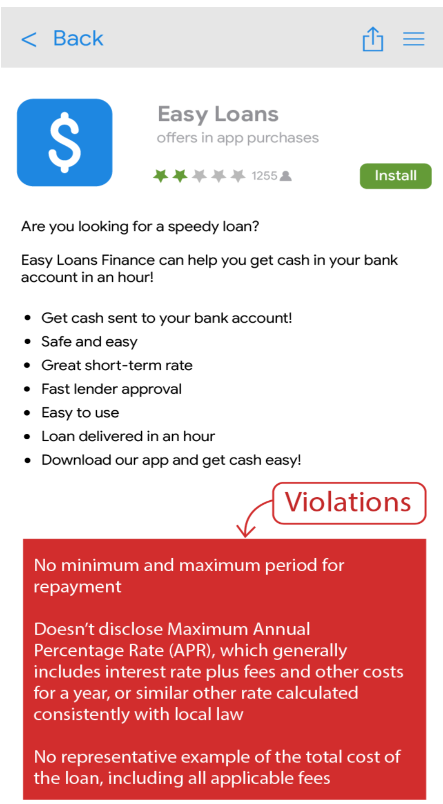
सूची में शामिल देशों में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन को अन्य ज़रूरी शर्तों को पूरा करना होगा. साथ ही, Play Console में अन्य ज़रूरी दस्तावेज़ भी जमा करने होंगे. ऐसा, वित्तीय सुविधाओं के एलान के तौर पर करना ज़रूरी है. Google Play के अनुरोध पर, आपको लागू होने वाले कानून और लाइसेंस की ज़रूरी शर्तों को पूरा करने से जुड़ी अन्य जानकारी या दस्तावेज़ उपलब्ध कराने होंगे.

1. **भारत**
   - अगर आपको निजी क़र्ज़ की सुविधा उपलब्ध कराने के लिए भारतीय रिज़र्व बैंक (आरबीआई) ने लाइसेंस दिया है, तो आपको अपने लाइसेंस की कॉपी सबमिट करनी होगी. हम उसकी जांच करेंगे.
   - अगर आप क़र्ज़ पर पैसे देने से जुड़ी गतिविधियों में सीधे तौर पर शामिल नहीं हैं और आपने सिर्फ़ एक ऐसा प्लैटफ़ॉर्म उपलब्ध कराया है जिसका इस्तेमाल करके, रजिस्ट्रेशन करा चुकी गैर-बैंकिंग वित्तीय कंपनियां (एनबीएफ़सी) या बैंक लोगों को क़र्ज़ पर पैसे दे सकते हैं, तो आपको एलान में साफ़ तौर पर इसके बारे में बताना होगा.
     - इसके अलावा, आपके ऐप्लिकेशन के ब्यौरे में, रजिस्टर की गई सभी गैर-बैंकिंग वित्तीय कंपनियों और बैंक के नाम साफ़ तौर पर ज़ाहिर किए जाने चाहिए.
2. **इंडोनेशिया**
   - अगर आपका ऐप्लिकेशन, OJK के रेगुलेशन नंबर 77/POJK.01/2016 (इसमें समय-समय पर बदलाव भी हो सकता है) के मुताबिक, पैसे क़र्ज़ पर देने की इन्फ़ॉर्मेशन टेक्नोलॉजी आधारित सेवाओं से जुड़ी गतिविधि में शामिल है, तो आपको अपने मान्य लाइसेंस की एक कॉपी सबमिट करनी होगी. हम उसकी जांच करेंगे.
3. **फ़िलिपींस**
   - ऑनलाइन लेंडिंग प्लैटफ़ॉर्म (ओएलपी) की मदद से क़र्ज़ देने वाली सभी फ़ाइनेंसिंग और क़र्ज़ देने वाली कंपनियों को, फ़िलिपींस सिक्योरिटी ऐंड एक्सचेंज कमीशन (पीएसईसी) से एसईसी रजिस्ट्रेशन नंबर और सर्टिफ़िकेट ऑफ़ अथॉरिटी (सीए) नंबर लेना होगा.
     - साथ ही, फ़ाइनेंसिंग/क़र्ज़ देने वाली कंपनी के तौर पर काम करने के लिए, आपको अपने ऐप्लिकेशन के ब्यौरे में कॉर्पोरेट नाम, कारोबार का नाम, पीएसईसी रजिस्ट्रेशन नंबर, और सर्टिफ़िकेट ऑफ़ अथॉरिटी के बारे में जानकारी देनी होगी.
   - कुछ ऐप्लिकेशन, क़र्ज़ के लिए चंदे के तौर पर पैसे जुटाने से जुड़ी गतिविधियों में शामिल होते हैं. इन गतिविधियों में, आपस में एक-दूसरे को क़र्ज़ देने की सुविधा (P2P) या चंदा जुटाने से जुड़ी गतिविधियों पर लागू होने वाले नियमों और कानूनों (चंदे से जुड़े नियम) के तहत परिभाषित गतिविधियां शामिल हैं. इन ऐप्लिकेशन के लिए ज़रूरी है कि वे लेन-देन को प्रोसेस करने के लिए, उन प्लैटफ़ॉर्म की मदद लें जो चंदे से जुड़ी गतिविधियों में मध्यस्थता करने वाले प्लैटफ़ॉर्म के तौर पर पीएसईसी में रजिस्टर हैं.
4. **नाइजीरिया**
   - डिजिटल प्लैटफ़ॉर्म पर क़र्ज़ देने की सुविधा उपलब्ध कराने वालों (डिजिटल मनी लेंडर यानी डीएमएल) को फ़ेडरल कॉम्पिटीशन ऐंड कंज़्यूमर प्रोटेक्शन कमीशन (एफ़सीसीपीसी) ऑफ़ नाइजीरिया की ओर से जारी किए गए, लिमिटेड इंटरिम रेगुलेटरी/रजिस्ट्रेशन फ़्रेमवर्क ऐंड गाइडलाइन्स फ़ॉर डिजिटल लेंडिंग, 2022 (इसमें समय-समय पर बदलाव भी हो सकता है) के नियमों का पालन करना होगा और ज़रूरी शर्तों को भी पूरा करना होगा. साथ ही, एफ़सीसीपीसी से ऐसा अप्रूवल लेटर लेना होगा जिसकी पुष्टि की जा सके.
   - लोन एग्रीगेटर को, डिजिटल प्लैटफ़ॉर्म पर क़र्ज़ देने की सेवाओं के लिए, ज़रूरी दस्तावेज़ और/या सर्टिफ़िकेट देना होगा. साथ ही, डीएमएल की सेवा देने वाले अपने हर एक पार्टनर की संपर्क जानकारी भी देनी होगी.
5. **केन्या**
   - डिजिटल क्रेडिट प्रोवाइडर (डीसीपी) को, डीसीपी के रजिस्ट्रेशन से जुड़ी प्रक्रिया पूरी करनी होगी. साथ ही, सेंट्रल बैंक ऑफ़ केन्या (सीबीके) से लाइसेंस लेना होगा. आपको अपने एलान के तौर पर, सीबीके से मिले लाइसेंस की कॉपी देनी होगी.
   - अगर आप क़र्ज़ पर पैसे देने से जुड़ी गतिविधियों में सीधे तौर पर शामिल नहीं हैं और आपने सिर्फ़ एक ऐसा प्लैटफ़ॉर्म उपलब्ध कराया है जिसका इस्तेमाल करके, रजिस्ट्रेशन करा चुके डीसीपी क़र्ज़ दे सकते हैं, तो आपको एलान में साफ़ तौर पर इसके बारे में बताना होगा. साथ ही, आपको इसमें शामिल अपने पार्टनर के डीसीपी लाइसेंस की कॉपी भी उपलब्ध करानी होगी.

- फ़िलहाल, हम सिर्फ़ उन संस्थाओं के एलानों और लाइसेंस को स्वीकार करते हैं जो सीबीके की आधिकारिक वेबसाइट पर, डिजिटल क्रेडिट प्रोवाइडर की डायरेक्ट्री में पब्लिश किए गए हैं.

6. **पाकिस्तान**
   - क़र्ज़ देने वाली हर गैर-बैंकिंग फ़ाइनेंस कंपनी (एनबीएफ़सी), सिर्फ़ एक डिजिटल लेंडिंग ऐप्लिकेशन (डीएलए) पब्लिश कर सकती है. एक एनबीएफ़सी पर एक से ज़्यादा डीएलए पब्लिश करने की कोशिश करने वाले डेवलपर के डेवलपर खाते और उसके अन्य खातों को बंद किया जा सकता है.
   - पाकिस्तान में डिजिटल प्लैटफ़ॉर्म पर क़र्ज़ की सेवा देने या इसके लिए सहायक के तौर पर काम करने के लिए, एसईसीपी से अनुमति मिलने का सबूत सबमिट करना होगा.
7. **थाईलैंड**
   - थाईलैंड में, 15% या इससे ज़्यादा ब्याज दर पर निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन को बैंक ऑफ़ थाईलैंड (बीओटी) या वित्त मंत्रालय (एमओएफ़) से मान्य लाइसेंस लेना होगा. डेवलपर को ऐसे दस्तावेज़ जमा करने होंगे जिनसे यह पता चले कि उन्हें थाईलैंड में निजी क़र्ज़ देने या इसके लिए सहायक के तौर पर काम करने के लिए अनुमति मिली है. इसके लिए यह दस्तावेज़ देना होगा:
     - निजी क़र्ज़ देने वाले या नैनो फ़ाइनेंस ऑर्गनाइज़ेशन के तौर पर काम करने के लिए, बैंक ऑफ़ थाईलैंड से मिले लाइसेंस की कॉपी.
     - क़र्ज़ देने वाले पीको या पीको-प्लस ऑर्गनाइज़ेशन के तौर पर काम करने के लिए, वित्त मंत्रालय से मिले पीको-फ़ाइनेंस के कारोबार से जुड़े लाइसेंस की कॉपी.

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



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

हम उन ऐप्लिकेशन जिनमें असली पैसे दांव पर लगाकर जुआ खेला जाता है, उससे जुड़े विज्ञापनों, गेमिफ़ाइड नतीजों वाले लॉयल्टी कार्यक्रम, और डेली फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन को सिर्फ़ तब अनुमति देते हैं, जब वे ज़रूरी शर्तों को पूरा करते हैं.

जुए वाले ऐप्लिकेशन

Google Play की सभी नीतियों से जुड़ी पाबंदियों और नीतियों के पालन के हिसाब से, हम उन ऐप्लिकेशन को अनुमति देते हैं जो नीचे दी गई टेबल में शामिल देशों में ऑनलाइन जुए की सुविधा उपलब्ध कराते हैं. यह अनुमति तब दी जाती है, जब इन ऐप्लिकेशन के डेवलपर, Google Play पर जुए वाले ऐप्लिकेशन उपलब्ध कराने के लिए आवेदन की प्रक्रिया पूरी कर लेते हैं . इसके अलावा, उन्हें

किसी खास देश में सरकारी ऑपरेटर के तौर पर काम करने की मंज़ूरी मिली हो और/या वह, जुआ खेलने के नियम-कानून तय करने वाले विभाग के पास लाइसेंस पा चुके ऑपरेटर के तौर पर रजिस्टर हो. साथ ही, वे ऑनलाइन जुए से जुड़ा जिस तरह का प्रॉडक्ट ऑफ़र करना चाहते हैं उसके लिए उसे मान्य ऑपरेटिंग लाइसेंस दिया गया हो.

हम मान्य लाइसेंस वाले या अनुमति पा चुके, जुए वाले सिर्फ़ उन ऐप्लिकेशन को मंज़ूरी देते हैं जिनमें जुए से जुड़े नीचे दिए गए ऑनलाइन प्रॉडक्ट होते हैं

- ऑनलाइन कसीनो गेम
- स्पोर्ट्स बेटिंग
- घुड़दौड़ (उन देशों/इलाकों में लागू कानून के मुताबिक हो या लाइसेंस पा चुका हो जहां इसके लिए बनाए गए नियम स्पोर्ट्स बेटिंग के नियमों से अलग हों)
- लॉटरी
- डेली फ़ैंटेसी स्पोर्ट

मंज़ूरी पाने के लिए ऐप्लिकेशन को नीचे बताई गई ज़रूरी शर्तें पूरी करनी होंगी:

- Google Play पर अपने ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को ऐप्लिकेशन प्रोसेस सही तरीके से पूरी करनी होगी;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और इंडस्ट्री स्टैंडर्ड का पालन करना चाहिए जहां उसे उपलब्ध कराया जाता है;
- डेवलपर के पास हर उस देश या राज्य/इलाके के लिए जुए का एक मान्य लाइसेंस होना चाहिए जहां ऐप्लिकेशन को उपलब्ध कराया जाता है;
- डेवलपर को जुए से जुड़ा ऐसा कोई भी प्रॉडक्ट उपलब्ध नहीं कराना चाहिए जो जुए से जुड़े उसके लाइसेंस के दायरे से बाहर हो;
- कम उम्र के लोगों को ऐप्लिकेशन का इस्तेमाल करने से रोकना चाहिए;
- ऐप्लिकेशन को उन देशों, राज्यों/इलाकों या भौगोलिक जगहों पर इसे ऐक्सेस करने और इस्तेमाल करने से रोकना चाहिए जो डेवलपर के, जुए के लाइसेंस में शामिल नहीं हैं;
- ऐप्लिकेशन, पैसे चुकाकर Google Play से डाउनलोड किए जाने वाले ऐप्लिकेशन या Google Play इन-ऐप बिलिंग का इस्तेमाल करके खरीदे जाने वाले ऐप्लिकेशन के तौर पर मौजूद नहीं होना चाहिए;
- ऐप्लिकेशन ऐसा होना चाहिए जिसे Google Play Store से मुफ़्त में डाउनलोड और इंस्टॉल किया जा सके;
- ऐप्लिकेशन को AO (सिर्फ़ वयस्क) या IARC के तौर पर रेट किया जाना चाहिए; और
- ऐप्लिकेशन और इसकी ऐप लिस्टिंग में, ज़िम्मेदार तरीके से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए.

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

वे सभी ऐप्लिकेशन जो ऊपर बताई गई जुए से जुड़ी ज़रूरी शर्तों को पूरा नहीं करते और नीचे दी गई "असली पैसे दांव पर लगाकर खेले जाने वाले गेम के अन्य पायलट" की कैटगरी में शामिल नहीं किए गए हैं उनके लिए, हम ऐसे कॉन्टेंट या सेवाओं को अनुमति नहीं देते जो ऐप्लिकेशन का इस्तेमाल करने वाले लोगों को दांव लगाने, हिस्सेदारी या असली पैसों (इसमें पैसों से खरीदे गए इन-ऐप्लिकेशन आइटम भी शामिल हैं) के बदले में हिस्सा लेने की सुविधा देते हैं. ऐसा इसलिए किया जाता है, ताकि उन्हें ऐसा इनाम मिले जिसकी असल दुनिया में कोई कीमत है. इसमें ऑनलाइन कसीनो, स्पोर्ट बेटिंग, लॉटरी, और ऐसे गेम भी आते हैं जो नकद या असल दुनिया के अन्य इनाम ऑफ़र करते हैं. हालांकि, यह इन ही तक सीमित नहीं है. इसमें, गेम से जुड़े लॉयल्टी कार्यक्रम के बारे में नीचे बताई गई ज़रूरी शर्तों के तहत मंज़ूरी पाने वाले कार्यक्रम शामिल नहीं हैं.

उल्लंघनों के उदाहरण

- ऐसे गेम जो इनाम के तौर पर असली चीज़ या असली पैसे जीतने के मौके के बदले में पैसे लेते हैं
- वे ऐप्लिकेशन जिनमें नेविगेट किए जा सकने वाले ऐसे एलिमेंट या सुविधाएं (जैसे, मेन्यू आइटम, टैब, बटन, वेबव्यू वगैरह) शामिल हैं जो असली पैसों का इस्तेमाल करके खेले जाने वाले गेम, प्रतियोगिताएं या टूर्नामेंट में दांव लगाने, हिस्सेदारी लेने या हिस्सा लेने के लिए "कॉल टू ऐक्शन" की सुविधा देती हैं. उदाहरण के लिए, ऐसे नेविगेशनल एलिमेंट (मेन्यू आइटम, टैब, बटन वगैरह) जो लोगों को टूर्नामेंट में नकद इनाम जीतने का मौका देने के लिए "बेटिंग करने" या "रजिस्टर करने" या "खेलने" के लिए न्योता भेजते हैं.
- ऐसे ऐप्लिकेशन जो जुआ खेलने वाले लोगों, इन-ऐप्लिकेशन मुद्राओं, जीते गए इनाम को मंज़ूरी देते हैं या उन्हें मैनेज करते हैं. इसके अलावा, ऐसे ऐप्लिकेशन जो जुआ खेलने के लिए पैसे जमा करते हैं या इनाम के तौर पर असली चीज़ या असली पैसे ऑफ़र करते हैं.

असली पैसे दांव पर लगाकर खेले जाने वाले अन्य गेम के लिए पायलट

हम असली पैसे दांव पर लगाकर खेले जाने वाले कुछ खास तरह के गेम के लिए, सीमित अवधि वाले पायलट कार्यक्रम शुरू कर सकते हैं. ये कार्यक्रम कभी-कभी और कुछ चुनिंदा इलाकों के लिए ही होते हैं. ज़्यादा जानकारी के लिए, यहां दिए गए सहायता केंद्र के पेज पर जाएं. जापान में ऑनलाइन क्रेन गेम का पायलट कार्यक्रम 11 जुलाई, 2023 को बंद हो गया है. लागू कानून के दायरे में आने वाले और

कुछ खास शर्तों को पूरा करने वाले ऑनलाइन क्रेन गेम के ऐप्लिकेशन, 12 जुलाई, 2023 से Google Play पर दुनिया भर के उपयोगकर्ताओं के लिए उपलब्ध कराए जा सकते हैं.

गेम से जुड़े लॉयल्टी कार्यक्रम

जहां कानूनी तौर पर अनुमति हो और जुए या गेमिंग के लाइसेंस से जुड़ी अन्य ज़रूरी शर्तें लागू न हों वहां हम उन लॉयल्टी कार्यक्रमों को अनुमति देते हैं जो उपयोगकर्ताओं को असली इनाम या पैसे देते हैं. ये गेम 'Play स्टोर' की नीचे बताई गई ज़रूरी शर्तों के मुताबिक हैं:

सभी ऐप्लिकेशन के लिए (गेम और गेम के अलावा अन्य ऐप्लिकेशन):

- लॉयल्टी कार्यक्रम के फ़ायदे, सुविधाएं या इनाम, ऐप्लिकेशन में पैसे के किसी भी मान्य लेन-देन के लिए पूरी तरह से पूरक और अलग होने चाहिए. पैसे का कोई भी मान्य लेन-देन, सामान या सेवाओं के लिए ऐसा असली लेन-देन होना चाहिए जो लॉयल्टी कार्यक्रम पर निर्भर न करता हो. यह न तो खरीदारी पर निर्भर होना चाहिए और न ही किसी भी तरह की अदला-बदली से जुड़ा होना चाहिए. ऐसा न होने पर, पैसे दांव पर लगाकर खेले जाने वाले जुए, गेम, और प्रतियोगिताओं से जुड़ी नीति का उल्लंघन होगा.
  - उदाहरण के लिए, पैसे के किसी भी मान्य लेन-देन का कोई भी हिस्सा लॉयल्टी कार्यक्रम में हिस्सा लेने के लिए शुल्क या दांव पर लगाई गई रकम नहीं दिखा सकता. साथ ही, पैसे के किसी भी मान्य लेन-देन से उसकी सामान्य कीमत से ज़्यादा कीमत वाले सामान या सेवाएं नहीं खरीदनी चाहिए.

गेम ऐप्लिकेशन के लिए:

- पैसे के किसी भी मान्य लेन-देन से जुड़े फ़ायदों, सुविधाओं या इनाम वाले लॉयल्टी पॉइंट या इनाम सिर्फ़ तय अनुपात के आधार पर ही दिए और रिडीम किए जाने चाहिए. इस अनुपात के बारे में, ऐप्लिकेशन के साथ-साथ कार्यक्रम के लिए सार्वजनिक तौर पर उपलब्ध आधिकारिक नियमों में भी साफ़ तौर पर बताया जाता है. साथ ही, मिलने वाले फ़ायदों या छूट वाली कीमत का इस्तेमाल, गेम की परफ़ॉर्मेंस या मौके पर आधारित नतीजों, इनाम या फ़ायदे के तौर पर **नहीं** होना चाहिए.

गेम के अलावा अन्य ऐप्लिकेशन के लिए:

- लॉयल्टी पॉइंट या इनाम, किसी प्रतियोगिता या मौके पर आधारित नतीजों के साथ जोड़े जा सकते हैं. इसके लिए, उन्हें नीचे दी गई शर्तों को पूरा करना होगा. पैसे के किसी भी मान्य लेन-देन से जुड़े फ़ायदों, सुविधाओं या इनाम वाले लॉयल्टी कार्यक्रम के लिए इन शर्तों को पूरा करना ज़रूरी है:
  - कार्यक्रम के आधिकारिक नियमों को ऐप्लिकेशन में प्रकाशित करें.
  - ऐसे कार्यक्रमों के लिए जिनमें वैरिएबल, किसी भी क्रम में मिलने वाले इनाम सिस्टम या जोखिम शामिल हों: कार्यक्रम के लिए बताई गई आधिकारिक शर्तों के तहत ज़ाहिर करें, 1) इनाम पता करने की संभावना वाले इनाम कार्यक्रमों में, इनाम पाने की कितनी संभावना है और 2) इस तरह के बाकी सभी कार्यक्रमों के लिए, चुनने के तरीके (जैसे कि इनाम का पता लगाने में इस्तेमाल किए जाने वाले वैरिएबल).
  - ड्रॉइंग, स्वीपस्टैक्स या इसी तरह के अन्य प्रचार वाले कार्यक्रम की आधिकारिक शर्तों में, हर प्रचार के लिए विजेताओं की तय संख्या, हिस्सा लेने की आखिरी तारीख, और इनाम पाने की तारीख के बारे में खास तौर पर बताएं.
  - ऐप्लिकेशन या कार्यक्रम की आधिकारिक शर्तों के तहत, लॉयल्टी पॉइंट या लॉयल्टी इनाम को बढ़ाने और रिडीम करने के लिए, किसी तय अनुपात के बारे में खास तौर पर बताएं.

लॉयल्टी कार्यक्रम वाले ऐप्लिकेशन	**लॉयल्टी गेमिफ़िकेशन और कई इनाम**	**तय अनुपात/शेड्यूल के हिसाब से लॉयल्टी इनाम**	**लॉयल्टी कार्यक्रम के लिए ज़रूरी नियम और शर्तें**	**नियम और शर्तों में, मौके के हिसाब से काम करने वाले किसी भी लॉयल्टी कार्यक्रम से जुड़ी संभावनाओं या चुनने के तरीके की जानकारी देनी चाहिए**
गेम	अनुमति नहीं है	अनुमति है	ज़रूरी	लागू नहीं (गेम ऐप्लिकेशन, लॉयल्टी कार्यक्रम में मौके के हिसाब से काम करने वाले एलिमेंट का इस्तेमाल नहीं कर सकते)
गेम के अलावा अन्य ऐप्लिकेशन	अनुमति है	अनुमति है	ज़रूरी	ज़रूरी

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

जुए, असली पैसे दांव पर लगाकर खेले जाने वाले गेम, प्रतियोगिताओं, और टूर्नामेंट के प्रमोशन 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 दिखाने के लिए, ऐप्लिकेशन और विज्ञापन (इसमें विज्ञापन देने वाले लोग भी शामिल हैं) को उस इलाके में लागू होने वाले सभी कानूनों और उद्योग के मानकों का पालन करना होगा;
- विज्ञापन को जुए से जुड़े ऐसे सभी प्रॉडक्ट और सेवाओं के प्रचार के लाइसेंस के लिए लागू होने वाली सभी ज़रूरी स्थानीय शर्तों को पूरा करना चाहिए;
- ऐप्लिकेशन में जुए से जुड़ा कोई विज्ञापन, 18 साल से कम उम्र के लोगों को 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 के लैंडिंग पेज पर, विज्ञापन में दिखने वाली ऐप्लिकेशन लिस्ट 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. उदाहरण के लिए, सोशल कसीनो ऐप्लिकेशन और वर्चुअल स्लॉट मशीन वाले ऐप्लिकेशन;
- ऐप्लिकेशन में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट में मदद करने वाली या इनके साथ काम करने वाली सुविधाएं नहीं दी जानी चाहिए. उदाहरण के लिए, ऐसी सुविधा जो जुआ खेलने, पेआउट, खेल के स्कोर/ऑड्स/परफ़ॉर्मेंस को ट्रैक करने या इनमें हिस्सा लेने के लिए दिए जाने वाले पैसों को मैनेज करने में मदद करती है;
- ऐप्लिकेशन के कॉन्टेंट में जुए या असली पैसे दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट का प्रमोशन नहीं होना चाहिए. इसके अलावा, इसे ऐसी सेवाएं देने वाले पेज पर भी लोगों को नहीं ले जाना चाहिए

ऊपर दिए गए सेक्शन में बताई गई सभी ज़रूरी शर्तों को पूरा करने वाले ऐप्लिकेशन ही जुए या असली पैसे देकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट के विज्ञापन दिखा सकते हैं. जुआ या असली पैसों को दांव पर लगाकर खेले जाने वाले गेम, लॉटरी या टूर्नामेंट के विज्ञापन उन ऐप्लिकेशन में दिखाए जा सकते हैं जिन्हें जुए से जुड़े (जैसा कि ऊपर बताया गया है) या डेली फ़ैंटेसी स्पोर्ट (जैसा कि नीचे बताया गया है) वाले ऐप्लिकेशन के तौर पर अनुमति मिल चुकी है. साथ ही, वे ऊपर बताए गए एक से छह बिन्दु तक की सभी ज़रूरी शर्तों को पूरा करते हों.

उल्लंघनों के उदाहरण

- 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 विज्ञापन दिखाए जाते हैं. ये विज्ञापन, लोगों को स्पोर्ट बेटिंग साइट पर ले जाते हैं
- 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

डेली फ़ैंटेसी स्पोर्ट (DFS) वाले ऐप्लिकेशन

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

- ऐप्लिकेशन या तो 1) सिर्फ़ अमेरिका में उपलब्ध हो या उसे 2) अमेरिका के अलावा दूसरे देशों में, जुए से जुड़े ऐप्लिकेशन की ऊपर बताई गई ज़रूरी शर्तों और ऐप्लिकेशन प्रोसेस के तहत मंज़ूरी दी गई हो;
- 'Play स्टोर' पर ऐप्लिकेशन को उपलब्ध कराने के लिए, डेवलपर को DFS ऐप्लिकेशन प्रोसेस सही तरीके से पूरा करना होगा;
- ऐप्लिकेशन को हर उस देश में लागू सभी कानूनों और उद्योग के मानकों का पालन करना चाहिए जहां उसे उपलब्ध कराया 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 'Play स्टोर' से मुफ़्त में डाउनलोड और इंस्टॉल किए जा सकने वाला होना चाहिए;
- ऐप्लिकेशन को AO (सिर्फ़ वयस्क) या IARC के तौर पर रेट किया जाना चाहिए;
- ऐप्लिकेशन और उसकी ऐप्लिकेशन लिस्टिंग में, सही तरीके से जुआ खेलने से जुड़ी जानकारी को साफ़ तौर पर दिखाया जाना चाहिए;
- 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 रोकना चाहिए जहां डेवलपर के पास रोज़ाना के फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन के लिए ज़रूरी लाइसेंस नहीं है; और
- अमेरिका के जिन राज्यों और इलाकों में डेली फ़ैंटेसी स्पोर्ट वाले ऐप्लिकेशन गैरकानूनी हैं वहां ऐप्लिकेशन इस्तेमाल करने की अनुमति नहीं होनी चाहिए.

गैरकानूनी गतिविधियां

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

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

- गैर-कानूनी दवाएं बनाने या उनमें इस्तेमाल होने वाले पौधों को उगाने के लिए निर्देश.
- नाबालिगों को किसी नशीली दवा, शराब या तंबाकू का इस्तेमाल करते हुए या बेचते हुए दिखाना या बढ़ावा देना.
- गैर-कानूनी दवाएं उगाने या बनाने के निर्देश.

यूज़र जनरेटेड कॉन्टेंट

यूज़र जनरेटेड कॉन्टेंट (यूजीसी) ऐसा कॉन्टेंट होता है जिसे लोग किसी ऐप्लिकेशन में जोड़ते हैं. यह कॉन्टेंट, ऐप्लिकेशन इस्तेमाल करने वाले लोगों के कम से कम एक ग्रुप को दिखता है या वह उसे ऐक्सेस कर सकता है.

जिन ऐप्लिकेशन में यूजीसी (लोगों का बनाया कॉन्टेंट) शामिल होता है या दिखाया जाता है उनमें बेहतरीन, असरदार, और लगातार होने वाला यूजीसी मॉडरेशन लागू करना होगा. इनमें, वे ऐप्लिकेशन शामिल हैं जो उपयोगकर्ताओं को किसी यूजीसी प्लैटफ़ॉर्म पर भेजने के लिए खास ब्राउज़र या क्लाइंट के तौर पर काम करते हैं. यूजीसी मॉडरेशन में ये चीज़ें शामिल हैं:

- उपयोगकर्ताओं को यूजीसी बनाने या अपलोड करने से पहले ऐप्लिकेशन को इस्तेमाल करने की शर्तों और/या उपयोगकर्ता नीति को स्वीकार करना ज़रूरी है;
- Google Play Developer Program की नीतियों के मुताबिक यह तय करना कि किस तरह का कॉन्टेंट और बर्ताव आपत्तिजनक है. साथ ही, ऐप्लिकेशन के इस्तेमाल की शर्तों या उपयोगकर्ता नीतियों के तहत उन पर पाबंदी लगाना;
- ऐसा यूजीसी मॉडरेशन लागू करना जो ऐप्लिकेशन पर होस्ट किए गए यूजीसी के मुताबिक सही और एक जैसा हो. इसमें ऐसा इन-ऐप्लिकेशन सिस्टम उपलब्ध कराना शामिल है जो आपत्तिजनक यूजीसी और उपयोगकर्ताओं को ब्लॉक करने और उनकी शिकायत करने की सुविधा देता हो. साथ ही, यूजीसी या उपयोगकर्ताओं के सही न होने पर, उनके ख़िलाफ़ कार्रवाई करता हो. अलग-अलग तरह का यूजीसी उपलब्ध कराने के लिए, मॉडरेशन की अलग-अलग प्रक्रियाओं की ज़रूरत पड़ सकती है. उदाहरण के लिए:
  - कुछ ऐप्लिकेशन में यूजीसी की मदद से, खास उपयोगकर्ताओं की पहचान ऑफ़लाइन रजिस्ट्रेशन या पुष्टि करने जैसे तरीकों से की जाती है (जैसे, खास तौर पर किसी स्कूल या कंपनी जैसे संगठनों के लिए इस्तेमाल होने वाले ऐप्लिकेशन). इन्हें कॉन्टेंट और उपयोगकर्ताओं की शिकायत करने के लिए, इन-ऐप्लिकेशन सुविधाएं देनी होंगी.
  - जिन ऐप्लिकेशन में यूजीसी से जुड़ी सुविधाओं की मदद से, खास उपयोगकर्ताओं के साथ लोग 1:1 इंटरैक्शन (उदाहरण के लिए, डायरेक्ट मैसेज करना, लोगों को टैग करना, मेंशन करना वगैरह) कर सकते हैं उन्हें उपयोगकर्ताओं को ब्लॉक करने के लिए, इन-ऐप्लिकेशन सुविधाएं देनी होंगी.
  - जिन ऐप्लिकेशन में यूजीसी, सार्वजनिक तौर पर उपलब्ध है उन्हें उपयोगकर्ताओं और कॉन्टेंट की शिकायत करने और उपयोगकर्ताओं को ब्लॉक करने के लिए, इन-ऐप्लिकेशन सुविधाएं देनी होंगी. जैसे, सोशल नेटवर्किंग और ब्लॉगर ऐप्लिकेशन.
  - ऑगमेंटेड रिएलिटी (एआर) वाले ऐप्लिकेशन के मामले में, यूजीसी मॉडरेशन (जिसमें इन-ऐप्लिकेशन रिपोर्टिंग सिस्टम शामिल है) को, आपत्तिजनक एआर यूजीसी (उदाहरण के लिए, सेक्शुअल ऐक्ट वाली एआर इमेज) और संवेदनशील एआर एंकरिंग की जगह (उदाहरण के लिए, एआर एंकरिंग से प्रतिबंधित जगहों के मालिकों को समस्या हो सकती है, जैसे कि सेना का बेस या निजी प्रॉपर्टी) के लिए ज़िम्मेदारी लेनी होगी.
- ऐप्लिकेशन के अंदर कमाई करने की सुविधा का इस्तेमाल करने वाले उपयोगकर्ता के आपत्तिजनक बर्ताव को बढ़ावा देने से रोकता है.

इंसिडेंटल सेक्शुअल कॉन्टेंट

अगर यूजीसी वाले किसी ऐसे ऐप्लिकेशन में सेक्शुअल कॉन्टेंट दिखता है जिसमें (1) मुख्य रूप से सेक्शुअल कॉन्टेंट नहीं दिखाया जाता हो और (2) जो खास तौर पर, न तो सेक्शुअल कॉन्टेंट का प्रमोशन करता हो या न ही उसका सुझाव देता हो, तो उसे "इंसिडेंटल" कॉन्टेंट माना जाता है. लागू कानून के मुताबिक, सेक्शुअल कॉन्टेंट गैर-कानूनी है. साथ ही, बच्चों के लिए खतरनाक कॉन्टेंट को न तो "इंसिडेंटल" कॉन्टेंट माना जाता है और न ही इसकी अनुमति है.

यूजीसी वाले ऐप्लिकेशन में इंसिडेंटल सेक्शुअल कॉन्टेंट शामिल किया जा सकता है. इसके लिए, इन सभी ज़रूरी शर्तों को पूरा करना होगा:

- इंसिडेंटल कॉन्टेंट को डिफ़ॉल्ट रूप से, फ़िल्टर की मदद से छिपाया गया हो. उदाहरण के लिए, अगर "सेफ़ सर्च" की सुविधा बंद न की गई हो, तो डिफ़ॉल्ट रूप से, पेज पर इंसिडेंटल कॉन्टेंट को अस्पष्ट करके या उसे दिखने से रोकने वाले फ़िल्टर की मदद से छिपाया गया हो. साथ ही, इन फ़िल्टर को पूरी तरह से बंद करने के लिए, उपयोगकर्ता को कम से कम दो कार्रवाइयां करनी होंगी.
- परिवार से जुड़ी नीति के मुताबिक, न्यूट्रल एज स्क्रीन जैसे उम्र की पुष्टि करने के सिस्टम या लागू कानून के मुताबिक बनाए गए अन्य सिस्टम की मदद से, बच्चों पर आपके ऐप्लिकेशन को इस्तेमाल करने की पाबंदी हो.
- आपका ऐप्लिकेशन, कॉन्टेंट रेटिंग की नीति के मुताबिक, यूजीसी की रेटिंग पाने के लिए सवालों की सूची का सटीक जवाब देता हो.

ऐसे ऐप्लिकेशन जिनका मुख्य मकसद आपत्तिजनक यूजीसी को शामिल करना है उन्हें Google Play से हटा दिया जाएगा. इसी तरह, उन ऐप्लिकेशन को भी Google Play से हटा दिया जाएगा जो खास तौर पर आपत्तिजनक यूजीसी होस्ट करने के लिए इस्तेमाल किए जाते हैं या ऐप्लिकेशन इस्तेमाल करने वाले लोगों के बीच आपत्तिजनक यूजीसी जैसे कॉन्टेंट दिखाने वाले ऐप्लिकेशन की छवि बनाते हैं.

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

- अश्लीलता फैलाने वाले ऐसे यूज़र जनरेटेड कॉन्टेंट को बढ़ावा देना जिसमें मुख्य तौर पर 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 के उपायों की कमी हो, खासकर नाबालिगों को लेकर.
- किसी ऐप्लिकेशन में शामिल ऐसी पोस्ट, टिप्पणियां या फ़ोटो जिनका मुख्य मकसद किसी दूसरे व्यक्ति से बुरा बर्ताव करना, नुकसान पहुंचाने वाला हमला करना या मज़ाक़ उड़ाने के लिए उसे प्रताड़ित करना या अकेला छोड़ देना हो.
- ऐसे ऐप्लिकेशन, जो आपत्तिजनक कॉन्टेंट के बारे में उपयोगकर्ता की शिकायतों को हल करने में लगातार नाकामयाब हो रहे हों.

सेहत से जुड़ा कॉन्टेंट और सेवाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो लोगों के स्वास्थ्य को नुकसान पहुंचाने वाला कॉन्टेंट और सेवाएं उपलब्ध कराते हैं.

अगर आपका ऐप्लिकेशन, स्वास्थ्य से जुड़ा कॉन्टेंट और सेवाएं उपलब्ध कराता है या इनका प्रचार करता है, तो आपको यह पक्का करना होगा कि ऐप्लिकेशन में सभी नियमों और कानूनों का पालन किया जा रहा है.

सेहत से जुड़े ऐप्लिकेशन

अगर आपका ऐप्लिकेशन स्वास्थ्य से जुड़ा ऐप्लिकेशन है या उसमें स्वास्थ्य से जुड़ी सुविधाएं हैं और वह स्वास्थ्य की जानकारी से जुड़ा डेटा ऐक्सेस कर सकता है, तो उसे डेवलपर के लिए बनाई गई Google Play की मौजूदा नीतियों का पालन करना चाहिए. इन नीतियों में निजता, धोखाधड़ी, और गलत इस्तेमाल और संवेदनशील घटनाओं से जुड़ी नीति शामिल है. इनके अलावा, ऐप्लिकेशन को यहां बताई गई ज़रूरी शर्तों को भी पूरा करना होगा:

- **Play Console में किया जाने वाला एलान:**
  - Play Console में ऐप्लिकेशन कॉन्टेंट पेज (नीति > ऐप्लिकेशन कॉन्टेंट) पर जाएं और अपने ऐप्लिकेशन की कैटगरी चुनें.
- **निजता नीति और साफ़ तौर पर जानकारी ज़ाहिर करने से जुड़ी ज़रूरी शर्तें:**
  - ऐप्लिकेशन डेवलपर के लिए ज़रूरी है कि वे Play Console में, तय की गई जगह पर निजता नीति का लिंक पोस्ट करें. इसके अलावा, उन्हें ऐप्लिकेशन के अंदर भी निजता नीति का लिंक या टेक्स्ट पोस्ट करना होगा. कृपया यह पक्का करें कि आपकी निजता नीति किसी ऐसे यूआरएल पर उपलब्ध हो जो काम करता हो, जिसे सभी ऐक्सेस कर सकें, और जिसकी जियोफ़ेंसिंग नहीं की गई हो. साथ ही, उसमें बदलाव न किया जा सके. ऐसा डेटा की सुरक्षा वाले सेक्शन के हिसाब से होना चाहिए. निजता नीति को PDF के रूप में उपलब्ध नहीं कराना चाहिए.
  - आपके ऐप्लिकेशन की निजता नीति में, ऐप्लिकेशन में ज़ाहिर की जाने वाली जानकारी के साथ-साथ, इस बात की पूरी जानकारी भी साफ़ तौर पर दी जानी चाहिए कि आपका ऐप्लिकेशन, उपयोगकर्ता के निजी और संवेदनशील डेटा को कैसे ऐक्सेस, इकट्ठा, शेयर, और इस्तेमाल करता है. डेटा की सुरक्षा वाले सेक्शन में दी गई जानकारी के अलावा, यह जानकारी भी देनी होगी. ऐप्लिकेशन को साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों को पूरा करना होगा. इसमें, ऐप्लिकेशन में की जाने वाली ऐसी कोई भी गतिविधि या डेटा शामिल है जिसके लिए रनटाइम की अनुमतियां या ऐसी अनुमतियां ज़रूरी हैं जो उपयोगकर्ता की सुरक्षा के लिहाज़ से खतरनाक हो सकती हैं.
  - ऐसी अनुमतियों का अनुरोध नहीं किया जाना चाहिए जो स्वास्थ्य से जुड़े ऐप्लिकेशन के मुख्य फ़ंक्शन के काम करने के लिए ज़रूरी नहीं है. साथ ही, इस्तेमाल नहीं की जा रही अनुमतियों को हटा देना चाहिए. स्वास्थ्य से जुड़ी संवेदनशील जानकारी के दायरे में आने वाली अनुमतियों की सूची के बारे में जानने के लिए, स्वास्थ्य से जुड़े ऐप्लिकेशन की कैटगरी और अन्य जानकारी देखें.
  - अगर आपका ऐप्लिकेशन मुख्य रूप से स्वास्थ्य से जुड़ा ऐप्लिकेशन नहीं है, लेकिन यह स्वास्थ्य की जानकारी का डेटा ऐक्सेस कर सकता है और इसमें स्वास्थ्य से जुड़ी सुविधाएं हैं, तब भी यह ऐप्लिकेशन, स्वास्थ्य ऐप्लिकेशन वाली नीति के दायरे में आता है. उपयोगकर्ताओं को ऐप्लिकेशन के मुख्य फ़ंक्शन के साथ-साथ यह भी पता होना चाहिए कि उनसे जुटाए गए स्वास्थ्य से जुड़े डेटा का इस्तेमाल इस फ़ंक्शन के लिए कैसे किया जाएगा. जैसे, बीमा सेवाएं देने वाली कंपनियां, ऐसे गेमिंग ऐप्लिकेशन जो गेमप्ले को

बेहतर बनाने के लिए, उपयोगकर्ता की गतिविधि से जुड़ा डेटा इकट्ठा करते हैं वगैरह. ऐप्लिकेशन की निजता नीति में डेटा के इस सीमित इस्तेमाल की जानकारी होनी चाहिए.

- **अन्य ज़रूरी शर्तें:**
  Play Console में कैटगरी चुनने के अलावा, अगर आपका ऐप्लिकेशन यहां दी गई किसी कैटगरी के दायरे में आता है, तो उसके लिए आपके ऐप्लिकेशन को ज़रूरी शर्तें पूरी करनी होंगी:
  - **सरकार के तहत काम करने वाले स्वास्थ्य से जुड़े ऐप्लिकेशन:** अगर सरकार या स्वास्थ्य सेवा देने वाले किसी मान्य संगठन ने आपको स्वास्थ्य से जुड़े ऐप्लिकेशन बनाने और उसे उपलब्ध कराने की अनुमति दी है, तो आपको पहले से दी जाने वाली सूचना का फ़ॉर्म भरकर ज़रूरी शर्तें पूरी करने का सबूत सबमिट करना होगा.
  - **संक्रमित व्यक्ति के संपर्क में आए लोगों का पता लगाना/स्वास्थ्य की जांच का नतीजा दिखाने वाले ऐप्लिकेशन:** अगर आपका ऐप्लिकेशन संक्रमित व्यक्ति के संपर्क में आए लोगों का पता लगाने और/या स्वास्थ्य की जांच का नतीजा दिखाने वाला ऐप्लिकेशन है, तो कृपया Play Console में "बीमारी से बचाव और सार्वजनिक स्वास्थ्य" को चुनें और पहले से सूचना देने के लिए इस्तेमाल होने वाला ऊपर दिया गया फ़ॉर्म भरकर ज़रूरी जानकारी दें.
  - **लोगों पर की जाने वाली रिसर्च से जुड़े ऐप्लिकेशन:** लोगों के स्वास्थ्य पर रिसर्च करने वाले ऐप्लिकेशन को सभी नियमों और कानूनों का पालन करना होगा. साथ ही, इस तरह की रिसर्च में शामिल होने वाले लोगों की सहमति लेना भी ज़रूरी है. अगर हिस्सा लेने वाले नाबालिग हों, तो उनके माता-पिता या अभिभावक की अनुमति लेनी होगी. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं. सेहत से जुड़ी रिसर्च करने वाले ऐप्लिकेशन को इंस्टिट्यूशनल रिव्यू बोर्ड (आईआरबी) और/या एथिक्स कमिटी से मंज़ूरी लेनी होगी. हालांकि, उन ऐप्लिकेशन को ऐसा करना ज़रूरी नहीं है जिन्हें इससे छूट दी गई हो. मांगे जाने पर, इस बात का सबूत देना होगा कि आपको यह मंज़ूरी मिल गई है.
  - **मेडिकल डिवाइस या SaMD ऐप्लिकेशन:** जिन ऐप्लिकेशन को मेडिकल डिवाइस या SaMD माना जाता है उनके पास क्लीयरेंस लेटर या अनुमति से जुड़ा कोई अन्य दस्तावेज़ होना चाहिए. यह दस्तावेज़, रेगुलेटरी अथॉरिटी या स्वास्थ्य से जुड़े ऐप्लिकेशन को मैनेज करने और उनसे जुड़े नियम लागू करने वाली संस्था देती है. मांगे जाने पर, इस बात का सबूत देना होगा कि आपको क्लीयरेंस या मंज़ूरी मिल गई है.

Health Connect से जुड़ा डेटा

जिस डेटा को Health Connect की अनुमतियों की मदद से ऐक्सेस किया जाता है उसे निजी और संवेदनशील माना जाता है. इस पर उपयोगकर्ता के डेटा से जुड़ी नीति लागू होती है. इसके अलावा, अन्य ज़रूरी शर्तें भी लागू होती हैं.

डॉक्टर के पर्चे पर मिलने वाली दवाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो डॉक्टर के पर्चे से मिलने वाली दवाओं को डॉक्टर के पर्चे के बगैर, खरीदने या बेचने की सुविधा उपलब्ध कराए.

वे प्रॉडक्ट या दवाइयां जिनके विज्ञापन की मंज़ूरी नहीं है

Google Play कानूनी दावे के बावजूद भी, उन प्रॉडक्ट या दवाइयों का प्रचार करने या बेचने वाले ऐप्लिकेशन को अनुमति नहीं देता है जिनके विज्ञापन की मंज़ूरी नहीं है.

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

- पाबंदी वाली दवाओं और सप्लीमेंट की उस सूची के सभी आइटम जिसमें पूरी जानकारी नहीं है.
- ऐसे प्रॉडक्ट जिनमें इफ़ेड्रा है.
- वज़न घटाने या वज़न कंट्रोल करने से जुड़े या एनाबॉलिक स्टेरॉइड के साथ प्रचार किए गए ह्यूमन कोरियोनिक गॉनाडोट्रॉपिन (एचसीजी) वाले प्रॉडक्ट.
- एक्टिव फ़ार्मास्यूटिकल या खतरनाक सामग्री वाले हर्बल और डाइट सप्लीमेंट.
- सेहत से जुड़े झूठे या गुमराह करने वाले दावे, जिनमें यह कहा गया हो कि प्रॉडक्ट डॉक्टर के पर्चे से मिलने वाली दवाओं या नियंत्रित पदार्थों की तरह काम करता है.
- किसी खास बीमारी या रोग को रोकने, उसका इलाज या देखभाल करने के लिए सुरक्षित या प्रभावी होने के दावे के साथ बेचे जाने वाले ऐसे प्रॉडक्ट जिनकी सरकार ने मंज़ूरी न दी हो.
- ऐसे प्रॉडक्ट जिन पर कोई सरकारी या कानूनी कार्रवाई या चेतावनी लागू हो.
- ऐसे प्रॉडक्ट जिनका नाम बिना मंज़ूरी वाली दवाओं या सप्लीमेंट या नियंत्रित पदार्थों से मिलता-जुलता हो.

बिना मंज़ूरी वाली या गुमराह करने वाली जिन दवाओं और सप्लीमेंट पर, हम नज़र रखते हैं उनके बारे में ज़्यादा जानकारी के लिए, कृपया www.legitscript.com पर जाएं.

इलाज के बारे में गलत जानकारी

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें सेहत के बारे में गुमराह करने वाले दावे किए गए हों. इनमें ऐसे दावे शामिल हैं जो चिकित्सा क्षेत्र की संस्थाओं या विशेषज्ञों से मान्यता पा चुकी जानकारी से मेल न खाते हों या जिनसे उपयोगकर्ताओं को नुकसान पहुंच सकता है.

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

- टीकों के बारे में गुमराह करने वाले दावे. जैसे, टीके से किसी व्यक्ति के डीएनए में बदलाव हो सकता है.
- इलाज के ऐसे तरीकों का प्रचार जो नुकसानदेह होते हैं और जिन्हें मंज़ूरी नहीं मिली है.
- इलाज के कुछ अन्य तरीकों का प्रचार जो सेहत को नुकसान पहुंचा सकते हैं. जैसे, सेक्शुअल ओरिएंटेशन (यौन रुझान) बदलने के लिए की जाने वाली थेरेपी.

इलाज से जुड़ी सुविधाएं

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें इलाज या सेहत से जुड़ी गुमराह करने वाली या नुकसान पहुंचा सकने वाली सुविधाएं शामिल हों. उदाहरण के लिए, हम उन ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जो सिर्फ़ ऐप्लिकेशन का इस्तेमाल करके, खून में ऑक्सीजन का लेवल जांचने यानी ऑक्सीमेट्री की सुविधा देने का दावा करते हैं. ऑक्सीमीटर की सुविधा देने वाले ऐप्लिकेशन ऐसे होने चाहिए जो किसी बाहरी हार्डवेयर, पहने जाने वाले डिवाइस के साथ काम करते हों या फिर उन्हें ऑक्सीमेट्री की सुविधा को सपोर्ट करने वाले स्मार्टफ़ोन सेंसर के साथ काम करने के लिए बनाया गया हो. इस तरह की सुविधाएं देने वाले ऐप्लिकेशन में खंडन करने वाला ऐसा मेटाडेटा होना चाहिए जो यह बताता हो कि ये ऐप्लिकेशन किसी इलाज के मकसद से नहीं बनाए गए हैं. इन्हें सिर्फ़ फ़िटनेस और सेहत से जुड़ी सामान्य जानकारी देने के मकसद से डिज़ाइन किया गया है. ऐसे ऐप्लिकेशन के साथ फ़ोन का इस्तेमाल, मेडिकल डिवाइस के तौर पर नहीं किया जाना चाहिए. साथ ही, इनमें साफ़ तौर पर यह भी ज़ाहिर किया जाना चाहिए कि कौनसे हार्डवेयर मॉडल/डिवाइस मॉडल के साथ ये काम करते हैं.

पैसे चुकाना - चिकित्सा से जुड़ी सेवाएं

कानून के दायरे में आने वाली चिकित्सा सेवाओं से जुड़े लेन-देन में, Google Play के बिलिंग सिस्टम का इस्तेमाल नहीं किया जाना चाहिए. ज़्यादा जानकारी के लिए, पेमेंट से जुड़ी Google Play की नीति को समझना देखें.

ब्लॉकचेन पर आधारित कॉन्टेंट

ब्लॉकचेन टेक्नोलॉजी तेज़ी से आगे बढ़ रही है. इसलिए, हमारा मकसद डेवलपर को ऐसा प्लैटफ़ॉर्म उपलब्ध कराना है जिसकी मदद से, वे कुछ नया कर सकें. साथ ही, ऐसा ऐप्लिकेशन बना सकें जिससे उपयोगकर्ताओं को नया और बेहतर अनुभव दिया जा सके.

इस नीति के हिसाब से हम ब्लॉकचेन पर आधारित कॉन्टेंट को टोकन के तौर पर मौजूद डिजिटल ऐसेट मानते हैं. यह एक ऐसी डिजिटल ऐसेट है जो ब्लॉकचेन में सुरक्षित रहती है. अगर आपके ऐप्लिकेशन में ब्लॉकचेन आधारित कॉन्टेंट मौजूद है, तो आपको ये ज़रूरी शर्तें पूरी करनी होंगी.

क्रिप्टो करंसी एक्सचेंज और सॉफ़्टवेयर वॉलेट

जिन देशों/इलाकों में क्रिप्टो करंसी मान्य हैं वहां क्रिप्टो करंसी की खरीदारी, होल्डिंग या लेन-देन किसी सर्टिफ़ाइड सेवा की मदद से किया जाना चाहिए.

आपको उस इलाके या देश में लागू होने वाले कानूनों का भी पालन करना होगा जहां आपको ऐप्लिकेशन उपलब्ध कराना है. साथ ही, उस देश या इलाके में इसे पब्लिश करने से बचना होगा जहां आपके प्रॉडक्ट और सेवाओं पर पाबंदी लगी हो. Google Play, लाइसेंस की ज़रूरी शर्तों को पूरा करने या लागू होने वाले किसी कानून के पालन के दस्तावेज़ या अतिरिक्त जानकारी देने का अनुरोध कर सकता है.

क्रिप्टो करंसी की माइनिंग

हम उन ऐप्लिकेशन को अनुमति नहीं देते हैं जो डिवाइसों पर क्रिप्टो करंसी की माइनिंग करते हैं. हम ऐसे ऐप्लिकेशन को मंज़ूरी देते हैं जो क्रिप्टो करंसी की माइनिंग को बारीकी से मैनेज करते हैं.

टोकन के तौर पर मौजूद डिजिटल ऐसेट के डिस्ट्रिब्यूशन में पारदर्शिता लाने से जुड़ी ज़रूरी शर्तें

अगर आपका ऐप्लिकेशन, टोकन के तौर पर मौजूद डिजिटल ऐसेट बेचता है या फिर इन्हें हासिल करने में उपयोगकर्ता की मदद करता है, तो आपको इस बारे में बताना होगा. इसके लिए, आपको Play Console के ऐप्लिकेशन कॉन्टेंट पेज पर मौजूद वित्तीय सूचना की जानकारी देने वाला फ़ार्म भरना होगा.

ऐप्लिकेशन में खरीदने के लिए उपलब्ध प्रॉडक्ट बनाते समय, आपको 'प्रॉडक्ट के बारे में जानकारी' सेक्शन में इस बात की जानकारी देनी होगी कि यह टोकन के तौर पर मौजूद एक डिजिटल ऐसेट है. ज़्यादा जानकारी के लिए, ऐप्लिकेशन में खरीदने के लिए प्रॉडक्ट बनाना पर जाएं.

गेम खेलने या ट्रेडिंग करने से हुई कमाई को बढ़ा-चढ़ाकर या लालच पैदा करने वाले तरीके से पेश नहीं किया जा सकता.

एनएफ़टी गेमिफ़िकेशन के लिए अन्य ज़रूरी शर्तें

Google Play की असली पैसे दांव पर लगाकर खेले जाने वाले जुए, गेम, और प्रतियोगिताओं से जुड़ी नीति के मुताबिक, जुआ खेलने की सुविधा देने वाले उन ऐप्लिकेशन के लिए आवेदन की प्रक्रिया पूरी करना ज़रूरी है जो एनएफ़टी जैसी टोकन वाली डिजिटल ऐसेट का इंटिग्रेशन करते हैं.

ऐसे ऐप्लिकेशन जो जुआ खेलने की सुविधा देने वाले ऐप्लिकेशन की ज़रूरी शर्तों को पूरा नहीं करते और न ही असली पैसे दांव पर लगाकर खेले जाने वाले अन्य गेम के पायलट कार्यक्रम में शामिल हैं उन्हें अज्ञात कीमत के एनएफ़टी पाने के बदले असल पैसे की कोई भी चीज़ स्वीकार नहीं करनी चाहिए. खरीदे गए एनएफ़टी को इस्तेमाल कर लेना चाहिए या उनका इस्तेमाल गेम के अनुभव को बेहतर बनाने में किया जाना चाहिए. इसके अलावा, गेम में अगले लेवल पर जाने के लिए भी उनका इस्तेमाल किया जा सकता है. एनएफ़टी को असल दुनिया में किसी कीमत वाले पुरस्कार को पाने के लिए न तो गेम में दांव पर लगाया जाना चाहिए और न ही किसी तरह के लेन-देन में शामिल करना चाहिए. इनमें, अन्य एनएफ़टी भी शामिल हैं.

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

- बंडल में एनएफ़टी बेचने वाले ऐसे ऐप्लिकेशन जो इनका कॉन्टेंट और वैल्यू ज़ाहिर नहीं करते.
- पैसे देकर खेले जाने वाले ऐसे सोशल कसीनो गेम जो इनाम के तौर पर एनएफ़टी देते हैं. जैसे- स्लॉट मशीन.

एआई से बनाया गया कॉन्टेंट

जब जनरेटिव एआई मॉडल ज़्यादा जगहों पर डेवलपर के लिए उपलब्ध होंगे, तब इन मॉडल को अपने ऐप्लिकेशन में शामिल किया जा सकेगा. इनकी मदद से, ज़्यादा से ज़्यादा उपयोगकर्ताओं को अपने ऐप्लिकेशन से जोड़ा जा सकेगा और उन्हें बेहतर उपयोगकर्ता अनुभव भी दिया जा सकेगा. Google Play यह पक्का करने में डेवलपर की मदद करना चाहता है कि एआई से बनाया गया कॉन्टेंट सभी उपयोगकर्ताओं के लिए सुरक्षित हो. साथ ही, उपयोगकर्ताओं से मिले सुझावों की मदद से डेवलपर बेहतर ऐप्लिकेशन तैयार कर सकें.

एआई से बनाया गया कॉन्टेंट

उपयोगकर्ता के दिए गए प्रॉम्प्ट के आधार पर, जनरेटिव एआई मॉडल की मदद से तैयार किए गए कॉन्टेंट को, एआई से बनाया गया कॉन्टेंट कहा जाता है. एआई से बनाए गए कॉन्टेंट के कुछ उदाहरण यहां दिए गए हैं:

- वे टेक्स्ट जो जनरेटिव एआई चैटबॉट बातचीत के दौरान लिखता है. इसमें, चैटबॉट से इंटरैक्शन करना ही ऐप्लिकेशन की मुख्य सुविधा होती है
- टेक्स्ट, इमेज या वॉइस प्रॉम्प्ट के आधार पर एआई की मदद से तैयार की गई इमेज

उपयोगकर्ता को आपत्तिजनक कॉन्टेंट से बचाने के लिए और Google Play की नीति के पालन के लिए, उन सभी ऐप्लिकेशन को डेवलपर के लिए बनाई गई Google Play की मौजूदा नीतियों का पालन करना होगा जो एआई की मदद से कॉन्टेंट तैयार करते हैं. इसके तहत, बच्चों के यौन शोषण को बढ़ावा देने और धोखा देने वाले प्रतिबंधित कॉन्टेंट को तैयार करने पर रोक लगाना और उसे प्रतिबंधित करना शामिल है.

एआई की मदद से कॉन्टेंट तैयार करने वाले ऐप्लिकेशन के लिए ज़रूरी है कि उनके अंदर ही, उपयोगकर्ताओं के लिए आपत्तिजनक कॉन्टेंट को रिपोर्ट या फ़्लैग करने की सुविधा उपलब्ध हो. इसके लिए, उपयोगकर्ताओं को ऐप्लिकेशन बंद करके बाहर न निकलना पड़े. साथ ही, उपयोगकर्ताओं की रिपोर्ट की मदद से डेवलपर, कॉन्टेंट फ़िल्टर करने की सुविधा के बारे में जानकारी दें और अपने ऐप्लिकेशन पहले से बेहतर बनाएं.

बौद्धिक संपत्ति

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

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

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

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

अगर आपके पास कोई ऐसा दस्तावेज़ है, जो आपको अपने ऐप्लिकेशन या स्टोर पेज (जैसे ब्रैंड का नाम, लोगो, और ग्राफ़िक रचनाएं) में किसी तीसरे पक्ष की बौद्धिक संपत्ति का इस्तेमाल करने की अनुमति देता है, तो आप सबमिशन से पहले ही Google Play टीम से संपर्क करें. इससे आप यह पक्का कर सकते हैं कि आपका ऐप्लिकेशन बौद्धिक संपत्ति के उल्लंघन के लिए अस्वीकार न हो जाए.

कॉपीराइट वाले कॉन्टेंट का बिना मंज़ूरी इस्तेमाल करना

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

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

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

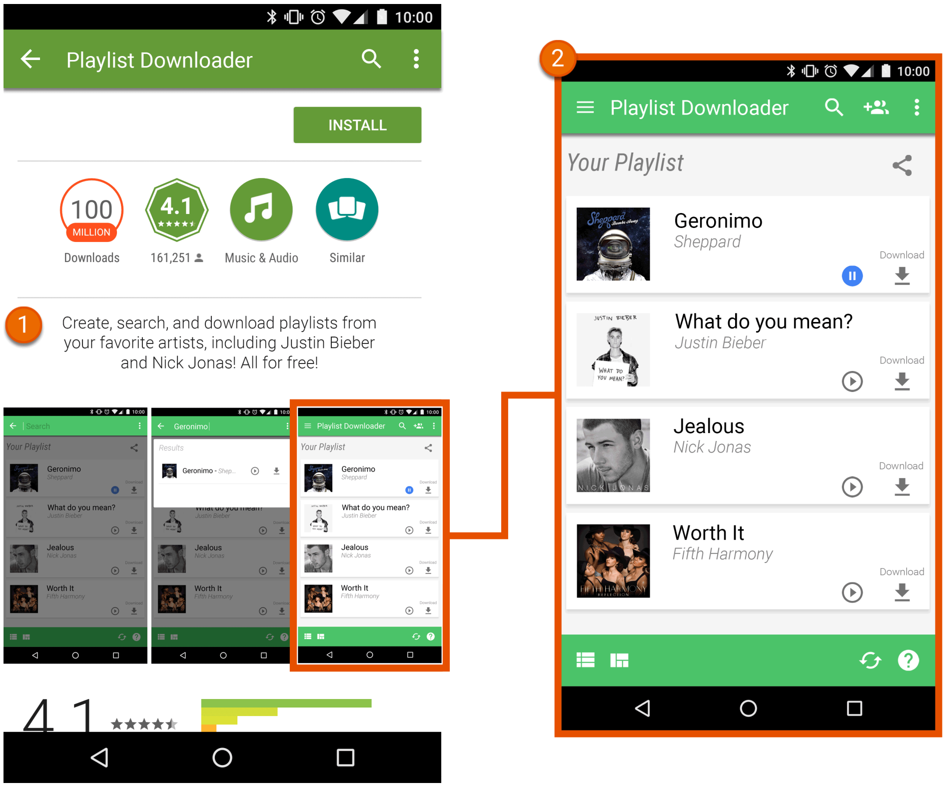
- संगीत एल्बम, वीडियो गेम, और किताबों के लिए कवर आर्ट.
- फ़िल्मों, टेलीविजन या वीडियो गेम की मार्केटिंग इमेज.
- कॉमिक बुक, कार्टून, फ़िल्मों, संगीत वीडियो या टेलीविज़न के आर्टवर्क या इमेज.
- कॉलेज और पेशेवर खेल टीम के लोगो.
- किसी लोकप्रिय हस्ती के सोशल मीडिया खाते से ली गई फ़ोटो.
- लोकप्रिय हस्तियों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

कॉपीराइट के उल्लंघन को बढ़ावा देना

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

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

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



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

ट्रेडमार्क का उल्लंघन करना

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

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

नकली

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

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.

उपयोगकर्ता का डेटा

उपयोगकर्ता के डेटा को कैसे संभाला जाता है, इस बारे में आपको साफ़ तौर पर जानकारी देनी चाहिए. उदाहरण के लिए, किसी उपयोगकर्ता इकट्ठा की गई या उसके बारे में इकट्ठा की गई जानकारी. इसमें डिवाइस की जानकारी भी शामिल है. इसका मतलब है कि

आपको यह ज़ाहिर करना चाहिए कि आपके ऐप्लिकेशन से, लोगों का कौनसा डेटा ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर किया जा रहा है. साथ ही, यह भी ज़ाहिर किया जाना चाहिए कि आपका ऐप्लिकेशन, नीति का पालन करते हुए किसी और काम के लिए लोगों के डेटा का इस्तेमाल नहीं करता है. कृपया ध्यान रखें कि उपयोगकर्ता के निजी और संवेदनशील डेटा का कोई भी रखरखाव, नीचे दिए गए "उपयोगकर्ता का निजी और संवेदनशील डेटा" सेक्शन में बताई गई अन्य ज़रूरी शर्तों पर भी निर्भर करता है. Google Play की ये ज़रूरी शर्तें, निजता और डेटा की सुरक्षा के लागू कानूनों में बताई गई ज़रूरी शर्तों से अलग हैं.

अगर आपके ऐप्लिकेशन में तीसरे पक्ष के कोड (उदाहरण के लिए, कोई SDK टूल) का इस्तेमाल किया जा रहा है, तो आपको यह पक्का करना होगा कि आपके ऐप्लिकेशन में इस्तेमाल किया गया तीसरे पक्ष का कोड और उस तीसरे पक्ष की ओर से उपयोगकर्ता के डेटा का किया गया इस्तेमाल, Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक हो. इसमें, डेटा के इस्तेमाल और साफ़ तौर पर जानकारी ज़ाहिर करने से जुड़ी शर्तों को पूरा करना भी शामिल है. उदाहरण के लिए, आपको यह पक्का करना होगा कि ऐप्लिकेशन में जिन कंपनियों के SDK टूल इस्तेमाल किए जा रहे हैं वे आपके ऐप्लिकेशन से मिले उपयोगकर्ता के निजी और संवेदनशील डेटा को बेचती न हों. यह ज़रूरी शर्त हर हाल में लागू होगी. भले ही, उपयोगकर्ता का डेटा, सर्वर पर भेजने के बाद ट्रांसफ़र किया गया हो या आपके ऐप्लिकेशन में तीसरे पक्ष के कोड को एम्बेड करने के बाद उसे ट्रांसफ़र किया गया हो.

उपयोगकर्ता का निजी और संवेदनशील डेटा

उपयोगकर्ता के निजी और संवेदनशील डेटा में व्यक्तिगत पहचान से जुड़ी जानकारी, वित्तीय और क्रेडिट/डेबिट कार्ड की जानकारी, पुष्टि करने की जानकारी, फ़ोनबुक, संपर्क, डिवाइस की जगह की जानकारी, एसएमएस और कॉल से जुड़ा डेटा, स्वास्थ्य की जानकारी से जुड़ा डेटा, Health Connect से मिला डेटा, डिवाइस पर मौजूद अन्य ऐप्लिकेशन की इन्वेंट्री, माइक्रोफ़ोन, कैमरा, और अन्य संवेदनशील डिवाइस या उसके इस्तेमाल के बारे में डेटा शामिल होता है. हालांकि, इसमें इनके अलावा अन्य जानकारी भी शामिल हो सकती है. अगर आपका ऐप्लिकेशन, उपयोगकर्ता का निजी और संवेदनशील डेटा मैनेज करता है, तो आपको इन बातों का ध्यान रखना चाहिए:

- एक ऐप्लिकेशन से दूसरे ऐप्लिकेशन पर या सेवा लागू करके, उपयोगकर्ता के लिए गए निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करने की सुविधा को सीमित करें. साथ ही, नीतियों का पालन करते हुए, उपयोगकर्ता की उम्मीद के हिसाब से इकट्ठा किए गए डेटा का भी सीमित इस्तेमाल करें:
  - विज्ञापन दिखाने के लिए उपयोगकर्ता के निजी और संवेदनशील डेटा का इस्तेमाल करने वाले ऐप्लिकेशन को Google Play की विज्ञापन नीति का पालन करना होगा.
  - ज़रूरत पड़ने पर, आपको सेवा देने वाली कंपनियों को डेटा ट्रांसफ़र करना पड़ सकता है या ऐसा कानूनी वजहों से भी हो सकता है. जैसे- किसी मान्य सरकारी अनुरोध या लागू कानून का पालन करने के लिए. इसके अलावा, आपको उपयोगकर्ताओं को कानूनी रूप से ज़रूरी सूचना देकर, किसी मर्जर या मालिकाना हक के लिए भी डेटा ट्रांसफ़र करना पड़ सकता है.
- उपयोगकर्ता के सभी निजी और संवेदनशील डेटा को सुरक्षित तरीके से मैनेज करना चाहिए. इसमें, आधुनिक क्रिप्टोग्राफ़ी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करके डेटा को ट्रांसफ़र करना भी शामिल है.
- Android की अनुमतियों से सुरक्षित किया गया डेटा ऐक्सेस करने से पहले, जब भी रनटाइम अनुमतियां उपलब्ध हों, तब इनके अनुरोध का इस्तेमाल करें.
- उपयोगकर्ता के निजी और संवेदनशील डेटा को बेचना नहीं चाहिए.
  - "बिक्री" का मतलब है कि कमाई करने के मकसद से, उपयोगकर्ता के निजी और संवेदनशील डेटा को किसी तीसरे पक्ष से आपस में शेयर या ट्रांसफ़र करना.
    - उपयोगकर्ता के निजी और संवेदनशील डेटा को उन्हीं की ओर से ट्रांसफ़र करने (जैसे- जब उपयोगकर्ता किसी तीसरे पक्ष को फ़ाइल ट्रांसफ़र करने के लिए, ऐप्लिकेशन की किसी सुविधा का इस्तेमाल करता है या किसी ऐसे ऐप्लिकेशन का इस्तेमाल करता है जिसका खास मकसद, खोज या अध्ययन करना हो) की प्रक्रिया को बिक्री के तौर पर नहीं माना जाता है.

साफ़ तौर पर जानकारी देने और सहमति देने से जुड़ी ज़रूरी शर्तें

ऐसे मामले जहां दिए गए सवाल में प्रॉडक्ट या सुविधा का इस्तेमाल करने वाले उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल या शेयर करने की सुविधा उपयोगकर्ता की उम्मीद के हिसाब से नहीं बताई जाती है (उदाहरण के लिए, ऐप्लिकेशन के बैकग्राउंड में डेटा तब इकट्ठा किया जाना, जब उपयोगकर्ता आपके ऐप्लिकेशन का इस्तेमाल न करता हो), तो आपको नीचे दी गई ज़रूरी शर्तें पूरी करनी होंगी:

साफ़ तौर पर जानकारी ज़ाहिर करना: आपको डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने से जुड़ी जानकारी ऐप्लिकेशन में 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 दिखनी चाहिए और उपयोगकर्ता को इसके लिए मेन्यू या सेटिंग में जाने की ज़रूरत नहीं पड़नी चाहिए;
- इसमें ऐक्सेस या इकट्ठा किए जा रहे डेटा की पूरी जानकारी दी जानी चाहिए;
- इसमें यह बताया जाना चाहिए कि डेटा को कैसे इस्तेमाल और/या शेयर किया जाएगा;

- इसे सिर्फ़ किसी निजता नीति या सेवा की शर्तों में नहीं रखा जा सकता; और
- इसे ऐसी दूसरी जानकारी के साथ नहीं दिखाया जाना चाहिए जो उपयोगकर्ता के निजी और संवेदनशील डेटा इकट्ठा करने से जुड़ी नहीं है.

सहमति और रनटाइम से जुड़ी अनुमतियां: उपयोगकर्ता की सहमति और रनटाइम की अनुमति पाने से जुड़े अनुरोधों के ठीक पहले, ऐप्लिकेशन में ऐसा मैसेज दिखाया जाना चाहिए जो यह ज़ाहिर करता हो कि वह ऐप्लिकेशन नीति की ज़रूरी शर्तों को पूरा करता है. सहमति के लिए ऐप्लिकेशन का अनुरोध:

- सहमति संवाद को साफ़ और सीधे तौर पर पेश किया जाना चाहिए;
- ऐसा कोई विकल्प ज़रूर देना चाहिए जिसका इस्तेमाल करके लोग अपनी सहमति दे सकें. जैसे- स्वीकार करने के लिए टैप करने और चेक बॉक्स पर सही का निशान लगाने का विकल्प;
- अगर उपयोगकर्ता, जहां जानकारी दी गई है वहां से कहीं और जाता है (उदाहरण के लिए, टैप करके बाहर जाना या वापस जाने वाला बटन या होम बटन दबाना), तो इसे उसकी सहमति नहीं समझनी चाहिए;
- उपयोगकर्ता की सहमति लेने के लिए, अपने-आप खारिज या खत्म होने वाले मैसेज का इस्तेमाल नहीं किया जाना चाहिए; और
- आपके ऐप्लिकेशन को उपयोगकर्ता के निजी और संवेदनशील डेटा को इकट्ठा या ऐक्सेस करने से पहले, उपयोगकर्ता की अनुमति लेनी होगी.

ऐसे ऐप्लिकेशन जो उपयोगकर्ता के निजी और संवेदनशील डेटा को सहमति के बिना प्रोसेस करने के लिए, अन्य कानूनी आधारों पर भरोसा करते हैं (जैसे कि ईयू जीडीपीआर के तहत कानूनी हित) उन्हें इस नीति के तहत लागू होने वाली सभी कानूनी शर्तों को पूरा करना होगा और उपयोगकर्ताओं को इसके बारे में साफ़ तौर पर बताना होगा. इसमें, इस नीति के तहत ज़रूरत के मुताबिक ऐप्लिकेशन में ज़ाहिर की जाने वाली जानकारी भी शामिल है.

नीति से जुड़ी ज़रूरी शर्तें पूरी करने के लिए, यह सलाह दी जाती है कि रेफ़रंस के लिए, आप साफ़ तौर पर जानकारी ज़ाहिर करने (ज़रूरत पड़ने पर) के लिए नीचे दिए गए उदाहरण का फ़ॉर्मैट देखें:

- “[in what scenario] में ["feature"] को चालू करने के लिए, [This app] [type of data] को इकट्ठा/शेयर/सिंक/स्टोर करता है."
- *उदाहरण: “Fitness Funds, ऐप्लिकेशन बंद होने या इस्तेमाल में न होने पर भी फ़िटनेस ट्रैकिंग को चालू रखने के लिए, जगह की जानकारी का डेटा इकट्ठा करता है. इसका इस्तेमाल, विज्ञापन के लिए भी किया जाता है.”*
- *उदाहरण: “Call buddy, कॉल लॉग के डेटा को इकट्ठा करता है, पढ़ता है, और लिखता है, ताकि ऐप्लिकेशन के इस्तेमाल में न होने पर भी संगठन को संपर्क करने की सुविधा चालू रखी जा सके.”*

अगर आपका ऐप्लिकेशन तीसरे पक्ष के किसी ऐसे कोड (उदाहरण के लिए, कोई SDK टूल) को जोड़ता है जिसे डिफ़ॉल्ट तौर पर उपयोगकर्ता के निजी और संवेदनशील डेटा को इकट्ठा करने के लिए डिज़ाइन किया गया है, तो आपको Google Play से अनुरोध मिलने के दो हफ़्तों के अंदर (या अगर उस समयावधि के अंदर, Google Play का अनुरोध लंबी अवधि के लिए दिया जाता है), इसके ज़रूरी सबूत देने होंगे कि आपका ऐप्लिकेशन इस नीति की साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों को पूरा करता है. इसमें, तीसरे पक्ष के कोड की मदद से, डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल या शेयर करने की जानकारी भी शामिल है.

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

- ऐप्लिकेशन, डिवाइस की जगह की जानकारी इकट्ठा करता है, लेकिन इसमें यह साफ़ तौर नहीं बताया जाता कि कौनसी सुविधाएं इस डेटा का इस्तेमाल करती हैं और/या ऐप्लिकेशन बैकग्राउंड में इस डेटा का इस्तेमाल करता है.
- ऐप्लिकेशन में साफ़ तौर पर जानकारी ज़ाहिर करने से पहले, डेटा ऐक्सेस करने वाले रनटाइम की अनुमति से जुड़ा अनुरोध दिखता है, जो यह बताता है कि डेटा का इस्तेमाल किस वजह से किया जाता है.
- 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 मैनेज करने, 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 किसी व्यक्ति के फ़ोन या संपर्क सूची के डेटा को ऐक्सेस करता है और इस डेटा को ऊपर बताई गई निजता नीति, डेटा मैनेज करने, खास तौर पर जानकारी देने, और सहमति पाने की ज़रूरी शर्तों के मुताबिक, निजी या संवेदनशील डेटा के रूप में नहीं देखता है.
- ऐसा ऐप्लिकेशन जो किसी व्यक्ति की स्क्रीन रिकॉर्ड करता है और इस डेटा को इस नीति के मुताबिक, 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 सहमति भी नहीं लेता है.
- ऐसा ऐप्लिकेशन जो ट्रैकिंग, रिसर्च या मार्केटिंग के मकसद से, ऐप्लिकेशन के बैकग्राउंड में पाबंदी वाली अनुमतियों को इस्तेमाल करता है और इसके इस्तेमाल के बारे में पूरी जानकारी नहीं देता है. साथ ही, ऊपर दी गई ज़रूरी शर्तों के मुताबिक सहमति लेता है.

- SDK टूल वाला ऐसा ऐप्लिकेशन जिसमें उपयोगकर्ता का निजी और संवेदनशील डेटा इकट्ठा किया जाता है. साथ ही, जिसमें इस डेटा को उपयोगकर्ता के डेटा से जुड़ी नीति, उसे ऐक्सेस करने, मैनेज करने, और साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों के तौर पर नहीं देखा जाता है. इसमें, बिना अनुमति की बिक्री भी शामिल है.

साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्त के बारे में ज़्यादा जानकारी के लिए, यह लेख पढ़ें.

निजी और संवेदनशील जानकारी ऐक्सेस करने से जुड़ी पाबंदियां

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

गतिविधि	ज़रूरी शर्त
आपका ऐप्लिकेशन, वित्तीय या क्रेडिट/डेबिट कार्ड की जानकारी या सरकारी पहचान संख्याओं को मैनेज करता है	आपके ऐप्लिकेशन को वित्तीय या पेमेंट से जुड़ी गतिविधियों या किसी भी सरकारी पहचान संख्या से जुड़ा, उपयोगकर्ता का निजी और संवेदनशील डेटा, सार्वजनिक तौर पर ज़ाहिर नहीं करना चाहिए.
आपका ऐप्लिकेशन ऐसे फ़ोनबुक या संपर्क जानकारी को मैनेज करता है जो सार्वजनिक नहीं 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 प्राइवेसी पॉलिसी पोस्ट करनी चाहिए जिसमें ऐप्लिकेशन में दी गई किसी जानकारी के साथ यह भी बताया जाए कि आपका ऐप्लिकेशन, उपयोगकर्ता का कौनसा डेटा इकट्ठा करता है और दूसरों तक पहुंचाता है. साथ ही, पॉलिसी में यह भी बताया जाए कि उस डेटा का इस्तेमाल किस तरह से किया जाता है. इसके अलावा, प्राइवेसी पॉलिसी में उन ग्रुप की जानकारी भी शामिल होनी चाहिए जिनके साथ डेटा शेयर किया जाता है.
अगर आपका ऐप्लिकेशन बच्चों को टारगेट करता है	आपके ऐप्लिकेशन को ऐसे SDK टूल का इस्तेमाल नहीं करना चाहिए जिसे बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी नहीं मिली है. पूरी पॉलिसी और ज़रूरी शर्तों को देखने के लिए, बच्चों और परिवारों के लिए ऐप्लिकेशन बनाना लेख पर जाएं.
अगर आपका ऐप्लिकेशन, डिवाइस के स्थायी पहचानकर्ताओं (उदाहरण के लिए, IMEI, IMSI, SIM Serial # वगैरह) को इकट्ठा करता है या उनको जोड़ता है	डिवाइस के स्थायी पहचानकर्ताओं को उपयोगकर्ताओं के अन्य निजी और संवेदनशील डेटा या डिवाइस के रीसेट हो सकने वाले पहचानकर्ताओं से नहीं जोड़ा जा सकता. हालांकि, नीचे बताए गए मकसदों के लिए ऐसा किया जा सकता है • किसी सिम कार्ड की पहचान से जुड़ी टेलिफ़ोन सेवा (उदाहरण के लिए, मोबाइल और इंटरनेट सेवा देने वाली कंपनी के खाते से जुड़ी, वाई-फ़ाई कॉलिंग की सुविधा) के लिए और • एंटरप्राइज़ से जुड़े डिवाइस को मैनेज करने वाले ऐसे ऐप्लिकेशन के लिए, जिनमें डिवाइस मालिक वाले मोड का इस्तेमाल होता है. इस तरह के इस्तेमाल की जानकारी, उपयोगकर्ताओं को साफ़ तौर पर ज़ाहिर की जानी चाहिए, जैसा कि उपयोगकर्ता के डेटा से जुड़ी पॉलिसी में बताया गया है. खास पहचानकर्ताओं के विकल्प के लिए, कृपया यह लेख पढ़ें. Android की विज्ञापन आईडी से जुड़े अन्य दिशा-निर्देशों के लिए, कृपया विज्ञापन पॉलिसी को पढ़ें.

डेटा की सुरक्षा वाला सेक्शन

सभी डेवलपर के लिए यह ज़रूरी है कि वे हर ऐप्लिकेशन के डेटा की सुरक्षा वाले सेक्शन में पूरी जानकारी दें. इसमें, उपयोगकर्ता के निजी और संवेदनशील डेटा को इकट्ठा, इस्तेमाल, और शेयर करने के बारे में साफ़ और सही तौर पर बताना होगा. इस लेबल के सही होने और इसकी जानकारी को अप-टू-डेट रखने की ज़िम्मेदारी डेवलपर की है. जहां ज़रूरी हो वहां डेटा की सुरक्षा वाले सेक्शन और ऐप्लिकेशन की निजता नीति, दोनों ही जगह पर दी गई जानकारी एक जैसी होनी चाहिए.

डेटा की सुरक्षा वाले सेक्शन को भरने से जुड़ी ज़्यादा जानकारी के लिए, कृपया यह लेख पढ़ें.

निजता नीति

सभी ऐप्लिकेशन डेवलपर के लिए ज़रूरी है कि वे Play Console में, तय की गई जगह पर निजता नीति का लिंक पोस्ट करें. इसके अलावा, उन्हें ऐप्लिकेशन के अंदर भी निजता नीति का लिंक या टेक्स्ट पोस्ट करना होगा. निजता नीति में, ऐप्लिकेशन में ज़ाहिर की जाने वाली जानकारी के साथ-साथ, इस बात की पूरी जानकारी भी साफ़ तौर पर दी जानी चाहिए कि आपका ऐप्लिकेशन, उपयोगकर्ता के डेटा को कैसे ऐक्सेस, इकट्ठा, शेयर, और इस्तेमाल करता है. डेटा की सुरक्षा वाले सेक्शन में दी गई जानकारी के अलावा, यह जानकारी भी देनी होगी. इसमें नीचे बताई गई जानकारी भी शामिल होनी चाहिए:

- डेवलपर की जानकारी और निजता से जुड़े सवालों के लिए, संपर्क करने या सवालों को सबमिट करने का कोई तरीका.
- आपकी निजता नीति में यह शामिल होना चाहिए कि आपका ऐप्लिकेशन, उपयोगकर्ता के किस तरह के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करता है. साथ ही, आपको यह भी बताना होगा कि इस डेटा को किन पक्षों के साथ शेयर

किया जाता है.

- उपयोगकर्ता के निजी और संवेदनशील डेटा को सुरक्षित तरीके से मैनेज करना.
- डेटा मिटाने और उसका रखरखाव करने की डेवलपर की नीति.
- लेबल पर साफ़ तौर पर निजता नीति लिखा होना चाहिए (उदाहरण के लिए, शीर्षक में “निजता नीति”).

निजता नीति में उसी इकाई (जैसे कि डेवलपर या कंपनी) का नाम दिया जाना चाहिए जिसका नाम Google Play पर मौजूद, ऐप्लिकेशन के स्टोर पेज पर दिया गया हो या फिर निजता नीति में, ऐप्लिकेशन का नाम दिया जाना चाहिए. ऐसे ऐप्लिकेशन जो उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस नहीं करते, उन्हें भी निजता नीति सबमिट करनी होगी.

कृपया यह पक्का करें कि आपकी निजता नीति किसी ऐसे यूआरएल (PDFs नहीं) पर उपलब्ध हो जो काम करता हो, जिसे सभी ऐक्सेस कर सकें, और जिसकी जियोफ़ेंसिंग नहीं की गई है. साथ ही, उसमें बदलाव न किया जा सके.

खाता मिटाने की ज़रूरी शर्तें

अगर उपयोगकर्ताओं को आपके ऐप्लिकेशन में अपना खाता बनाने की सुविधा है, तो उन्हें अपना खाता मिटाने का अनुरोध करने की अनुमति भी मिलनी चाहिए. ऐप्लिकेशन में बनाए गए खाते को मिटाने की प्रक्रिया शुरू करने के लिए, आपके ऐप्लिकेशन में एक ऐसा विकल्प होना चाहिए जिसे उपयोगकर्ता आसानी से खोज सकें. उपयोगकर्ताओं के पास यह विकल्प भी होना चाहिए कि वे आपके ऐप्लिकेशन के बाहर से भी खाता मिटाने की प्रक्रिया शुरू कर सकें. जैसे, आपकी वेबसाइट पर जाकर. इस वेबसाइट का एक लिंक, Play Console में यूआरएल के लिए तय जगह पर डालना होगा.

किसी उपयोगकर्ता के अनुरोध पर, ऐप्लिकेशन में बनाए गए किसी खाते को मिटाने पर, आपको उस खाते का डेटा भी मिटाना होगा. ऐप्लिकेशन में बनाए गए खाते को कुछ समय के लिए हटाना, बंद करना या "फ़्रीज" करना, खाता मिटाने की गिनती में नहीं आएगा. अगर आपको किसी कानूनी वजह, जैसे कि सुरक्षा, धोखाधड़ी से रोकथाम या कानून के पालन के लिए कुछ डेटा को अपने पास रखने की ज़रूरत है, तो आपको उपयोगकर्ताओं को डेटा के रखरखाव के अपने तरीकों के बारे में साफ़ तौर पर बताना होगा. जैसे, अपनी निजता नीति में.

खाता मिटाने की ज़रूरी शर्तों के बारे में ज़्यादा जानने के लिए, सहायता केंद्र का यह लेख पढ़ें. डेटा सुरक्षा फ़ॉर्म को अपडेट करने के बारे में ज़्यादा जानकारी के लिए, यह लेख पढ़ें.

ऐप्लिकेशन सेट आईडी का इस्तेमाल

कुछ ज़रूरी मामलों में आपकी मदद के लिए, Android नई आईडी लाने वाला है. इन मामलों में, धोखाधड़ी से बचना और एनालिटिक्स शामिल हैं. इस आईडी के इस्तेमाल की शर्तें नीचे दी गई हैं.

- **इस्तेमाल**: ऐप्लिकेशन सेट आईडी का इस्तेमाल, दिलचस्पी के मुताबिक विज्ञापन दिखाने और विज्ञापनों के आकलन के लिए नहीं किया जाना चाहिए.
- **व्यक्तिगत पहचान से जुड़ी जानकारी या अन्य पहचानकर्ता से कनेक्ट करना:** ऐप्लिकेशन सेट आईडी को विज्ञापन के मकसद से, किसी भी Android पहचानकर्ता (उदाहरण के लिए, AAID) या निजी और संवेदनशील जानकारी से कनेक्ट नहीं किया जा सकता.
- **पारदर्शिता और सहमति:** उपयोगकर्ताओं को ऐप्लिकेशन सेट आईडी इकट्ठा और इस्तेमाल करने की जानकारी, कानूनी तौर पर ज़रूरी निजता सूचना में दी जानी चाहिए. यह जानकारी प्राइवेसी पॉलिसी में भी दी जानी चाहिए. इनमें, इन शर्तों को पूरा करने के वादों के बारे में भी बताया जाना चाहिए. ज़रूरत पड़ने पर, आपको उपयोगकर्ताओं से कानूनी तौर पर मान्य सहमति लेनी होगी. निजता मानकों के बारे में ज़्यादा जानकारी के लिए, कृपया उपयोगकर्ता के डेटा की पॉलिसी देखें.

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

अगर आप Google की ओर से दी गई ऐसी निजी जानकारी को ऐक्सेस, प्रोसेस या उसका इस्तेमाल करते हैं जो सीधे तौर पर या दूसरे तरीके से किसी व्यक्ति की पहचान करती है और जो मूल रूप से यूरोपीय संघ या स्विट्ज़रलैंड में जनरेट हुई (“यूरोपीय संघ की निजी जानकारी”) है, तो आपको ये काम करने होंगे:

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

आपको समय-समय पर देखना होगा कि इन शर्तों का पालन ठीक तरीके से हो रहा है या नहीं. अगर आप किसी भी समय इन शर्तों का पालन नहीं कर पाते (या अगर इस बात का जोखिम ज़्यादा है कि आप उनका पालन नहीं कर पाएंगे), तो ज़रूरी है कि आप हमें data-

protection-office@google.com पर ईमेल करके तुरंत सूचना दें. साथ ही, आपको यूरोपीय संघ से जुड़ी निजी जानकारी को प्रोसेस करना तुरंत रोक देना चाहिए या सुरक्षा के स्तर को पहले जैसा बनाए रखने के लिए उचित और ज़रूरी कदम उठाने चाहिए.

Google मूल रूप से यूरोपियन इकनॉमिक एरिया या यूके में जनरेट हुए डेटा को अमेरिका में ट्रांसफ़र करने के लिए, अब EU-U.S. Privacy Shield (यूरोपीय संघ–अमेरिका Privacy Shield) पर निर्भर नहीं रह गया है. यह निर्भरता 16 जुलाई, 2020 से खत्म हो गई है. (ज़्यादा जानें.) DDA के सेक्शन 9 में इससे जुड़ी ज़्यादा जानकारी दी गई है.

संवेदनशील जानकारी को ऐक्सेस करने वाले एपीआई और अनुमतियां

संवेदनशील जानकारी को ऐक्सेस करने वाले सिर्फ़ ऐसे एपीआई और अनुमतियों के लिए अनुरोध करें जो उपयोगकर्ताओं के काम की हों. संवेदनशील जानकारी को ऐक्सेस करने वाले सिर्फ़ ऐसे एपीआई या अनुमतियों के लिए अनुरोध किया जा सकता है जो आपके ऐप्लिकेशन में, उन मौजूदा सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं जिनके बारे में आपने Google Play के स्टोर पेज पर बताया हो. ऐसे एपीआई या अनुमतियों का इस्तेमाल नहीं किया जा सकता जिनमें उन सुविधाओं या उद्देश्यों के लिए उपयोगकर्ता या डिवाइस के डेटा को ऐक्सेस देते हैं जिनकी जानकारी न दी गई हो. इनका इस्तेमाल उन सुविधाओं या उद्देश्य के लिए भी नहीं किया जा सकता जिनकी जानकारी न दी गई हो, जो ऐप्लिकेशन में लागू न किया गया हो, जिनकी स्वीकृति न हो. अनुमतियों या एपीआई की मदद से, ऐक्सेस किए गए निजी या संवेदनशील डेटा को न तो कभी बेचा जा सकता है और न ही इसे बिक्री की सुविधा देने के मकसद से शेयर किया जा सकता है.

संवेदनशील जानकारी को ऐक्सेस करने वाली अनुमतियों या एपीआई के लिए, ज़रूरत के मुताबिक डेटा ऐक्सेस करने का अनुरोध करें, ताकि उपयोगकर्ता यह समझ सकें कि आपके ऐप्लिकेशन को अनुमति क्यों चाहिए. ऐसा ज़्यादा अनुमतियां मांगने की सुविधा की मदद से किया जा सकता है. डेटा का इस्तेमाल सिर्फ़ उन मकसद के लिए करें जिनके लिए उपयोगकर्ता ने सहमति दी है. अगर बाद में दूसरे मकसद के लिए डेटा का इस्तेमाल करना है, तो आपको उपयोगकर्ताओं से पूछना होगा और यह पक्का करना होगा कि वे डेटा के अतिरिक्त इस्तेमाल के लिए पूरी तरह से सहमत हों.

पाबंदी वाली अनुमतियां

ऊपर बताई गई अनुमतियों के अलावा, पाबंदी वाली अनुमतियां वे होती हैं जिन्हें हमारे डेवलपर दस्तावेज़ में खतरनाक , खास , अहम के तौर पर शामिल किया गया है या जिनके बारे में नीचे बताया गया है. ये अनुमतियां नीचे दी गई अन्य ज़रूरी शर्तों और पाबंदियों पर निर्भर करती हैं:

- उपयोगकर्ता या डिवाइस के जिस डेटा को पाबंदी वाली अनुमतियों का इस्तेमाल करके ऐक्सेस किया जाता है उसे उपयोगकर्ता का निजी और संवेदनशील डेटा माना जाता है. इस पर उपयोगकर्ता के डेटा से जुड़ी नीति की शर्तें लागू होती हैं.
- अगर उपयोगकर्ता पाबंदी वाली अनुमति देने से मना कर देते हैं, तो उनके फ़ैसलों का सम्मान करें. साथ ही, किसी ग़ैर-ज़रूरी अनुमति पर सहमति देने के लिए उपयोगकर्ताओं 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.
- Google Play की मैलवेयर से जुड़ी नीतियों का उल्लंघन करने वाली अनुमतियों का इस्तेमाल करना साफ़ तौर पर मना है. इनमें खास अधिकारों का गलत इस्तेमाल भी शामिल है.

पाबंदी वाली कुछ खास अनुमतियां, नीचे बताई गई दूसरी ज़रूरी शर्तों पर निर्भर हो सकती हैं. इन पाबंदियों का मकसद, ऐप्लिकेशन को इस्तेमाल करने वालों की निजता को सुरक्षित रखना है. हम नीचे दी गई ज़रूरी शर्तों में सीमित 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 पॉलिसी और आगे दी गई पाबंदियों के तहत, इस्तेमाल करने वाले का संवेदनशील डेटा माना जाता है:

पाबंदी वाली अनुमति	ज़रूरत
कॉल लॉग अनुमति ग्रुप (जैसे READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS)	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमएस) या सहायक हैंडलर के रूप में सही तरीके से रजिस्टर किया जाना चाहिए.
मैसेज (एसएमएस) अनुमति ग्रुप (जैसे READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS)	इसे डिवाइस पर डिफ़ॉल्ट मैसेज (एसएमए) या सहायक हैंडलर के रूप में सही तरीके से रजिस्टर किया जाना

पाबंदी वाली अनुमति	ज़रूरत
	चाहिए.

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

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

जगह की जानकारी की अनुमतियां

डिवाइस की जगह की जानकारी को उपयोगकर्ता की निजी और संवेदनशील जानकारी माना जाता है. यह निजी और संवेदनशील जानकारी से जुड़ी पॉलिसी, बैकग्राउंड में जगह की जानकारी ऐक्सेस करने का अनुरोध करने की पॉलिसी, और नीचे दी गई शर्तों पर निर्भर करती है:

- आपका ऐप्लिकेशन, ऐप्लिकेशन में मौजूदा सुविधाएं या सेवाएं देने की सुविधा बंद हो जाने के बाद, जगह की जानकारी (उदाहरण के लिए, ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION, ACCESS_BACKGROUND_LOCATION) की अनुमति की मदद से सुरक्षित डेटा को ऐक्सेस नहीं कर सकेगा.
- सिर्फ़ विज्ञापन दिखाने या आंकड़े पाने के लिए, आपको ऐप्लिकेशन इस्तेमाल करने वालों से जगह की जानकारी इस्तेमाल करने की अनुमति नहीं मांगनी चाहिए. विज्ञापन दिखाने के लिए इस डेटा के इस्तेमाल की अनुमति देने वाले ऐप्लिकेशन को हमारी विज्ञापन पॉलिसी के मुताबिक होना चाहिए.
- 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 ऐक्सेस करने का अनुरोध, सिर्फ़ ऐसी सुविधाएं देने के लिए किया जा सकता है जो उपयोगकर्ता 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:

- उपयोगकर्ताओं 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 से जुड़ी पॉलिसी का पालन करना होगा.

पॉलिसी से जुड़ी ज़रूरी शर्तों के बारे में ज़्यादा जानकारी के लिए, यह सहायता लेख पढ़ें.

सभी फ़ाइलें ऐक्सेस करने की अनुमति

निजी और संवेदनशील जानकारी पॉलिसी और नीचे दी गई ज़रूरी शर्तों के मुताबिक, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डिवाइस पर मौजूद फ़ाइलों और डायरेक्ट्री का डेटा उसका निजी और संवेदनशील डेटा माना जाता है:

- ऐप्लिकेशन को डिवाइस की उस स्टोरेज के ऐक्सेस का अनुरोध करना चाहिए जो ऐप्लिकेशन के काम करने के लिए ज़रूरी हो. किसी तीसरे पक्ष के लिए, डिवाइस के उस स्टोरेज के ऐक्सेस का अनुरोध नहीं किया जाना चाहिए जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों को मिलने वाली सुविधा के काम करने के लिए ज़रूरी न हो.

- डिवाइस की शेयर किए गए स्टोरेज का ऐक्सेस मैनेज करने के लिए, उन Android डिवाइस को MANAGE_EXTERNAL_STORAGE अनुमति लेनी होगी जो R या उसके बाद के वर्शन पर काम कर रहे हैं. जो ऐप्लिकेशन R वर्शन को टारगेट करते हैं और डिवाइस की शेयर किए गए स्टोरेज ("सभी फ़ाइलों का ऐक्सेस") का ऐक्सेस बढ़ाने का अनुरोध करते हैं उन्हें प्रकाशित करने से पहले उनकी समीक्षा ज़रूरी है. इस समीक्षा में यह साफ़ होना चाहिए कि ऐप्लिकेशन को सही तौर पर ऐक्सेस दिया गया है. जो ऐप्लिकेशन इस अनुमति का इस्तेमाल करते हैं उन्हें ऐप्लिकेशन इस्तेमाल करने वाले लोगों को साफ़ तौर पर यह सूचना देनी चाहिए कि वे "खास ऐप्लिकेशन के लिए ऐक्सेस" सेटिंग में जाकर इस तरह के ऐप्लिकेशन के लिए, "सभी फ़ाइलों का ऐक्सेस" चालू करें. R वर्शन से जुड़ी ज़रूरी शर्तों के बारे में ज़्यादा जानकारी के लिए, यह सहायता लेख पढ़ें.

पैकेज (ऐप्लिकेशन) से जुड़ी जानकारी ऐक्सेस करने की अनुमति

डिवाइस का इस्तेमाल करके, इंस्टॉल किए गए ऐप्लिकेशन की इन्वेंट्री के बारे में मांगी गई जानकारी को निजी और संवेदनशील जानकारी पॉलिसी के तहत, इस्तेमाल करने वाले का निजी और संवेदनशील डेटा माना जाता है. इसके लिए इन बातों का ध्यान रखा जाता है:

जिन ऐप्लिकेशन का मुख्य उद्देश्य लॉन्च करना, खोजना या डिवाइस पर मौजूद दूसरे ऐप्लिकेशन के साथ काम करना होता है, वे डिवाइस पर इंस्टॉल किए गए दूसरे ऐप्लिकेशन पा सकते हैं, जैसा कि नीचे बताया गया है:

- **ऐप्लिकेशन की ज़्यादा से ज़्यादा जानकारी देखने की क्षमता:** वह क्षमता जिससे किसी ऐप्लिकेशन को, डिवाइस पर इंस्टॉल किए गए ऐप्लिकेशन ("पैकेज") की पूरी ("या ज़्यादा से ज़्यादा") जानकारी दिखती है.
  - एपीआई लेवल 30 या इसके बाद के वर्शन को टारगेट करने वाले ऐप्लिकेशन के लिए, QUERY_ALL_PACKAGES अनुमति की मदद से, डिवाइस पर इंस्टॉल किए गए अन्य ऐप्लिकेशन की ज़्यादा से ज़्यादा जानकारी देखने की क्षमता को सीमित किया गया है. अगर ऐप्लिकेशन को किसी एक और सभी ऐप्लिकेशन के साथ मिलकर काम करने की ज़रूरत होगी और/या उसे अन्य ऐप्लिकेशन के बारे में जानकारी रखने की ज़रूरत होगी, तभी उसे यह अनुमति मिलेगी.
    - अगर आपका ऐप्लिकेशन लक्षित दायरे में रखे गए पैकेज की ही जानकारी को टारगेट करने का एलान करके काम कर सकता है, तो हो सकता है कि आप QUERY_ALL_PACKAGES अनुमति का इस्तेमाल न कर पाएं. उदाहरण के लिए, ज़्यादा से ज़्यादा जानकारी देखने का अनुरोध करने के बजाय, ऐप्लिकेशन की खास जानकारी के लिए क्वेरी या इंटरैक्ट करना.
  - उन तरीकों पर भी पाबंदी है जिनके इस्तेमाल से QUERY_ALL_PACKAGES की अनुमति से जुड़ी ज़्यादा से ज़्यादा जानकारी शेयर करने या दिखाने की सुविधा के लेवल का अनुमान लगाया जा सकता है. इन तरीकों का इस्तेमाल सिर्फ़ तब किया जा सकता है, जब QUERY_ALL_PACKAGES की अनुमति का इस्तेमाल, उपयोगकर्ता को दी जाने वाली आपके ऐप्लिकेशन की मुख्य सुविधा के लिए ज़रूरी हो. इसके अलावा, आपका ऐप्लिकेशन किसी दूसरे ऐप्लिकेशन के साथ किस तरह काम करता है, इसका पता लगाने के लिए भी इन तरीकों का इस्तेमाल किया जा सकता है.
  - QUERY_ALL_PACKAGES अनुमति का इस्तेमाल किन-किन मामलों में किया जा सकता है, यह जानने के लिए इस सहायता केंद्र लेख को पढ़ें.
- **सीमित जानकारी का ऐक्सेस:** कम से कम जानकारी देखने का मतलब है कि जब कोई ऐप्लिकेशन, बेहतर तरीके से टारगेट करने वाले ("ज़्यादा से ज़्यादा जानकारी" देखने के बजाय) तरीके का इस्तेमाल करके, कुछ खास ऐप्लिकेशन के बारे में क्वेरी करता है और इस तरह, कम से कम डेटा ऐक्सेस करता है. उदाहरण के लिए, उन खास ऐप्लिकेशन से जुड़ी जानकारी के लिए क्वेरी करना जिनके बारे में आपके ऐप्लिकेशन के मेनिफ़ेस्ट में बताया जाता है. अगर आपका ऐप्लिकेशन, इन ऐप्लिकेशन के साथ मिलकर काम करने की पॉलिसी का पालन करता हो या इन्हें मैनेज करता हो, तो आप इस तरीके का इस्तेमाल करके उन ऐप्लिकेशन से जुड़ी जानकारी के लिए क्वेरी कर सकते हैं.
- किसी डिवाइस पर इंस्टॉल किए गए ऐप्लिकेशन की इन्वेंट्री की जानकारी देखने की अनुमति सिर्फ़ तब होनी चाहिए, जब आपके ऐप्लिकेशन के मुख्य मकसद को पूरा करने के लिए या वे मुख्य सुविधाएं देने के लिए ऐसा करना ज़रूरी हो जिन्हें आपका ऐप्लिकेशन इस्तेमाल करने वाले लोग ऐक्सेस करते हैं.

Play पर मौजूद ऐप्लिकेशन की क्वेरी से मिलने वाला ऐप्लिकेशन इन्वेंट्री डेटा न तो कभी बेचा जा सकता है और न ही आंकड़े जुटाने या विज्ञापनों से कमाई करने के मकसद से उसे शेयर किया जा सकता है.

ऐक्सेसिबिलिटी एपीआई

ऐक्सेसिबिलिटी एपीआई का इस्तेमाल, इनके लिए नहीं किया जा सकता:

- उपयोगकर्ता की अनुमति के बिना, उपयोगकर्ता सेटिंग में बदलाव करने या उपयोगकर्ताओं को किसी ऐप्लिकेशन या सेवा को बंद करने या अनइंस्टॉल करने की सुविधा इस्तेमाल करने से रोकने के लिए. हालांकि, माता-पिता के कंट्रोल वाले ऐप्लिकेशन की मदद से, माता-पिता या अभिभावक की अनुमति के बाद या एंटरप्राइज़ मैनेजमेंट सॉफ़्टवेयर की मदद से, अधिकृत एडमिन की अनुमति से ऐसा किया जा सकता है;
- Android में पहले से मौजूद, निजता सेटिंग और सूचनाएं देने की सुविधा में बदलाव करने के लिए; या
- यूज़र इंटरफ़ेस में बदलाव करने या फ़ायदा उठाने के लिए इस तरह से इस्तेमाल करना जिससे कि धोखाधड़ी की संभावना हो या डेवलपर के लिए बनाई गई Google Play की नीतियों का उल्लंघन हो.

ऐक्सेसिबिलिटी एपीआई को किसी दूसरी जगह से ऑडियो कॉल रिकॉर्ड करने के लिए नहीं बनाया गया है. साथ ही, इसके लिए अनुरोध भी नहीं किया जा सकता.

ऐक्सेसिबिलिटी एपीआई के इस्तेमाल के बारे में, Google Play के स्टोर पेज पर बताया जाना चाहिए.

IsAccessibilityTool के लिए दिशा-निर्देश

ऐसे ऐप्लिकेशन जो खास तौर पर दिव्यांग व्यक्तियों के लिए हैं वे **IsAccessibilityTool** का इस्तेमाल कर सकते हैं. इससे, उन ऐप्लिकेशन को ऐक्सेसिबिलिटी ऐप्लिकेशन के तौर पर सूची में शामिल किया जाता है.

ऐसे ऐप्लिकेशन जो **IsAccessibilityTool** का इस्तेमाल करने की ज़रूरी शर्तें पूरी नहीं करते, हो सकता है कि वे फ़्लैग की सुविधा का इस्तेमाल न कर पाएं. इसके अलावा, उन्हें उपयोगकर्ता के डेटा से जुड़ी नीति में बताई गई जानकारी देनी होगी और सहमति की ज़रूरी शर्तों को पूरा करना होगा. ऐसा इसलिए, क्योंकि आम तौर पर उयोगकर्ताओं को यह जानकारी नहीं होती कि ऐप्लिकेशन में ऐक्सेसिबिलिटी की सुविधा उपलब्ध है. ज़्यादा जानकारी के लिए, AccessibilityService एपीआई के सहायता केंद्र का लेख पढ़ें.

ऐप्लिकेशन के किसी खास फ़ंक्शन को इस्तेमाल करने के लिए, ऐक्सेसिबिलिटी एपीआई के बजाय, एपीआई और अनुमतियों का इस्तेमाल करना ज़्यादा सही होता है.

पैकेज इंस्टॉल करने की अनुमति के लिए अनुरोध करना

REQUEST_INSTALL_PACKAGES अनुमति से, किसी ऐप्लिकेशन को ऐप्लिकेशन पैकेज इंस्टॉल करने के लिए अनुरोध करने की मंज़ूरी मिल जाती है. इस अनुमति का इस्तेमाल करने के लिए, आपके ऐप्लिकेशन के मुख्य फ़ंक्शन में नीचे बताई गई सुविधाएं शामिल होनी चाहिए:

- ऐप्लिकेशन के पैकेज भेजने या पाने की सुविधा और
- वह सुविधा जिससे उपयोगकर्ता, ऐप्लिकेशन के पैकेज इंस्टॉल करने की प्रक्रिया शुरू कर सके.

इन कामों की अनुमति है:

- वेब ब्राउज़िंग या वेब खोज
- ऐसी कम्यूनिकेशन सेवाएं जिनमें अटैचमेंट की सुविधा काम करती हो
- फ़ाइल शेयर, ट्रांसफ़र या मैनेज करने की सुविधा
- एंटरप्राइज़ से जुड़े डिवाइस मैनेज करने की सुविधा
- बैकअप और पहले जैसा करने की सुविधा
- एक डिवाइस से दूसरे डिवाइस पर या एक फ़ोन से दूसरे फ़ोन पर डेटा भेजने की सुविधा
- साथी ऐप्लिकेशन, जो पहने जाने वाले या IoT डिवाइस (जैसे कि स्मार्ट वॉच या स्मार्ट टीवी) को फ़ोन के साथ सिंक करता है

मुख्य फ़ंक्शन, ऐप्लिकेशन का खास मकसद होता है. मुख्य फ़ंक्शन के साथ-साथ इस मुख्य फ़ंक्शन में शामिल अन्य सभी मुख्य सुविधाओं के बारे में ऐप्लिकेशन के ब्यौरे में साफ़ तौर पर जानकारी ज़ाहिर करनी चाहिए और उनका प्रमोशन किया जाना चाहिए.

हो सकता है कि REQUEST_INSTALL_PACKAGES अनुमति इस्तेमाल करके, ऐसेट फ़ाइल में अन्य APKs को खुद अपडेट नहीं किया जा सके. इसके अलावा, उसमें बदलाव नहीं किया जा सके या उनका बंडल नहीं बनाया जा सके. हालांकि, डिवाइस मैनेज करने के मकसद से ऐसा किया जा सकता है. पैकेज को अपडेट करने या इंस्टॉल करने की सभी प्रक्रिया, Google Play की डिवाइस और नेटवर्क के गलत इस्तेमाल को रोकने से जुड़ी नीति के मुताबिक होनी चाहिए. साथ ही, यह भी ज़रूरी है कि उपयोगकर्ता ही इन प्रक्रिया को शुरू और पूरा करे.

Health Connect by Android की अनुमतियां

Health Connect एक Android प्लैटफ़ॉर्म है. इसकी मदद से, किसी डिवाइस पर सेहत और फ़िटनेस से जुड़े अलग-अलग ऐप्लिकेशन के डेटा को एक जगह सेव और शेयर किया जा सकता है. इसमें लोगों को एक ही जगह पर यह कंट्रोल करने की सुविधा मिलती है कि कौनसे ऐप्लिकेशन, सेहत और फ़िटनेस से जुड़े डेटा को देख सकते हैं और उसमें बदलाव कर सकते हैं. Health Connect, अलग-अलग तरह का डेटा देखने और उसमें बदलाव करने की सुविधा देता है. जैसे, शरीर का तापमान और चले गए कदम.

जिस डेटा को Health Connect की अनुमतियों की मदद से ऐक्सेस किया जाता है उसे निजी और संवेदनशील माना जाता है. इस पर उपयोगकर्ता के डेटा से जुड़ी नीति लागू होती है. अगर आपका ऐप्लिकेशन स्वास्थ्य से जुड़ा ऐप्लिकेशन है या उसमें स्वास्थ्य से जुड़ी सुविधाएं हैं और यह स्वास्थ्य की जानकारी का डेटा (जैसे, Health Connect का डेटा) ऐक्सेस कर सकता है, तो इसे सेहत से जुड़े ऐप्लिकेशन के लिए बनी नीति का पालन भी करना होगा.

Health Connect का इस्तेमाल शुरू करने का तरीका जानने के लिए, कृपया Android डेवलपर की यह गाइड देखें. Health Connect के अलग-अलग डेटा को ऐक्सेस करने का अनुरोध करने के लिए, कृपया यहां जाएं.

Google Play से डिस्ट्रिब्यूट किए गए हर ऐप्लिकेशन को, Health Connect में मौजूद डेटा को देखने और/या उसमें बदलाव करने के लिए, नीति से जुड़ी इन ज़रूरी शर्तों को पूरा करना होगा.

Health Connect को ऐक्सेस करने और इस्तेमाल करने का सही तरीका

Health Connect का इस्तेमाल, लागू होने वाली नीतियों के साथ-साथ नियमों और शर्तों के मुताबिक ही किया जा सकता है. इसका इस्तेमाल, नीति में बताए गए उन मामलों में भी किया जा सकता है जिनके लिए अनुमति ली जा सकती है. इसका मतलब यह है कि अनुमतियों के ऐक्सेस का अनुरोध सिर्फ़ तब किया जा सकता है, जब आपका ऐप्लिकेशन या सेवा इस्तेमाल के ऐसे मामलों में शामिल हो जिनके लिए अनुमति ली जा सकती है.

ऐप्लिकेशन को इन मामलों में इस्तेमाल की अनुमति मिल सकती है: फ़िटनेस और सेहत, इनाम, फ़िटनेस कोचिंग, कॉर्पोरेट के लिए स्वास्थ्य सुविधाएं, चिकित्सा से जुड़ी सेवाएं, सेहत से जुड़ी रिसर्च, और गेम. जिन ऐप्लिकेशन को ये अनुमतियां मिलती हैं वे इनका इस्तेमाल, बिना जानकारी दिए या बिना अनुमति वाले कामों के लिए नहीं कर सकते.

Health Connect की अनुमतियों के ऐक्सेस का अनुरोध सिर्फ़ वे ऐप्लिकेशन या सेवाएं कर सकती हैं जिनकी एक या एक से ज़्यादा सुविधाओं का मुख्य मकसद, लोगों की सेहत और फ़िटनेस को बेहतर करना हो. इनमें ये शामिल हैं:

- ऐसे ऐप्लिकेशन या सेवाएं जिनकी मदद से लोग सीधे तौर पर अपनी शारीरिक गतिविधि, नींद, मानसिक स्वास्थ्य, पोषण, सेहत से जुड़ी जानकारी, शारीरिक बनावट, और/या सेहत या फ़िटनेस से जुड़े अन्य ब्यौरों और माप को **नोट कर सकते हैं, उसकी रिपोर्ट तैयार कर सकते हैं, उस पर नज़र रख सकते हैं, और/या उसका विश्लेषण कर सकते हैं.**
- ऐसे ऐप्लिकेशन या सेवाएं जिनकी मदद से लोग अपनी **शारीरिक गतिविधि, नींद, मानसिक स्वास्थ्य, पोषण, सेहत से जुड़ी जानकारी, शारीरिक बनावट** से जुड़ी जानकारी, और/या सेहत या फ़िटनेस से जुड़े अन्य ब्यौरों और माप को अपने फ़ोन और/या पहने जाने वाले डिवाइस पर सेव कर सकते हैं. साथ ही, वे डेटा को अपने डिवाइस पर उपलब्ध ऐसे अन्य ऐप्लिकेशन के साथ भी शेयर कर सकते हैं जो इस्तेमाल के इन मामलों के मुताबिक हों.

Health Connect का इस्तेमाल तब नहीं किया जाना चाहिए, जब इस नीति का या Health Connect के लागू होने वाले अन्य नियमों और शर्तों या नीतियों का उल्लंघन हो रहा हो. इसमें ये मकसद भी शामिल हैं:

- Health Connect का इस्तेमाल ऐसे ऐप्लिकेशन, नेटवर्क या गतिविधियों के लिए या उनकी मदद करने के लिए न करें जहां Health Connect के नाकाम होने पर किसी की मौत होने, चोट लगने, पर्यावरण या प्रॉपर्टी को नुकसान पहुंचने का खतरा हो. जैसे, परमाणु से संबंधित संस्थाओं को बनाने और चलाने के लिए, एयर ट्रैफ़िक कंट्रोल सिस्टम, लाइफ़ सपोर्ट सिस्टम या हथियारों के लिए.
- बिना ग्राफ़िक यूज़र इंटरफ़ेस वाला ऐप्लिकेशन इस्तेमाल करके, Health Connect से मिला डेटा ऐक्सेस न करें. ऐप्लिकेशन को ऐप्लिकेशन ट्रे, डिवाइस ऐप्लिकेशन सेटिंग, सूचना आइकॉन वगैरह में साफ़ तौर से पहचाने जाने लायक आइकॉन दिखाने चाहिए.
- Health Connect का इस्तेमाल उन ऐप्लिकेशन के साथ न करें जो साथ काम न करने वाले डिवाइसों या प्लैटफ़ॉर्म के बीच डेटा सिंक करते हैं.
- Health Connect का इस्तेमाल उन ऐप्लिकेशन, सेवाओं या सुविधाओं के साथ न करें जिनमें सिर्फ़ बच्चों को टारगेट किया जाता है.
- Health Connect को बिना अनुमति के या गैर-कानूनी तरीके से ऐक्सेस करने, इस्तेमाल करने, खत्म करने, नुकसान पहुंचाने, बदलाव करने या ज़ाहिर करने वाले सभी ऐप्लिकेशन या सिस्टम से बचाने के लिए, उचित और सही कदम उठाएं.

यह पक्का करना भी आपकी जिम्मेदारी है कि Health Connect और उससे मिले किसी भी डेटा का इस्तेमाल जिस मकसद के लिए किया जा रहा है उसके लिए लागू होने वाले सभी नियमों या कानूनी समझौते की शर्तों का पालन किया जा रहा हो. लेबल में साफ़ तौर पर दी गई जानकारी या Google के खास प्रॉडक्ट या सेवाओं के लिए Google ने जो जानकारी दी है उसके अलावा, किसी भी तरह के इस्तेमाल या मकसद के लिए Google न तो Health Connect में मौजूद किसी डेटा के इस्तेमाल की सलाह देता है और न ही उसके सही होने की गारंटी देता है. खास तौर पर तब, जब इस डेटा का इस्तेमाल रिसर्च, सेहत या चिकित्सा के लिए किया जा रहा हो. Google, Health Connect से मिले डेटा के इस्तेमाल से जुड़ी सभी तरह की कानूनी जवाबदेही का खंडन करता है.

सीमित इस्तेमाल

अगर कोई उपयोगकर्ता Health Connect का इस्तेमाल कर रहा है, तो उपयोगकर्ता के डेटा को ऐक्सेस करने और इस्तेमाल करने के लिए डेवलपर को खास सीमाओं का पालन करना होगा. जैसे:

- डेटा का इस्तेमाल, ऐप्लिकेशन के यूज़र इंटरफ़ेस में दिखाई गई सुविधाएं या तरीकों को उपलब्ध कराने/बेहतर बनाने के लिए ही किया जाना चाहिए.
- उपयोगकर्ता का डेटा उसकी सहमति के बाद ही तीसरे पक्षों के साथ शेयर किया जाना चाहिए. यह डेटा, सुरक्षा से जुड़े मामलों में (जैसे, डेटा के गलत इस्तेमाल की जांच करना), लागू कानूनों/नियमों का पालन करने के लिए या कंपनी मर्ज करने/उसके अधिकार हासिल करने के मामलों में शेयर होता है.
- उपयोगकर्ता के डेटा का इस्तेमाल कोई तब तक नहीं कर सकता, जब तक उपयोगकर्ता ने खास तौर पर इसके लिए सहमति न दी हो. यह भी ज़रूरी है कि डेटा, कानून का पालन करने के लिए, सुरक्षा से जुड़े मामलों में या कानूनी समझौते की शर्तों के तहत संगठन के

कामकाज के लिए इकट्ठा किया जाता हो.

- अन्य सभी मामलों में, Health Connect से मिले डेटा को ट्रांसफ़र करने, इस्तेमाल करने या बेचने पर पाबंदी है. इनमें ये मामले भी शामिल हैं:
  - उपयोगकर्ता के डेटा को तीसरे पक्षों को ट्रांसफ़र करना या बेचना. जैसे, विज्ञापन प्लैटफ़ॉर्म, डेटा ब्रोकर या जानकारी को दोबारा बेचने वाले लोग (रीसेलर).
  - विज्ञापन दिखाने के लिए, उपयोगकर्ता के डेटा को इस्तेमाल करना, ट्रांसफ़र करना या बेचना. इसमें, लोगों के हिसाब से बनाए गए विज्ञापन या दिलचस्पी के आधार पर विज्ञापन दिखाना भी शामिल है.
  - क़र्ज़ लेने या देने की स्थिति तय करने के लिए, उपयोगकर्ता के डेटा को इस्तेमाल करना, ट्रांसफ़र करना या बेचना.
  - ऐसे किसी भी प्रॉडक्ट या सेवा के लिए, उपयोगकर्ता का डेटा इस्तेमाल करना, ट्रांसफ़र करना या बेचना जो फ़ेडरल फ़ूड ड्रग ऐंड कॉस्मैटिक ऐक्ट के सेक्शन 201(h) के हिसाब से मेडिकल डिवाइस हो. साथ ही, उस मेडिकल डिवाइस में उपयोगकर्ता के डेटा का इस्तेमाल तय किए गए नियमों के मुताबिक किया जा रहा हो.
  - Google से कोई लिखित मंज़ूरी लिए बिना, स्वास्थ्य की सुरक्षित जानकारी (हिपा के मुताबिक) के लिए या इससे जुड़े किसी अन्य मकसद के लिए उपयोगकर्ता के डेटा को इस्तेमाल करना, ट्रांसफ़र करना या बेचना.

कम से कम अनुमतियों का ऐक्सेस मांगें

सिर्फ़ उन अनुमतियों के ऐक्सेस का अनुरोध करें जो आपके प्रॉडक्ट की सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं. ऐक्सेस के ऐसे अनुरोध, सिर्फ़ उस डेटा से जुड़े होने चाहिए जिसकी ज़रूरत है. अन्य डेटा के ऐक्सेस का अनुरोध नहीं किया जाना चाहिए.

साफ़ तौर पर दी गई सही सूचना और कंट्रोल

Health Connect लोगों की सेहत और फ़िटनेस के डेटा को मैनेज करता है. इस डेटा में संवेदनशील जानकारी भी शामिल होती है. इसलिए, यह ज़रूरी है कि Health Connect से लिंक किए गए सभी ऐप्लिकेशन के लिए एक निजता नीति तय की गई हो. साथ ही, इस नीति में पूरी जानकारी दी गई हो. यह भी ज़रूरी है कि निजता नीति में इस बारे में साफ़ तौर पर बताया गया हो कि कोई ऐप्लिकेशन किस तरह उपयोगकर्ता के डेटा को इकट्ठा करता है, उसका इस्तेमाल करता है, और उसे शेयर करता है. कानूनी समझौते की शर्तों के अलावा, डेवलपर को निजता नीति में यहां दी गई जानकारी भी शामिल करनी होगी:

- ऐप्लिकेशन के बारे में साफ़ तौर पर जानकारी देना. जैसे, यह लोगों का किस तरह का डेटा ऐक्सेस कर सकता है और उस डेटा के आधार पर, कौनसी मुख्य सुविधाएं या किस तरह के सुझाव दिए जाते हैं
- निजी डेटा का रखरखाव और उसे मिटाने के तरीके के बारे में जानकारी देना
- डेटा मैनेज करने की प्रोसेस के बारे में जानकारी देना. जैसे, निजी डेटा को एचटीटीपीएस जैसी मॉर्डन क्रिप्टोग्राफ़ी का इस्तेमाल करके ट्रांसफ़र करना

डेटा की सुरक्षित तरीके से हैंडलिंग

आपको उपयोगकर्ता का पूरा डेटा सुरक्षित तरीके से मैनेज करना होगा. Health Connect को बिना अनुमति के या गैरकानूनी तरीके से ऐक्सेस करने, इस्तेमाल करने, खत्म करने, नुकसान पहुंचाने, बदलाव करने या ज़ाहिर करने वाले सभी ऐप्लिकेशन या सिस्टम से बचाने के लिए, उचित और सही कदम उठाएं.

सुरक्षा के जो तरीके सुझाए गए हैं उनमें इंफ़ॉर्मेशन सिक्योरिटी मैनेजमेंट सिस्टम को लागू करना और उसका रखरखाव करना शामिल है. इसके बारे में, आईएसओ/आईईसी 27001 में बताया गया है. इसके अलावा, आपको यह भी पक्का करना होगा कि आपका ऐप्लिकेशन या वेब सेवा बेहतरीन है और उसमें सुरक्षा से जुड़ी आम समस्याएं नहीं हैं. इन समस्याओं की जानकारी, 'OWASP मुख्य 10' में दी गई है.

अगर आपका प्रॉडक्ट उपयोगकर्ता के डेटा को उसके डिवाइस के बाहर ट्रांसफ़र करता है, तो आपको अपने ऐप्लिकेशन या सेवा का समय-समय पर सुरक्षा आकलन कराना होगा और अनुमति पा चुके किसी तीसरे पक्ष से 'आकलन पत्र' लेना होगा. यह प्रक्रिया, ऐक्सेस किए जाने वाले एपीआई और उपयोगकर्ता की अनुमतियों की संख्या या उपयोगकर्ताओं की संख्या के हिसाब से तय होती है.

Health Connect से जुड़ने वाले ऐप्लिकेशन की ज़रूरी शर्तों के बारे में ज़्यादा जानने के लिए, कृपया यह सहायता लेख पढ़ें.

वीपीएन सेवा

VpnService , ऐप्लिकेशन के लिए बेस क्लास की तरह है. इसकी मदद से, वे वीपीएन का अपना नेटवर्क बनाते हैं और उसके दायरे को बढ़ाते हैं. सिर्फ़ वे ऐप्लिकेशन किसी रिमोट सर्वर के लिए डिवाइस लेवल का एक सुरक्षित टनल बना सकते हैं जो VpnService का इस्तेमाल करते हैं और वीपीएन उनके मुख्य फ़ंक्शन के तौर पर शामिल होता है. उन ऐप्लिकेशन को छूट है जिन्हें मुख्य फ़ंक्शन के लिए किसी रिमोट सर्वर की ज़रूरत होती है, जैसे कि:

- माता-पिता के कंट्रोल वाले और संगठन को मैनेज करने के लिए इस्तेमाल होने वाले ऐप्लिकेशन.
- ऐप्लिकेशन के इस्तेमाल को ट्रैक करना.

- डिवाइस की सुरक्षा वाले ऐप्लिकेशन, जैसे कि एंटी-वायरस, मोबाइल डिवाइस मैनेजमेंट, फ़ायरवॉल.
- नेटवर्क से जुड़े टूल, जैसे कि कहीं से भी ऐक्सेस करने की सुविधा.
- वेब ब्राउज़िंग ऐप्लिकेशन.
- मोबाइल और इंटरनेट सेवा देने वाली कंपनी के ऐसे ऐप्लिकेशन जिनके लिए वीपीएन फ़ंक्शन का इस्तेमाल करना ज़रूरी होता है. इसकी मदद से, वे टेलिफ़ोन या कनेक्टिविटी सेवाएं देते हैं.

VpnService का इस्तेमाल इन कामों के लिए नहीं किया जा सकता:

- साफ़ तौर पर जानकारी ज़ाहिर किए बिना और उपयोगकर्ता की सहमति लिए बिना, उपयोगकर्ता का निजी और संवेदनशील डेटा इकट्ठा करना.
- कमाई करने के मकसद से, उपयोगकर्ता ट्रैफ़िक को अन्य ऐप्लिकेशन से किसी डिवाइस पर भेजना. उदाहरण के लिए,विज्ञापन ट्रैफ़िक को किसी ऐसे देश भेजना जो उपयोगकर्ता का देश नहीं है.

VpnService इस्तेमाल करने वाले ऐप्लिकेशन को:

- VpnService के इस्तेमाल के बारे में, Google Play के स्टोर पेज पर बताना चाहिए.
- डिवाइस से वीपीएन टनल के एंड पॉइंट तक जाने वाले डेटा को सुरक्षित करना चाहिए.
- डेवलपर कार्यक्रम की सभी नीतियों का पालन करना चाहिए. इसमें, विज्ञापन से होने वाली धोखाधड़ी, अनुमतियों, और मैलवेयर से जुड़ी नीतियां शामिल हैं.

एग्ज़ैक्ट अलार्म अनुमति

एक नई अनुमति, USE_EXACT_ALARM, शुरू की जाएगी. इससे, उन ऐप्लिकेशन को एग्ज़ैक्ट अलार्म फ़ंक्शन का ऐक्सेस मिल सकेगा जिनमें कम से कम Android वर्शन 13 (एपीआई टारगेट लेवल 33) हो.

USE_EXACT_ALARM एक पाबंदी वाली अनुमति है. ऐप्लिकेशन को इस अनुमति का एलान सिर्फ़ तब करना चाहिए, जब उनके मुख्य फ़ंक्शन को एग्ज़ैट अलार्म की ज़रूरत हो. जो ऐप्लिकेशन इस पाबंदी वाली अनुमति के लिए अनुरोध करेंगे उनकी समीक्षा की जाएगी. इनमें से जो ऐप्लिकेशन उचित इस्तेमाल के उदाहरण की शर्तों को पूरा नहीं करेंगे उन्हें Google Play पर पब्लिश करने की अनुमति नहीं दी जाएगी.

एग्ज़ैक्ट अलार्म अनुमति के लिए, उचित इस्तेमाल के उदाहरण वाले मामले

आपके ऐप्लिकेशन में USE_EXACT_ALARM का इस्तेमाल सिर्फ़ तब किया जाना चाहिए, जब आपके ऐप्लिकेशन के मुख्य फ़ंक्शन के लिए बिल्कुल ठीक समय पर की जाने वाली कार्रवाइयों की ज़रूरत हो, जैसे कि:

- ऐप्लिकेशन, अलार्म या टाइमर ऐप्लिकेशन हो.
- ऐप्लिकेशन कोई ऐसा कैलेंडर ऐप्लिकेशन हो जो इवेंट की सूचनाएं दिखाता हो.

अगर आपके पास एग्ज़ैक्ट अलार्म फ़ंक्शन के लिए इस्तेमाल का कोई ऐसा उदाहरण है जिसके बारे में ऊपर नहीं बताया गया है, तो आपको यह देखना होगा कि SCHEDULE_EXACT_ALARM को विकल्प के तौर पर इस्तेमाल करने की सुविधा है या नहीं.

एग्ज़ैक्ट अलार्म फ़ंक्शन के बारे में ज़्यादा जानकारी के लिए, कृपया डेवलपर के लिए दिए गए इन दिशा-निर्देशों को देखें.

फ़ुल-स्क्रीन पर सूचनाएं दिखाने की अनुमति

Android 14 (एपीआई टारगेट लेवल 34) और इसके बाद के वर्शन को टारगेट करने वाले ऐप्लिकेशन के लिए USE_FULL_SCREEN_INTENT, विशेष ऐप्लिकेशन ऐक्सेस करने की अनुमति है. ऐप्लिकेशन, USE_FULL_SCREEN_INTENT अनुमति का अपने-आप इस्तेमाल सिर्फ़ तब कर पाएंगे, जब उनके मुख्य फ़ंक्शन नीचे दी गई हाई-प्रायॉरिटी नोटिफ़िकेशन वाली किसी एक कैटगरी में आते हों:

- अलार्म सेट करना
- फ़ोन या वीडियो कॉल लेना

जो ऐप्लिकेशन इस अनुमति के लिए अनुरोध करेंगे उनकी समीक्षा की जाएगी. इसके अलावा, जो ऐप्लिकेशन ऊपर दी गई ज़रूरी शर्तों के हिसाब से नहीं हैं उन्हें अपने-आप अनुमति नहीं मिलेगी. ऐसे में, ऐप्लिकेशन को USE_FULL_SCREEN_INTENT का इस्तेमाल करने के लिए उपयोगकर्ता से अनुमति का अनुरोध करना होगा.

आपको याद दिला दें कि USE_FULL_SCREEN_INTENT अनुमति का इस्तेमाल, डेवलपर के लिए बनाई गई Google Play की नीतियों को ध्यान में रखकर किया जाना चाहिए. इसमें मोबाइल के अनचाहे सॉफ़्टवेयर, डिवाइस और नेटवर्क के गलत इस्तेमाल को रोकना, और विज्ञापन की नीतियां शामिल हैं. फ़ुल-स्क्रीन के इंटेंट वाली सूचनाओं को उपयोगकर्ता के डिवाइस में गड़बड़ी या नुकसान नहीं

पहुंचाना चाहिए और उन्हें गलत तरीके से ऐक्सेस नहीं करना चाहिए. साथ ही, डिवाइस के इस्तेमाल में रुकावट नहीं डालनी चाहिए. इसके अलावा, ऐप्लिकेशन को दूसरे ऐप्लिकेशन या डिवाइस के इस्तेमाल में रुकावट नहीं डालनी चाहिए.

हमारे सहायता केंद्र पर जाकर, USE_FULL_SCREEN_INTENT अनुमति के बारे में ज़्यादा जानें.

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. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं

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

Google Play से इंस्टॉल होने वाले ऐप्लिकेशन को अपडेट करने, बदलने या उसमें बदलाव करने के लिए, सिर्फ़ Google Play के अपडेट करने का तरीका इस्तेमाल किया जा सकता है. किसी और तरीके से शायद ऐसा नहीं हो पाए. इसी तरह, किसी ऐप्लिकेशन के लिए Google Play के अलावा किसी अन्य स्रोत से एक्ज़ीक्यूटेबल कोड (उदाहरण के लिए, dex, JAR, .so फ़ाइलें) डाउनलोड नहीं किया जा सकता. यह पाबंदी, उस कोड पर लागू नहीं होती जो किसी वर्चुअल मशीन या इंटरप्रटर पर काम करता है और दोनों में से किसी को Android एपीआई का सीधे तौर पर ऐक्सेस (जैसे कि वेबव्यू या ब्राउज़र में JavaScript) नहीं देता है.

ऐसे ऐप्लिकेशन या तीसरे पक्ष के कोड (उदाहरण के लिए, SDK टूल) को किसी भी स्थिति में Google Play की नीतियों का उल्लंघन नहीं करने देना चाहिए जो रन टाइम (उदाहरण के लिए, बिना ऐप्लिकेशन पैकेज के) पर लोड की गई भाषाओं (उदाहरण के लिए, JavaScript, Python, Lua वगैरह) का इस्तेमाल करते हैं.

हम सुरक्षा में जोखिम की संभावना पैदा करने वाले या उनका फ़ायदा उठाने वाले कोड को अनुमति नहीं देते. डेवलपर के लिए हाल ही में फ़्लैग की गई सुरक्षा से जुड़ी समस्याओं के बारे में जानने के लिए, ऐप्लिकेशन की सुरक्षा को बेहतर बनाने वाला प्रोग्राम देखें.

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

डिवाइस और नेटवर्क के गलत इस्तेमाल से जुड़े आम तौर पर होने वाले उल्लंघनों के उदाहरण:

- ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने पर अन्य ऐप्लिकेशन को ब्लॉक कर देते हैं या फिर उसमें रुकावट डालते हैं.
- गेम में धोखाधड़ी करने वाले ऐप्लिकेशन जो अन्य ऐप्लिकेशन के गेमप्ले पर असर डालते हैं.
- ऐसे ऐप्लिकेशन जो सेवाओं, सॉफ़्टवेयर या हार्डवेयर को हैक करने का तरीका बताते हैं या उसकी सुविधा देते हैं. साथ ही, वे उसके सुरक्षा उपायों को गच्चा देने में भी मदद करते हैं.
- ऐसे ऐप्लिकेशन जो किसी सेवा या एपीआई का इस्तेमाल या ऐक्सेस इस तरह करते हैं, जिससे इसकी सेवा की शर्तों का उल्लंघन होता है.
- ऐसे ऐप्लिकेशन जिन्हें कुछ खास सुविधाओं या सेवाओं को ऐक्सेस करने की अनुमति नहीं है. साथ ही, जो सिस्टम पावर मैनेजमेंट को नज़रअंदाज़ करने की कोशिश करते हैं.
- ऐसे ऐप्लिकेशन जो तीसरे पक्ष को प्रॉक्सी सेवा देते हैं. ऐसा सिर्फ़ उन ऐप्लिकेशन में किया जा सकता है जिनका मुख्य मकसद ही प्रॉक्सी सेवा देना है.
- वे ऐप्लिकेशन या तीसरे पक्ष के कोड (उदाहरण के लिए, SDK टूल) जो Google Play के अलावा किसी अन्य सोर्स से एक्ज़ीक्यूटेबल कोड डाउनलोड करते हैं, जैसे कि dex फ़ाइलें या नेटिव कोड.
- 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 लिंक कर देते हैं या लोगों तक उन्हें पहुंचाने या इंस्टॉल करने की सुविधा देते हैं.
- वे ऐप्लिकेशन या तीसरे पक्ष के कोड (उदाहरण के लिए, SDK टूल) जिनमें JavaScript इंटरफ़ेस वाला वेबव्यू होता है. यह वेबव्यू गैर-भरोसेमंद वेब कॉन्टेंट (जैसे कि http:// URL) या गैर-भरोसेमंद सोर्स (जैसे कि गलत इंटेंट वाले यूआरएल) से मिले, बिना पुष्टि वाले यूआरएल लोड करता है.
- ऐसे ऐप्लिकेशन जो फ़ुल-स्क्रीन इंटेंट अनुमति का इस्तेमाल करके, परेशान करने वाले विज्ञापन या सूचनाओं की मदद से यूज़र इंटरैक्शन करते हैं.

फ़ोरग्राउंड सेवा का इस्तेमाल

फ़ोरग्राउंड सेवा से जुड़ी अनुमति से यह पक्का किया जाता है कि उपयोगकर्ताओं के लिए उपलब्ध फ़ोरग्राउंड सेवाओं का सही इस्तेमाल हो. Android 14 और इससे नए वर्शन को टारगेट करने वाले ऐप्लिकेशन के लिए, आपको अपने ऐप्लिकेशन में इस्तेमाल होने वाली हर फ़ोरग्राउंड सेवा के लिए एक मान्य फ़ोरग्राउंड सेवा के टाइप की जानकारी देनी होगी. साथ ही, आपको उस फ़ोरग्राउंड सेवा के लिए

अनुमति के बारे में भी बताना होगा जो इस टाइप की सेवा के इस्तेमाल के लिए सही होगी. उदाहरण के लिए, अगर आपके ऐप्लिकेशन के इस्तेमाल के लिए मैप जियोलोकेशन की ज़रूरत है, तो आपको अपने ऐप्लिकेशन के मेनिफ़ेस्ट में FOREGROUND_SERVICE_LOCATION अनुमति के बारे में बताना होगा.

ऐप्लिकेशन को फ़ोरग्राउंड सेवा के लिए अनुमति का इस्तेमाल करने की इजाज़त तब ही दी जाएगी, अगर:

- उसका इस्तेमाल करने से उपयोगकर्ता को कोई फ़ायदेमंद सुविधा मिलती हो और वह ऐप्लिकेशन के मुख्य फ़ंक्शन से जुड़ी हो
- उपयोगकर्ता खुद उस सेवा का इस्तेमाल शुरू करे या उसे यह पता हो कि उसके डिवाइस पर फ़ोरग्राउंड सेवा से जुड़ा कोई टास्क चल रहा है. उदाहरण के लिए, कोई गाना चलाने पर सुनाई देने वाला ऑडियो, मीडिया को दूसरे डिवाइस पर कास्ट करना, लोगों को सही और सटीक सूचना मिलना, लोगों का क्लाउड पर कोई फ़ोटो अपलोड करने का अनुरोध करना
- उसके इस्तेमाल को उपयोगकर्ता बंद कर सकता है या रोक सकता है
- उसके इस्तेमाल को उपयोगकर्ता का अनुभव खराब किए बिना सिस्टम की तरफ़ से रोका या टाला नहीं जा सकता. ऐसा भी न हो कि उपयोगकर्ता को दी जाने वाली सुविधा उसकी उम्मीद के मुताबिक काम न करे. उदाहरण के लिए, फ़ोन कॉल करने में सिस्टम की वजह से देरी नहीं होनी चाहिए
- तब ही इस्तेमाल की जाती हो, जब किसी टास्क को पूरा करने की ज़रूरत हो

ऊपर दी गई शर्तों में, फ़ोरग्राउंड सेवा के इस्तेमाल के ये मामले शामिल नहीं होते:

- फ़ोरग्राउंड सेवा का टाइप systemExempted या shortService हो;
- फ़ोरग्राउंड सेवा का टाइप dataSync हो. इसे सिर्फ़ तब शामिल नहीं किया जाएगा, जब Play ऐसेट डिलीवरी की सुविधाओं का इस्तेमाल किया जा रहा हो

फ़ोरग्राउंड सेवा के इस्तेमाल के बारे में ज़्यादा जानकारी यहां दी गई है.

User-Initiated Data Transfer Jobs

ऐप्लिकेशन को सिर्फ़ user-initiated data transfer jobs API का इस्तेमाल करने की अनुमति है, अगर:

- उपयोगकर्ता की तरफ़ से इस्तेमाल शुरू किया जाता है
- नेटवर्क डेटा ट्रांसफ़र से जुड़े टास्क के लिए इस्तेमाल किया जाता है
- सिर्फ़ तभी तक चलता है, जब तक डेटा ट्रांसफ़र को पूरा करने की ज़रूरत होती है

User-Initiated Data Transfer APIs के बारे में ज़्यादा जानकारी यहां दी गई है.

Flag_Secure सेटिंग के लिए ज़रूरी शर्तें

FLAG_SECURE एक डिसप्ले फ़्लैग है, जिसे ऐप्लिकेशन के कोड में शामिल किया जाता है. यह इस बात का संकेत देता है कि ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) में संवेदनशील जानकारी है जिसका इस्तेमाल सीमित डिसप्ले के साथ किया जाता है. इस जानकारी को तब ऐक्सेस किया जा सकता है, जब ऐप्लिकेशन का इस्तेमाल किसी सुरक्षित आउटपुट वाले डिसप्ले पर किया जा रहा हो. जानकारी को स्क्रीनशॉट या असुरक्षित डिसप्ले में दिखने से रोकने के लिए इसे डिज़ाइन किया गया है. डेवलपर इस फ़्लैग का इस्तेमाल तब करते हैं, जब ऐप्लिकेशन के कॉन्टेंट को उपयोगकर्ता के डिवाइस या ऐप्लिकेशन के बाहर ब्रॉडकास्ट करने, दिखाने या भेजने से रोकना हो.

सुरक्षा और निजता के मकसद से, Google Play पर उपलब्ध कराए जाने वाले सभी ऐप्लिकेशन को अन्य ऐप्लिकेशन के FLAG_SECURE का सम्मान करना ज़रूरी होता है. इसका मतलब यह है कि ऐप्लिकेशन को अन्य ऐप्लिकेशन में मौजूद FLAG_SECURE सेटिंग को बायपास करने का कोई तरीका आज़माना नहीं चाहिए या उसमें मदद नहीं करनी चाहिए.

जिन ऐप्लिकेशन को सुलभता टूल के तौर पर मंज़ूरी मिली होती है उन्हें इस शर्त को पूरा नहीं करना पड़ता. उन्हें यह छूट तब तक मिलती है, जब तक वे FLAG_SECURE से सुरक्षित कॉन्टेंट को उपयोगकर्ता के डिवाइस के बाहर ऐक्सेस किए जाने के लिए, न तो भेजते हैं और न ही उसे स्टोर या कैश मेमोरी में सेव करते हैं.

उपयोगकर्ता के डिवाइस पर मौजूद Android कंटेनर पर काम करने वाले ऐप्लिकेशन

उपयोगकर्ता के डिवाइस पर मौजूद Android कंटेनर ऐप्लिकेशन, Android OS के सभी या कुछ हिस्सों को अलग से सिम्युलेट करता है. हालांकि, इस दौरान Android सुरक्षा से जुड़ी सुविधा, को पूरी तरह से सिम्युलेट नहीं किया जाता. इसी वजह से डेवलपर, उपयोगकर्ता के डिवाइस पर एक सिक्योर एनवायरमेंट मेनिफ़ेस्ट फ़्लैग को जोड़ने का विकल्प चुन सकते हैं. इससे, डिवाइस पर मौजूद Android कंटेनर को यह बताया जा सकता है कि सिम्युलेशन के दौरान इन कंटेनर को काम नहीं करना चाहिए.

सिक्योर एनवायरमेंट मेनिफ़ेस्ट फ़्लैग

REQUIRE_SECURE_ENV एक तरह का फ़्लैग है. किसी ऐप्लिकेशन के मेनिफ़ेस्ट में इस फ़्लैग से यह जानकारी दी जा सकती है कि ऐप्लिकेशन को उपयोगकर्ता के डिवाइस के Android कंटेनर ऐप्लिकेशन पर नहीं चलाया जाना चाहिए. सुरक्षा और निजता बनाए रखने के लिए, उपयोगकर्ता के डिवाइस पर Android कंटेनर मुहैया कराने वाले ऐप्लिकेशन, इस फ़्लैग वाले सभी ऐप्लिकेशन के मुताबिक होने चाहिए और:

- इस फ़्लैग के लिए, ऐप्लिकेशन के उन मेनिफ़ेस्ट की समीक्षा करें जिन्हें डिवाइस में मौजूद Android कंटेनर में लोड करना है.
- उन ऐप्लिकेशन को लोड न करें जिन्होंने इस फ़्लैग के बारे में अपने डिवाइस में मौजूद Android कंटेनर में एलान किया है.
- इन ऐप्लिकेशन को डिवाइस के एपीआई को इंटरसेप्ट या इस्तेमाल करके, प्रॉक्सी के तौर पर इस तरह काम नहीं करना चाहिए कि वे कंटेनर में इंस्टॉल किए गए ऐप्लिकेशन की तरह दिखें.
- फ़्लैग को बायपास करने का कोई तरीका नहीं आज़माना चाहिए या उसमें मदद नहीं करनी चाहिए, जैसे कि मौजूदा ऐप्लिकेशन के REQUIRE_SECURE_ENV फ़्लैग को बायपास करने के लिए, किसी ऐप्लिकेशन के पुराने वर्शन का इस्तेमाल करना.

इस नीति के बारे में ज़्यादा जानने के लिए, हमारे सहायता केंद्र पर जाएं.

धोखाधड़ी वाला व्यवहार

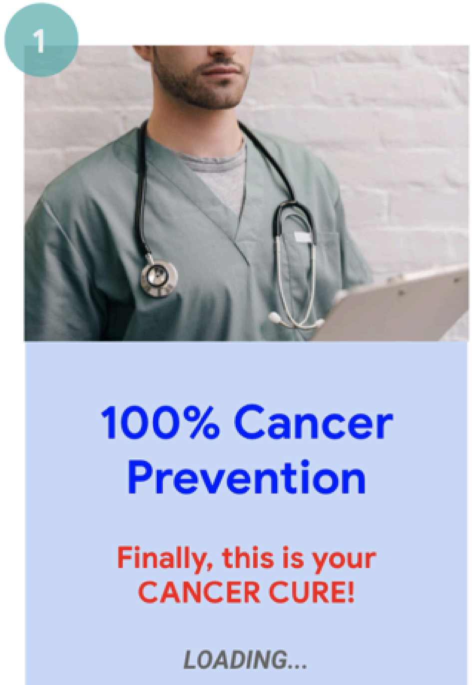
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों के साथ धोखाधड़ी करने की कोशिश करते हैं या बेईमानी करते हैं. इनमें वे ऐप्लिकेशन भी शामिल हैं जो ऐसी सुविधाएं देने का दावा करते हैं जिन्हें पूरा नहीं किया जा सकता. ऐप्लिकेशन को पूरे मेटाडेटा में अपनी सुविधाओं के बारे में सही जानकारी, ब्यौरा, और फ़ोटो/वीडियो देना ज़रूरी है. 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, उपयोगकर्ता की जानकारी और सहमति से ही किए जाने चाहिए. ये बदलाव ऐसे हों जिन्हें उपयोगकर्ता पहले जैसा कर सके.

गुमराह करने वाले दावे

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

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

- ऐसे ऐप्लिकेशन जो अपनी सुविधाओं को गलत तरीके से पेश करते हैं या सही जानकारी नहीं देते:
  - ऐसा ऐप्लिकेशन जिसके ब्यौरे और स्क्रीनशॉट में रेसिंग गेम होने का दावा किया जाता हो, जबकि असल में वह पज़ल ब्लॉक गेम हो, जिसमें एक कार की तस्वीर का इस्तेमाल किया गया हो.
  - ऐसा ऐप्लिकेशन जो एंटी-वायरस ऐप्लिकेशन होने का दावा करता हो, जबकि उसमें सिर्फ़ वायरस हटाने का तरीका बताने वाली एक गाइड दी गई हो.
- जो सुविधाएं देना मुमकिन नहीं है उनकी पेशकश करने वाले ऐप्लिकेशन, जैसे कि कीड़े भगाने का दावा करने वाले ऐप्लिकेशन. भले ही, इन्हें शरारत, झूठ, मज़ाक़ वगैरह के तौर पर पेश किया गया हो.
- ऐसे ऐप्लिकेशन जिन्हें गलत कैटगरी में रखा गया है. इनमें ऐप्लिकेशन की रेटिंग या ऐप्लिकेशन की कैटगरी के अलावा, और भी चीज़ें शामिल हो सकती हैं.
- धोखाधड़ी या गुमराह करने वाला ऐसा कॉन्टेंट जिसका इस्तेमाल साफ़ तौर पर मतदान की प्रक्रिया में रुकावट डालने या चुनावों के नतीजों की जानकारी देने के लिए किया जाता है.
- ऐसे ऐप्लिकेशन जो किसी सरकारी 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 किसी जानी-मानी इकाई का आधिकारिक ऐप्लिकेशन होने का झूठा दावा करते हैं. ज़रूरी अनुमतियों या अधिकारों के बिना, “जस्टिन बीबर आधिकारिक” जैसे शीर्षकों का इस्तेमाल करने की अनुमति नहीं है.



(1) यह ऐप्लिकेशन, इलाज या सेहत से जुड़ी ऐसी सुविधाएं देने का दावा करता है जो गुमराह करने वाली हैं. जैसे, कैंसर का इलाज.
(2) यह ऐप्लिकेशन, ऐसी सुविधाएं देने का दावा करता है जो नहीं दी जा सकतीं. जैसे, अपने फ़ोन को सांसों की जांच करने वाले डिवाइस के तौर पर इस्तेमाल करना.

डिवाइस की सेटिंग में, गुमराह करने वाले बदलाव

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

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

- 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 उपयोगकर्ताओं को, तीसरे पक्ष के ऐप्लिकेशन हटाने या बंद करने या डिवाइस की सेटिंग और सुविधाओं में बदलाव करने का बढ़ावा देते हैं. ऐसे ऐप्लिकेशन को तब तक अनुमति नहीं दी जाती है, जब तक वह किसी ऐसी सुरक्षा सेवा का हिस्सा न हो जिसकी पुष्टि हो चुकी हो.

धोखाधड़ी को बढ़ावा देना

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते 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, बैंक खाते, और ड्राइविंग लाइसेंस बनाने में इस्तेमाल होने वाले या इसमें मदद करने वाले ऐप्लिकेशन. इसमें इन चीज़ों से जुड़े ऐप्लिकेशन के अलावा, और भी ऐप्लिकेशन शामिल हो सकते हैं. ऐप्लिकेशन के कॉन्टेंट और/या उसकी सुविधाओं के बारे में सटीक जानकारी देनी होगी, जैसे कि ऐप्लिकेशन का नाम, उसका ब्यौरा, और इमेज/वीडियो वगैरह. साथ ही, ऐप्लिकेशन को इस्तेमाल करने का अनुभव बिल्कुल वैसा ही होना चाहिए जैसा उपयोगकर्ता ने उम्मीद की थी.

ऐप्लिकेशन के दूसरे संसाधन (जैसे कि गेम एसेट) सिर्फ़ तब डाउनलोड किए जा सकेंगे, जब वे उपयोगकर्ता के ऐप्लिकेशन में इस्तेमाल के लिए बहुत ज़रूरी हों. डाउनलोड किए गए संसाधन, Google Play नीतियों के मुताबिक होने चाहिए. साथ ही, डाउनलोड करने से पहले, ऐप्लिकेशन के उपयोगकर्ताओं को 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.

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

- ऐसे ऐप्लिकेशन जो किसी दूसरे ऐप्लिकेशन या वेबसाइटों की नकल करके, उपयोगकर्ताओं से निजी जानकारी या पुष्टि करने की जानकारी मांगते हैं.
- ऐसे ऐप्लिकेशन जो बिना पुष्टि वाले या असली फ़ोन नंबर, संपर्क, और पते दिखाते हैं. इसके अलावा, व्यक्ति या किसी इकाई की सहमति के बिना निजी रूप से पहचान करने वाली जानकारी भी दिखाते हैं.
- ऐसे ऐप्लिकेशन जिनकी मुख्य सुविधाएं, उपयोगकर्ता के इलाके, डिवाइस पैरामीटर या उपयोगकर्ता से मिलने वाले अन्य डेटा पर निर्भर हों और इनकी वजह से आने वाले बदलाव के बारे में स्टोर पेज में साफ़ तौर पर नहीं बताया गया हो.
- ऐसे ऐप्लिकेशन जो उपयोगकर्ता को सूचना दिए बिना, वर्शन में बदलाव करते हैं (जैसे, '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) से डाउनलोड किए जा सकने वाले ऐसे ऐप्लिकेशन जो डाउनलोड होने से पहले उपयोगकर्ता को डाउनलोड साइज़ के बारे में साफ़ तौर पर नहीं बताते हैं.

ऐसा कॉन्टेंट जिसमें छेड़छाड़ की गई हो

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो इमेज, ऑडियो, 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. साथ ही, उन ऐप्लिकेशन को भी अनुमति नहीं है जो तस्वीरों, वीडियो और/या टेक्स्ट के ज़रिए धोखाधड़ी को बढ़ावा देते हैं. इनकी वजह से संवेदनशील घटना, राजनैतिक, सामाजिक या दूसरे सार्वजनिक मामलों में नुकसान पहुंच सकता है.

कुछ ऐप्लिकेशन चीज़ों को साफ़ तौर पर दिखाने या क्वालिटी सुधारने के पारंपरिक और संपादकीय तरीकों से अलग हटकर कॉन्टेंट में बदलाव करते हैं या उसे दूसरे तरीके से दिखाते हैं. ऐप्लिकेशन को ऐसे कॉन्टेंट में बदलाव की जानकारी साफ़ तौर पर देनी चाहिए या वॉटरमार्क के साथ पेश करना चाहिए जिसके बारे में आम व्यक्ति को पता न चल सके कि कॉन्टेंट में बदलाव किया गया है. हालांकि, लोगों के हित के लिए बनाए गए, व्यंग्य या पैरोडी वाले कॉन्टेंट को छूट मिल सकती है.

आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण यहां 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 हस्ती 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 करने की सुविधा देता है. साथ ही, वॉटरमार्क के बिना, क्लिप में मशहूर और जानी-मानी हस्तियों को जोड़ने की सुविधा देता है.

ऐप्लिकेशन के व्यवहार से जुड़ी पारदर्शिता नीति

आपके ऐप्लिकेशन की सुविधाओं के बारे में लोगों को साफ़ तौर पर जानकारी दी जानी चाहिए. इसमें, आपके ऐप्लिकेशन की छिपी, डॉरमेंट या दस्तावेज़ में नहीं बताई गई सुविधाएं शामिल नहीं हैं. साथ ही, ऐप्लिकेशन की समीक्षाओं से बचने वाली तकनीकों का इस्तेमाल न करें. ऐसा हो सकता है कि आपको अपने ऐप्लिकेशन के बारे में अतिरिक्त जानकारी देनी पड़े. इससे, यह पक्का किया जा सकेगा कि आपके ऐप्लिकेशन लोगों के लिए सुरक्षित हैं, नीति का पूरी तरह से पालन करते हैं, और इन पर सिस्टम को मज़बूत स्तर की पूरी सुरक्षा मिलती है.

गलत तरीके से पेश करना

हम ऐसे ऐप्लिकेशन या डेवलपर खातों को अनुमति नहीं देते हैं जो:

- किसी दूसरे व्यक्ति या संगठन के नाम पर काम करते हों. हम उन ऐप्लिकेशन या डेवलपर खातों को भी अनुमति नहीं देते जो किसी दूसरे व्यक्ति या संगठन के मालिकाना हक या असल मकसद को छिपाते हों या गलत तरीके से पेश करते हों.
- गिरोह बनाकर लोगों को गुमराह करने की गतिविधि से जुड़े हों. इसमें ऐसे ऐप्लिकेशन या डेवलपर खाते शामिल हैं जो अपने मूल देश के बारे में गलत जानकारी देते हैं या अपने मूल देश की जानकारी छिपाते हैं या किसी दूसरे देश के लोगों को कॉन्टेंट भेजते हैं. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.
- डेवलपर या ऐप्लिकेशन की पहचान छिपाने या उसे गलत तरीके से पेश करने के लिए, दूसरे ऐप्लिकेशन, साइटों, डेवलपर या दूसरे खातों के साथ मिलकर काम करते हैं. इसके अलावा, दूसरी गलत जानकारी को भी छिपाते हैं या उसे गलत तरीके से पेश करते हैं. यह उन मामलों के लिए होगा जिनमें आपका कॉन्टेंट, राजनीति, सामाजिक मुद्दों या लोगों से जुड़ा है.

Google Play के टारगेट एपीआई लेवल से जुड़ी नीति

Google Play के उपयोगकर्ताओं को सुरक्षित अनुभव देने के लिए, **सभी ऐप्लिकेशन** को Google Play के टारगेट एपीआई लेवल की इन शर्तों को पूरा करना होगा:

नए ऐप्लिकेशन और ऐप्लिकेशन अपडेट के लिए ज़रूरी है कि वे Android का नया वर्शन रिलीज़ होने के एक साल के अंदर किसी Android एपीआई लेवल को टारगेट करें. इस ज़रूरी शर्त को पूरा न करने वाले नए ऐप्लिकेशन और ऐप्लिकेशन अपडेट को Play Console पर सबमिट नहीं किया जा सकेगा.

Google Play पर पहले से मौजूद ऐसे ऐप्लिकेशन जिन्हें अपडेट नहीं किया गया है और जो Android का नया वर्शन रिलीज़ होने के दो साल के अंदर किसी एपीआई लेवल को टारगेट नहीं करते वे उन नए उपयोगकर्ताओं के लिए उपलब्ध नहीं होंगे जिनके डिवाइस Android OS के नए वर्शन पर काम करते हैं. जिन उपयोगकर्ताओं ने पहले ही Google Play से ऐप्लिकेशन इंस्टॉल किया है वे ऐप्लिकेशन को खोजने के साथ-साथ, उसे फिर से इंस्टॉल और इस्तेमाल कर सकेंगे. ऐसा Android OS के ऐसे किसी भी वर्शन पर किया जा सकेगा जिस पर वह ऐप्लिकेशन काम करता हो.

टारगेट एपीआई लेवल की शर्तों को पूरा करने के बारे में किसी तकनीकी सलाह के लिए, कृपया डेटा को दूसरी जगह भेजने से जुड़ी गाइड देखें.

समयावधि और अपवादों की पूरी जानकारी के लिए, कृपया सहायता केंद्र के लेख पर जाएं.

SDK टूल इस्तेमाल करने की ज़रूरी शर्तें

ऐप्लिकेशन डेवलपर अक्सर अपने ऐप्लिकेशन के अहम फ़ंक्शन और सेवाओं के लिए, तीसरे पक्ष के कोड का इस्तेमाल करते हैं. जैसे, कोई SDK टूल. अपने ऐप्लिकेशन में किसी SDK टूल को इस्तेमाल करने का मकसद, यह पक्का करना होता है कि उपयोगकर्ताओं का डेटा सुरक्षित रहे और ऐप्लिकेशन को इस्तेमाल करने में कोई जोखिम न हो. इस सेक्शन में, हमने यह बताया है कि SDK टूल के इस्तेमाल पर निजता और सुरक्षा से जुड़ी हमारी कुछ मौजूदा शर्तें कैसे लागू होती हैं. इन शर्तों में इस बात का ध्यान रखा गया है कि डेवलपर आसान और सुरक्षित तरीके से अपने ऐप्लिकेशन में SDK टूल जोड़ पाएं.

अपने ऐप्लिकेशन में कोई SDK टूल जोड़ने पर यह पक्का करना आपकी जिम्मेदारी होगी कि तीसरे पक्ष के कोड और उसका इस्तेमाल करने से Google Play के डेवलपर कार्यक्रम की नीतियों का उल्लंघन न हो. आपके लिए यह जानना ज़रूरी है कि आपके ऐप्लिकेशन में इस्तेमाल हुए SDK टूल, उपयोगकर्ता के डेटा को किस तरह इस्तेमाल करते हैं. साथ ही, आपको यह भी पता होना चाहिए कि किन अनुमतियों का इस्तेमाल किया जाता है, कौनसा डेटा इकट्ठा किया जाता है, और ऐसा क्यों किया जाता है. इस बात का ध्यान रखें कि SDK टूल आपके ऐप्लिकेशन पर लागू होने वाली नीति के मुताबिक ही उपयोगकर्ता के डेटा को इकट्ठा और इस्तेमाल करें.

यह पक्का करने के लिए कि कोई SDK टूल, ऐप्लिकेशन पर लागू होने वाली नीति की ज़रूरी शर्तों का उल्लंघन न करे, इन नीतियों को अच्छी तरह से पढ़ें और समझें. साथ ही, SDKs टूल के बारे में नीचे दी गई ज़रूरी शर्तों का भी ध्यान रखें:

उपयोगकर्ता के डेटा से जुड़ी नीति

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को कैसे इस्तेमाल किया जाता है, इस बारे में आपको साफ़ तौर पर जानकारी देनी चाहिए. उदाहरण के लिए, ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति से इकट्ठा की गई या उसके बारे में इकट्ठा की गई जानकारी, डिवाइस की जानकारी वगैरह. इसका मतलब है कि आपको यह बताना चाहिए कि आपके ऐप्लिकेशन से, लोगों का कौनसा डेटा ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर किया जा रहा है. साथ ही, यह भी बताया जाना चाहिए कि आपका ऐप्लिकेशन, नीति का पालन करते हुए किसी और काम के लिए लोगों के डेटा का इस्तेमाल नहीं करता है.

अगर आपने ऐप्लिकेशन में तीसरे पक्ष के कोड (उदाहरण के लिए, कोई SDK टूल) का इस्तेमाल किया है, तो आपको यह पक्का करना होगा कि ऐप्लिकेशन में मौजूद तीसरे पक्ष का कोड और उस तीसरे पक्ष की ओर से आपके ऐप्लिकेशन के उपयोगकर्ताओं के डेटा का इस्तेमाल, Google Play Developer Program की नीतियों के मुताबिक किया जाए. इसमें, डेटा के इस्तेमाल और साफ़ तौर पर जानकारी देने की शर्तों को पूरा करना भी शामिल है. उदाहरण के लिए, आपको यह पक्का करना होगा कि ऐप्लिकेशन में जिन कंपनियों के SDK टूल इस्तेमाल किए जा रहे हैं वे आपके ऐप्लिकेशन से मिले उपयोगकर्ता के निजी और संवेदनशील डेटा को बेचती न हों. यह ज़रूरी शर्त हर हाल में लागू होगी. भले ही, उपयोगकर्ता का डेटा, सर्वर पर भेजने के बाद ट्रांसफ़र किया गया हो या आपके ऐप्लिकेशन में तीसरे पक्ष के कोड को एम्बेड करने के बाद उसे ट्रांसफ़र किया गया हो.

उपयोगकर्ता का निजी और संवेदनशील डेटा

- एक ऐप्लिकेशन से दूसरे ऐप्लिकेशन पर या किसी सेवा के ज़रिए मिले उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर करने की सुविधा को सीमित करें. साथ ही, नीतियों का पालन करते हुए, उपयोगकर्ता की उम्मीद के हिसाब से इकट्ठा किए गए डेटा का भी सीमित इस्तेमाल करें:
  - विज्ञापन दिखाने के लिए उपयोगकर्ता के निजी और संवेदनशील डेटा का इस्तेमाल करने वाले ऐप्लिकेशन को Google Play की विज्ञापन नीति का पालन करना होगा.
- उपयोगकर्ता के निजी और संवेदनशील डेटा को सुरक्षित तरीके से इस्तेमाल करना चाहिए. इसमें, आधुनिक क्रिप्टोग्राफ़ी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करके डेटा को ट्रांसफ़र करना भी शामिल है.
- Android की अनुमतियों से सुरक्षित किया गया डेटा ऐक्सेस करने से पहले, जब भी रनटाइम अनुमतियां उपलब्ध हों, तब इनके अनुरोध का इस्तेमाल करें

उपयोगकर्ता के निजी और संवेदनशील डेटा की बिक्री

उपयोगकर्ता के निजी और संवेदनशील डेटा को बेचना नहीं चाहिए.

- "बिक्री" का मतलब है कि कमाई करने के मकसद से, उपयोगकर्ता के निजी और संवेदनशील डेटा को किसी तीसरे पक्ष से आपस में शेयर या ट्रांसफ़र करना.
  - जब उपयोगकर्ता अपने निजी और संवेदनशील डेटा को खुद ट्रांसफ़र करते हैं, तो उसे बिक्री नहीं माना जाता. जैसे- जब कोई उपयोगकर्ता किसी तीसरे पक्ष को फ़ाइल ट्रांसफ़र करने के लिए, ऐप्लिकेशन की किसी सुविधा का इस्तेमाल करता है या किसी ऐसे ऐप्लिकेशन का इस्तेमाल करता है जिसका खास मकसद, खोज या अध्ययन करना हो.

साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तें

ऐसे मामले जहां दिए गए सवाल में प्रॉडक्ट या सुविधा का इस्तेमाल करने वाले उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल या शेयर करने की सुविधा उपयोगकर्ता की उम्मीद के हिसाब से नहीं बताई जाती हैं, तो आपको उपयोगकर्ता के डेटा से जुड़ी नीति की साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तें पूरी करनी होंगी.

अगर आपका ऐप्लिकेशन तीसरे पक्ष के किसी ऐसे कोड (उदाहरण के लिए, कोई SDK टूल) को जोड़ता है जिसे डिफ़ॉल्ट तौर पर उपयोगकर्ता के निजी और संवेदनशील डेटा को इकट्ठा करने के लिए डिज़ाइन किया गया है, तो आपको Google Play से अनुरोध मिलने के दो हफ़्तों के अंदर (या अगर उस समयावधि के अंदर, Google Play का अनुरोध लंबी अवधि के लिए दिया जाता है), इसके ज़रूरी सबूत देने होंगे कि आपका ऐप्लिकेशन इस नीति की साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों को पूरा करता है. इसमें, तीसरे पक्ष के कोड की मदद से, डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल या शेयर करने की जानकारी भी शामिल है.

यह पक्का करें कि ऐप्लिकेशन में किसी तीसरे पक्ष का कोड (जैसे, कोई SDK टूल) इस्तेमाल करने से, उपयोगकर्ता के डेटा से जुड़ी नीति का उल्लंघन न हो.

साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों के बारे में ज़्यादा जानने के लिए, सहायता केंद्र का यह लेख पढ़ें.

SDK टूल की वजह से हुए उल्लंघन के उदाहरण

- SDK टूल वाला ऐसा ऐप्लिकेशन जिसमें उपयोगकर्ता का निजी और संवेदनशील डेटा इकट्ठा किया जाता है. साथ ही, जिसमें इस डेटा को उपयोगकर्ता के डेटा से जुड़ी नीति, उसे ऐक्सेस करने, मैनेज करने, और साफ़ तौर पर जानकारी ज़ाहिर करने और सहमति देने से जुड़ी ज़रूरी शर्तों के तौर पर नहीं देखा जाता है. इसमें, बिना अनुमति की बिक्री भी शामिल है.
- SDK टूल इस्तेमाल करने वाला ऐसा ऐप्लिकेशन जो उपयोगकर्ता के निजी और संवेदनशील डेटा को डिफ़ॉल्ट रूप से इकट्ठा करता है और इससे उपयोगकर्ता की सहमति से जुड़ी और साफ़ तौर पर जानकारी ज़ाहिर करने की शर्तों का उल्लंघन होता है.
- SDK टूल वाला ऐसा ऐप्लिकेशन जो धोखाधड़ी और डेटा के गलत इस्तेमाल से बचाव के लिए, उपयोगकर्ता का निजी और संवेदनशील डेटा इकट्ठा करने का दावा करता है, लेकिन डेटा को विज्ञापन या आंकड़े उपलब्ध कराने के मकसद से तीसरे पक्ष के साथ शेयर करता है.
- SDK टूल वाला ऐसा ऐप्लिकेशन जो साफ़ तौर पर जानकारी ज़ाहिर करने के दिशा-निर्देशों और/या नीति के दिशा-निर्देशों की शर्तें पूरी किए बिना ही उपयोगकर्ताओं के इंस्टॉल किए गए पैकेज की जानकारी को दूसरी जगह भेजता है.
  - मोबाइल का अनचाहा सॉफ़्टवेयर नीति को भी पढ़ें.

निजी और संवेदनशील जानकारी ऐक्सेस करने से जुड़ी अन्य ज़रूरी शर्तें

नीचे दी गई टेबल में खास गतिविधियों के लिए, ज़रूरी शर्तों के बारे में बताया गया है.

गतिविधि	ज़रूरी शर्त
अगर आपका ऐप्लिकेशन, डिवाइस के स्थायी पहचानकर्ताओं की जानकारी (उदाहरण के लिए, IMEI, IMSI, सिम का सीरियल नंबर # वगैरह) को इकट्ठा करता है या जोड़ता है	डिवाइस के स्थायी पहचानकर्ताओं को उपयोगकर्ताओं के अन्य निजी और संवेदनशील डेटा या डिवाइस के रीसेट हो सकने वाले पहचानकर्ताओं से नहीं जोड़ा जा सकता. हालांकि, नीचे बताए गए मकसद के लिए ऐसा किया जा सकता है: • किसी सिम कार्ड की पहचान से जुड़ी टेलिफ़ोन सेवा. उदाहरण के लिए, मोबाइल और इंटरनेट सेवा देने वाली कंपनी के खाते से जुड़ी, वाई-फ़ाई कॉलिंग की सुविधा के लिए और • एंटरप्राइज़ से जुड़े डिवाइस को मैनेज करने वाले ऐसे ऐप्लिकेशन के लिए जिनमें डिवाइस मालिक वाले मोड का इस्तेमाल होता है. इस तरह के इस्तेमाल की जानकारी, उपयोगकर्ताओं को साफ़ तौर पर बताई जानी चाहिए, जैसा कि उपयोगकर्ता के डेटा से जुड़ी नीति में बताया गया है. खास पहचानकर्ताओं के विकल्प के लिए, कृपया यह लेख पढ़ें. Android के विज्ञापन आईडी से जुड़े अन्य दिशा-निर्देशों के लिए, कृपया विज्ञापन नीति को ध्यान से पढ़ें.
अगर आपका ऐप्लिकेशन बच्चों को टारगेट करता है	आपके ऐप्लिकेशन में सिर्फ़ ऐसे SDK टूल इस्तेमाल किए जा सकते हैं जो बच्चों से जुड़ी सेवाओं के लिए नीतियों के मुताबिक काम करने का दावा करते हैं. नीति और भाषा से जुड़ी सारी शर्तें जानने के लिए, Families Self-Certified Ads SDK Program पर जाएं.

SDK टूल की वजह से हुए उल्लंघन के उदाहरण

- SDK टूल वाला ऐसा ऐप्लिकेशन जो Android आईडी और जगह की जानकारी को जोड़ता है
- SDK टूल वाला ऐसा ऐप्लिकेशन जो विज्ञापन या आंकड़े उपलब्ध कराने के मकसद से, AAID को डिवाइस आइडेंटिफ़ायर से जोड़ता है.
- SDK टूल वाला ऐसा ऐप्लिकेशन जो आंकड़ें उपलब्ध कराने के मकसद से, AAID और ईमेल पते को जोड़ देता है.

डेटा की सुरक्षा वाला सेक्शन

सभी डेवलपर के लिए यह ज़रूरी है कि वे हर ऐप्लिकेशन के डेटा की सुरक्षा वाले सेक्शन में पूरी जानकारी दें. इसमें, उपयोगकर्ता के निजी और संवेदनशील डेटा को इकट्ठा, इस्तेमाल, और शेयर करने के बारे में साफ़ और सही तौर पर बताना होगा. इसमें किसी तीसरे पक्ष की लाइब्रेरी या अपने ऐप्लिकेशन में इस्तेमाल किए गए SDKs टूल की मदद से इकट्ठा और मैनेज किया जाने वाला डेटा भी शामिल है. इस लेबल के सही होने और इसकी जानकारी को अप-टू-डेट रखने की ज़िम्मेदारी डेवलपर की है. जहां ज़रूरी हो वहां डेटा की सुरक्षा वाले सेक्शन और ऐप्लिकेशन की निजता नीति, दोनों ही जगह पर दी गई जानकारी एक जैसी होनी चाहिए.

डेटा की सुरक्षा वाला सेक्शन पूरा करने के बारे में ज़्यादा जानने के लिए सहायता केंद्र का यह लेख पढ़ें.

उपयोगकर्ता के डेटा से जुड़ी नीति पूरी पढ़ें.

संवेदनशील जानकारी ऐक्सेस करने वाली अनुमतियों और एपीआई से जुड़ी नीति

संवेदनशील जानकारी को ऐक्सेस करने वाले सिर्फ़ ऐसे एपीआई और अनुमतियों के लिए अनुरोध करें जो उपयोगकर्ताओं के काम की हों. संवेदनशील जानकारी को ऐक्सेस करने वाले सिर्फ़ ऐसे एपीआई या अनुमतियों का अनुरोध किया जा सकता है जो आपके ऐप्लिकेशन में मौजूदा सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं. ये वे सुविधाएं हैं जिनके बारे में आपने Google Play के स्टोर पेज पर बताया है. ऐसे एपीआई या अनुमतियों का इस्तेमाल नहीं किया जा सकता जिनमें उन सुविधाओं या मकसद के लिए उपयोगकर्ता या डिवाइस के डेटा को ऐक्सेस किया जाता है जिनकी जानकारी न दी गई हो. इनका इस्तेमाल उन सुविधाओं या मकसद के लिए भी नहीं किया जा सकता जो ऐप्लिकेशन में मौजूद न हों या जिनकी अनुमति न हो. अनुमतियों या एपीआई की मदद से, ऐक्सेस किए गए निजी या संवेदनशील डेटा को न तो कभी बेचा जा सकता है और न ही इसे बिक्री की सुविधा देने के मकसद से शेयर किया जा सकता है.

संवेदनशील जानकारी ऐक्सेस करने वाली अनुमतियां और एपीआई नीति पूरी देखें.

SDK टूल की वजह से हुए उल्लंघन के उदाहरण

- SDK टूल वाला ऐसा ऐप्लिकेशन जो बैकग्राउंड में जगह की जानकारी ऐक्सेस करने का अनुरोध करता है, लेकिन उसके मकसद की जानकारी नहीं देता या किसी ऐसी गतिविधि का हवाला देता है जिसकी अनुमति नहीं है.
- SDK टूल वाला ऐसा ऐप्लिकेशन जो उपयोगकर्ता की सहमति के बिना Android फ़ोन के IMEI नंबर की जानकारी अन्य लोगों को भेजता है.

मैलवेयर नीति

हमारी मैलवेयर नीति बहुत आसान है. हम मानते हैं कि Android नेटवर्क और उपयोगकर्ता के डिवाइस, नुकसान पहुंचाने वाली गतिविधियों (जैसे कि मैलवेयर) से दूर रहने चाहिए. Android नेटवर्क में Google Play Store भी शामिल है. इस बुनियादी सिद्धांत के साथ, हम अपने ऐप्लिकेशन इस्तेमाल करने वाले लोगों और उनके Android डिवाइस के लिए सुरक्षित Android नेटवर्क उपलब्ध कराने की कोशिश करते हैं.

मैलवेयर एक कोड होता 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. इनमें ट्रोजन, फ़िशिंग, और स्पायवेयर ऐप्लिकेशन जैसी कैटगरी शामिल हैं. इसके अलावा, हम लगातार नई कैटगरी जोड़ रहे हैं और उन्हें अपडेट कर रहे हैं.

इस नीति की ज़रूरी शर्तें, ऐप्लिकेशन में इस्तेमाल किए जाने वाले तीसरे पक्ष के सभी कोड पर लागू होती हैं (उदाहरण के लिए, एसडीके).

मैलवेयर नीति की पूरी जानकारी पढ़ें.

SDK टूल की वजह से हुए उल्लंघन के उदाहरण

- ऐसा ऐप्लिकेशन जिसमें नुकसान पहुंचाने वाला सॉफ़्टवेयर डिस्ट्रिब्यूट करने वाली कंपनी की एसडीके लाइब्रेरी 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.

- ऐसा ऐप्लिकेशन जिसमें शामिल एसडीके मकसद ज़ाहिर किए बिना डिवाइस पर मौजूद डेटा से खास सुविधाओं का ऐक्सेस हासिल करके, Android की अनुमतियों के मॉडल का उल्लंघन करता है.
- ऐसा ऐप्लिकेशन जिसमें कोड के साथ शामिल एसडीके की वजह से ऐप्लिकेशन इस्तेमाल करने लोग अनजाने में अपने कैरियर बिलिंग से कॉन्टेंट खरीदते या सदस्यता लेते हैं.

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

स्पायवेयर

स्पायवेयर, नुकसान पहुंचाने वाला एक ऐसा ऐप्लिकेशन, गतिविधि या कोड हो सकता है जो नीति का उल्लंघन करते हुए, उपयोगकर्ता या डिवाइस का डेटा बाहर निकालता है, उसे इकट्ठा या शेयर करता है.

इसके अलावा स्पायवेयर, नुकसान पहुंचाने वाली ऐसी गतिविधि या कोड हो सकता है जिसमें उपयोगकर्ता को ज़रूरी सूचना दिए बिना या उसकी सहमति के बिना उसका डेटा निकाला जा सकता है.

स्पायवेयर से जुड़ी नीति की पूरी जानकारी पढ़ें.

उदाहरण के लिए, एसडीके की वजह से स्पायवेयर के ज़रिए होने वाले उल्लंघनों में ये शामिल हैं. हालांकि, इनके अलावा और भी उल्लंघन हो सकते हैं:

- एसडीके वाला ऐसा ऐप्लिकेशन जो ऑडियो या कॉल रिकॉर्डिंग के डेटा को इकट्ठा या शेयर करता है, जबकि उसकी मुख्य सुविधाओं और उनके काम करने के तरीके में ऐसी गतिविधि का ज़िक्र नहीं किया गया हो.
- कोई ऐसा ऐप्लिकेशन जिसमें नुकसान पहुंचाने वाला तीसरे पक्ष का कोड (जैसे, एसडीके) मौजूद हो. इस कोड के ज़रिए डिवाइस का डेटा ट्रांसफ़र होते समय, उपयोगकर्ता को पता न चलता हो और/या उपयोगकर्ता को ज़रूरी सूचना दिए बिना या उसकी सहमति के बिना ऐसा किया जाता हो.

मोबाइल का अनचाहा सॉफ़्टवेयर

पारदर्शी 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, उपयोगकर्ताओं को गुमराह न करने वाले होने चाहिए.

उल्लंघनों के उदाहरण:

- विज्ञापन से होने वाली धोखाधड़ी
- सोशल इंजीनियरिंग

उपयोगकर्ता 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.

उल्लंघनों के उदाहरण:

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

पूरी मोबाइल का अनचाहा सॉफ़्टवेयर देखें

डिवाइस और नेटवर्क के गलत इस्तेमाल से जुड़ी नीति

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. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.

रन टाइम के दौरान लोड की गई इंटरप्रेटेड लैंग्वेज (उदाहरण के लिए, ऐसी लैंग्वेज जो ऐप्लिकेशन के पैकेज में शामिल न हो) का इस्तेमाल करने वाले रन टाइम के दौरान लोड की गई इंटरप्रेटेड लैंग्वेज (उदाहरण के लिए, ऐसी लैंग्वेज जो ऐप्लिकेशन के पैकेज में शामिल न हो) का इस्तेमाल करने वाले ऐसे ऐप्लिकेशन या तीसरे-पक्ष के कोड को किसी भी स्थिति में Google Play की नीतियों का उल्लंघन नहीं

करने देना चाहिए जो रन टाइम (उदाहरण के लिए, बिना ऐप्लिकेशन पैकेज के) पर लोड की गई भाषाओं (उदाहरण के लिए, JavaScript, Python, Lua वगैरह) का इस्तेमाल करते हैं.

हम सुरक्षा में जोखिम की संभावना पैदा करने वाले या उनका फ़ायदा उठाने वाले कोड को अनुमति नहीं देते. डेवलपर के लिए हाल ही में फ़्लैग की गई सुरक्षा से जुड़ी समस्याओं के बारे में जानने के लिए, App Security Improvement Program पर जाएं.

डिवाइस और नेटवर्क के गलत इस्तेमाल से जुड़ी नीति की पूरी जानकारी देखें.

SDK टूल की वजह से हुए उल्लंघन के उदाहरण

- ऐसे ऐप्लिकेशन जो तीसरे पक्ष को प्रॉक्सी सेवा देते हैं. ऐसा सिर्फ़ उन ऐप्लिकेशन में किया जा सकता है जिनका मुख्य मकसद ही प्रॉक्सी सेवा देना है.
- एसडीके का इस्तेमाल करने वाला ऐसा ऐप्लिकेशन जो Google Play के अलावा, किसी अन्य सोर्स से इस्तेमाल किया जा सकने वाला कोड डाउनलोड करता है. इस तरह के कोड में dex फ़ाइलें या नेटिव कोड शामिल हैं.
- एसडीके वाला ऐसा ऐप्लिकेशन जिसमें JavaScript इंटरफ़ेस वाला वेबव्यू होता है. यह वेबव्यू गैर-भरोसेमंद वेब कॉन्टेंट (जैसे कि http:// URL) या गैर-भरोसेमंद सोर्स (जैसे कि गलत इंटेंट वाले यूआरएल) से मिले, बिना पुष्टि वाले यूआरएल लोड करता है.
- एसडीके वाला ऐसा ऐप्लिकेशन जिसमें अपने APK को अपडेट करने वाला कोड शामिल है
- किसी ऐसे SDK टूल वाला ऐप्लिकेशन जो असुरक्षित कनेक्शन पर फाइलें डाउनलोड करके, उपयोगकर्ताओं के डेटा की सुरक्षा को खतरे में डालता है.
- एसडीके वाला ऐसा ऐप्लिकेशन जिसमें Google Play के बाहर ऐसे सोर्स से ऐप्लिकेशन डाउनलोड और इंस्टॉल करने के लिए कोड शामिल हैं जिनके बारे में कोई जानकारी नहीं है.
- आपके ऐप्लिकेशन में ऐसा एसडीके मौजूद है जो ज़रूरी जानकारी दिए बिना फ़ोरग्राउंड सेवाओं का इस्तेमाल करता है.
- आपके ऐप्लिकेशन में ऐसा एसडीके मौजूद है जो नीति का पालन करने की वजह से, फ़ोरग्राउंड सेवाओं का इस्तेमाल करता है. हालांकि, आपके ऐप्लिकेशन के मेनिफ़ेस्ट में इसकी जानकारी नहीं दी गई है.

धोखाधड़ी वाले व्यवहार से जुड़ी नीति

हम उन 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 को पूरे मेटाडेटा में अपनी सुविधाओं के बारे में सही जानकारी, ब्यौरा, और फ़ोटो/वीडियो देना ज़रूरी है. ऐप्लिकेशन को ऑपरेटिंग सिस्टम या दूसरे ऐप्लिकेशन की सुविधाओं या चेतावनियों की नकल करने की कोशिश नहीं करनी चाहिए. डिवाइस की सेटिंग में किसी भी तरह का बदलाव करने से पहले, इस्तेमाल करने वाले को जानकारी देना और उसकी सहमति लेना ज़रूरी है. साथ ही, ये बदलाव ऐसे होने चाहिए जिन्हें उपयोगकर्ता आसानी से पहले जैसा कर सके.

धोखाधड़ी वाले व्यवहार से जुड़ी नीति की पूरी जानकारी देखें.

ऐप्लिकेशन के व्यवहार से जुड़ी पारदर्शिता नीति

आपके ऐप्लिकेशन की सुविधाओं के बारे में लोगों को साफ़ तौर पर जानकारी दी जानी चाहिए. इसमें, आपके ऐप्लिकेशन की छिपी, डॉरमेंट या दस्तावेज़ में नहीं बताई गई सुविधाएं शामिल नहीं हैं. साथ ही, ऐप्लिकेशन की समीक्षाओं से बचने वाली तकनीकों का इस्तेमाल न करें. ऐसा हो सकता है कि आपको अपने ऐप्लिकेशन के लिए अतिरिक्त जानकारी देनी पड़े. इससे, यह पक्का किया जा सकेगा कि आपके ऐप्लिकेशन लोगों के लिए सुरक्षित हैं, नीति का पूरी तरह से पालन करते हैं, और इन पर सिस्टम को मज़बूत स्तर की पूरी सुरक्षा मिलती है.

SDK टूल की वजह से नीति के उल्लंघन का उदाहरण

- आपके ऐप्लिकेशन में ऐसा SDK टूल है जो ऐप्लिकेशन की समीक्षाओं से बचने के लिए इस्तेमाल किया जाता है.

Google Play की कौनसी डेवलपर नीतियां आम तौर पर SDK टूल वाले ऐप्लिकेशन की वजह से हो रहे उल्लंघन से जुड़ी हुई हैं?

यह पक्का करने के लिए कि आपका ऐप्लिकेशन, तीसरे पक्ष के जिस कोड का इस्तेमाल कर रहा है वह Google Play की डेवलपर कार्यक्रम की नीतियों के मुताबिक हो, कृपया यहां दी गई नीतियों को अच्छी तरह से पढ़ें:

- उपयोगकर्ता के डेटा से जुड़ी नीति
- संवेदनशील जानकारी ऐक्सेस करने वाली अनुमतियां और एपीआई
- डिवाइस और नेटवर्क के गलत इस्तेमाल से जुड़ी नीति
- मैलवेयर
- मोबाइल का अनचाहा सॉफ़्टवेयर

- Families Self-Certified Ads SDK Program
- विज्ञापन नीति
- धोखाधड़ी करना
- Google Play के डेवलपर कार्यक्रम की नीतियां

हालांकि, इन नीतियों को लागू करने के बारे में विचार किया जा रहा है. इसलिए, इस बात का ध्यान रखना बेहद ज़रूरी है कि नुकसान पहुंचाने वाले SDK कोड की वजह से, आपका ऐप्लिकेशन किसी ऐसी नीति का उल्लंघन कर सकता है जिसके बारे में ऊपर नहीं बताया गया है. समय-समय पर सभी नीतियों की समीक्षा करें और पूरी तरह से अप-टू-डेट रहें. यह ऐप्लिकेशन डेवलपर की ज़िम्मेदारी है कि जिन SDKs टूल का इस्तेमाल किया जा रहा है वे ऐप्लिकेशन डेटा को नीतियों के मुताबिक ही इस्तेमाल करें.

ज़्यादा जानने के लिए, कृपया हमारे सहायता केंद्र पर जाएं.

मैलवेयर

हमारी मैलवेयर नीति बहुत आसान है. हम मानते हैं कि Android नेटवर्क और उपयोगकर्ता के डिवाइस, नुकसान पहुंचाने वाली गतिविधियों (जैसे कि मैलवेयर) से दूर रहने चाहिए. Android नेटवर्क में Google Play Store भी शामिल है. इस बुनियादी सिद्धांत के साथ, हम अपने ऐप्लिकेशन इस्तेमाल करने वाले लोगों और उनके Android डिवाइस के लिए सुरक्षित Android नेटवर्क उपलब्ध कराने की कोशिश करते हैं.

मैलवेयर एक कोड होता 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. इनमें ट्रोजन, फ़िशिंग, और स्पायवेयर ऐप्लिकेशन जैसी कैटगरी शामिल हैं. इसके अलावा, हम लगातार नई कैटगरी जोड़ रहे हैं और उन्हें अपडेट कर रहे हैं.

इस नीति की ज़रूरी शर्तें, ऐप्लिकेशन में इस्तेमाल किए जाने वाले तीसरे पक्ष के सभी कोड पर लागू होती हैं (उदाहरण के लिए, एसडीके).

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

- उपयोगकर्ता के डिवाइस की सुरक्षा खतरे में डालना.
- उपयोगकर्ता के डिवाइस को कंट्रोल करना.
- किसी सायबर 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. इस वजह से, नुकसान पहुंचाने वाली गतिविधियां हो सकती हैं, भले ही उनका इरादा खतरा पैदा करना न हो. ऐसा इसलिए होता है, क्योंकि ऐप्लिकेशन, बाइनरी या फ़्रेमवर्क में होने वाले बदलाव अलग तरह से काम कर सकते हैं. ऐसा कई तरह के वैरिएबल मौजूद होने की वजह से होता 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 कैटगरी, 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 नेटवर्क को बेहतर बनाने में बढ़ावा देता है, ताकि उपयोगकर्ता भरोसा कर सकें.

ज़्यादा जानकारी के लिए, Google Play Protect पर जाएं.

बैकडोर

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

इन कार्रवाइयों में ऐसी गतिविधि शामिल हो सकती है जो उपयोगकर्ता की अनुमति के बिना ही, ऐप्लिकेशन, बाइनरी या फ़्रेमवर्क में हुए बदलाव को किसी भी तरह के मैलवेयर में शामिल कर सकती है. सामान्य तौर पर, बैकडोर की मदद से यह देखा जाता है कि किसी

डिवाइस पर किस तरह नुकसान पहुंचा रहा है. इसीलिए, यह बिलिंग से जुड़ी धोखाधड़ी करने वाली या कारोबारी स्पायवेयर से थोड़ा अलग होता है. इस वजह से, कुछ मामलों में बैकडोर के खास सेट को Google Play Protect को जोख़िम से भरा माना जाता है.

बिलिंग से जुड़ी धोखाधड़ी करना

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

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

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

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

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

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

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

Stalkerware

ऐसा कोड जो किसी डिवाइस से उपयोगकर्ता का निजी या संवेदनशील डेटा इकट्ठा करता है और उसे निगरानी के मकसद से किसी तीसरे पक्ष (संगठन या अन्य व्यक्ति) को भेजता है.

ऐप्लिकेशन को साफ़ तौर पर ज़रूरी जानकारी ज़ाहिर करनी चाहिए और सहमति लेनी चाहिए, जैसा कि उपयोगकर्ता के डेटा से जुड़ी नीति के तहत ज़रूरी है.

ऐप्लिकेशन की निगरानी के लिए दिशा-निर्देश

सिर्फ़ उन ऐप्लिकेशन को निगरानी करने वाले ऐप्लिकेशन के रूप में मंज़ूरी दी जाती है जो खास तौर पर, अन्य व्यक्ति की निगरानी के लिए बनाए और बेचे जाते हों. उदाहरण के लिए, बच्चों की निगरानी करने में अभिभावकों की मदद करने या कर्मचारियों की निगरानी में संगठन के मैनेजमेंट की मदद करने लिए. साथ ही, ये ऐप्लिकेशन नीचे बताई गई ज़रूरी शर्तों का पूरी तरह से पालन करते हों. लगातार सूचना दिखाने के बावजूद, इन ऐप्लिकेशन का इस्तेमाल करके किसी अन्य व्यक्ति (उदाहरण के लिए, पति या पत्नी) की निगरानी नहीं की जा सकती. ऐसा तब भी नहीं किया जा सकता, जब उसे इस बात की जानकारी दी गई हो और उसकी अनुमति ली गई हो. इन ऐप्लिकेशन की मेनिफ़ेस्ट फ़ाइल में IsMonitoringTool मेटाडेटा फ़्लैग का इस्तेमाल करना चाहिए. इससे, इन ऐप्लिकेशन को निगरानी वाले ऐप्लिकेशन के तौर पर सूची में शामिल किया जा सकेगा.

निगरानी करने वाले ऐप्लिकेशन को इन ज़रूरी शर्तों का पालन करना होगा:

- ऐप्लिकेशन को पेश करने के तरीके से ऐसा नहीं लगना चाहिए कि वे जासूसी के लिए बने हैं या गुप्त तौर पर निगरानी करने की सेवा देते हैं.
- ऐप्लिकेशन को निगरानी से जुड़ी गतिविधियां नहीं छिपानी चाहिए या उससे जुड़ी किसी जानकारी को गलत तरीके से पेश नहीं करना चाहिए. इसके अलावा, ऐसी सुविधा के बारे में लोगों को गुमराह नहीं करना चाहिए.
- जब ऐप्लिकेशन काम कर रहा हो, उस दौरान उपयोगकर्ताओं को लगातार सूचना दिखनी चाहिए. साथ ही, एक खास आइकॉन भी दिखना चाहिए, ताकि ऐप्लिकेशन को साफ़ तौर पर पहचाना जा सके.

- ऐप्लिकेशन को Google Play Store पर दिए गए उसके ब्यौरे में यह ज़ाहिर करना चाहिए कि उसमें निगरानी या ट्रैक करने का फ़ंक्शन है.
- Google Play पर मौजूद ऐप्लिकेशन और ऐप लिस्टिंग में, किसी भी सुविधा को चालू करने या उसे ऐक्सेस करने का ऐसा कोई तरीका उपलब्ध नहीं कराना चाहिए जिससे इन शर्तों का उल्लंघन होता हो. उदाहरण के लिए, Google Play से बाहर होस्ट किए गए और शर्तों का पालन न करने वाले APK से लिंक करना.
- ऐप्लिकेशन को उन सभी कानूनों का पालन करना होगा जो लागू हो. अपने ऐप्लिकेशन के लिए टारगेट की गई स्थान-भाषा की सभी कानूनी ज़िम्मेदारी सिर्फ़ आपकी है.

ज़्यादा जानकारी के लिए, सहायता केंद्र पर isMonitoringTool फ़्लैग इस्तेमाल करने का तरीका लेख पढ़ें.

सेवा में रुकावट (DoS)

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

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

गलत तरीके से डाउनलोड करने वाले मैलवेयर

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

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

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

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

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

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

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

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

फ़िशिंग

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

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

खास अधिकारों का गलत इस्तेमाल

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

उदाहरणों में ये शामिल हैं:

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

- ऐसा ऐप्लिकेशन जो SELinux को काम करने से रोकता है.

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

रैंसमवेयर

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

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

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

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

रूट किया जा रहा है

ऐसा कोड जो डिवाइस को रूट करता है.

नुकसान पहुंचाने के लिए डिवाइस को रूट करने वाला कोड और नुकसान नहीं पहुंचाने वाला कोड, दोनों में अंतर है. उदाहरण के लिए, नुकसान नहीं पहुंचाने के लिए डिवाइस को रूट करने वाले ऐप्लिकेशन, लोगों को डिवाइस रूट करने की जानकारी पहले ही दे देते हैं. साथ ही, ये ऐप्लिकेशन ऐसी कार्रवाइयां नहीं करते हैं जो डिवाइस की अन्य पीएचए की श्रेणियों पर लागू होती हैं.

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

स्पैम

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

स्पायवेयर

स्पायवेयर, नुकसान पहुंचाने वाला एक ऐसा ऐप्लिकेशन, गतिविधि या कोड हो सकता है जो नीति का उल्लंघन करते हुए, उपयोगकर्ता या डिवाइस का डेटा बाहर निकालता है, उसे इकट्ठा या शेयर करता है.

इसके अलावा स्पायवेयर, नुकसान पहुंचाने वाली ऐसी गतिविधि या कोड हो सकता है जिसमें उपयोगकर्ता को ज़रूरी सूचना दिए बिना या उसकी सहमति के बिना उसका डेटा निकाला जा सकता है.

उदाहरण के लिए, स्पायवेयर के ज़रिए होने वाले उल्लंघनों में ये शामिल हैं. हालांकि, इनके अलावा और भी उल्लंघन हो सकते हैं:

- फ़ोन से ऑडियो रिकॉर्ड करना या फ़ोन कॉल रिकॉर्ड करना
- ऐप्लिकेशन का डेटा चुराना
- कोई ऐसा ऐप्लिकेशन जिसमें नुकसान पहुंचाने वाला तीसरे पक्ष का कोड (जैसे, SDK टूल) मौजूद हो. इस कोड के ज़रिए डिवाइस का डेटा ट्रांसफ़र होते समय, उपयोगकर्ता को पता न चलता हो और/या उपयोगकर्ता को ज़रूरी सूचना दिए बिना या उसकी सहमति के बिना ऐसा किया जाता हो.

यह ज़रूरी है कि हर ऐप्लिकेशन, Google Play Developer Program की सभी नीतियों के मुताबिक हो. इसमें उपयोगकर्ता और डिवाइस का डेटा सुरक्षित रखने से जुड़ी नीतियां भी शामिल हैं. जैसे, मोबाइल का अनचाहा सॉफ़्टवेयर, उपयोगकर्ता का डेटा, संवेदनशील जानकारी ऐक्सेस करने वाली अनुमतियां और एपीआई, और SDK टूल इस्तेमाल करने की ज़रूरी शर्तें में बताई गई नीतियां.

ट्रोजन

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

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

असामान्य ऐप्लिकेशन पर नोट

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

बैकडोर वाले मैलवेयर पर नोट

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

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

मास्कवेयर

एक ऐसा ऐप्लिकेशन जो लोगों को ऐप्लिकेशन से जुड़ी अलग-अलग या नकली सुविधाएं देने के लिए, कई गलत तकनीकों का इस्तेमाल करता है. ये ऐप्लिकेशन खुद को भरोसेमंद ऐप्लिकेशन या गेम के तौर पर दिखाते हैं, ताकि ऐप स्टोर में इन्हें देखकर किसी तरह के नुकसान का डर न हो. नुकसान पहुंचाने वाला कॉन्टेंट दिखाने के लिए ये ऐप्लिकेशन अलग-अलग तकनीकों का इस्तेमाल करते हैं. जैसे, कोड को अस्पष्ट बनाना, डाइनैमिक कोड लोडिंग या क्लोकिंग.

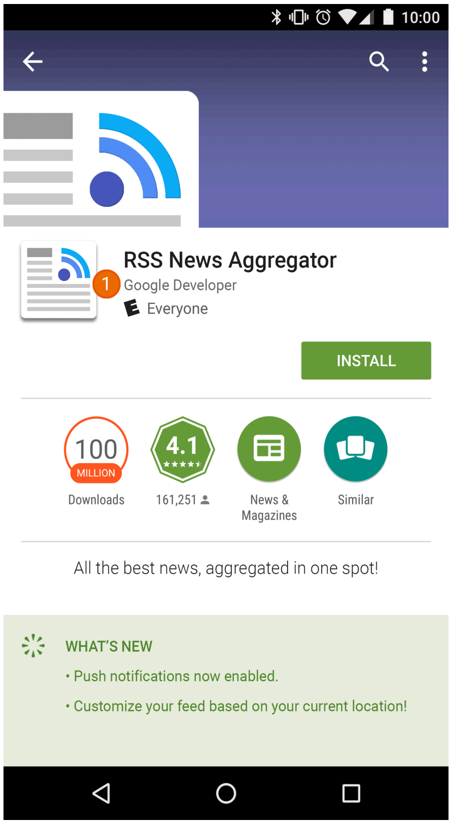
मास्कवेयर, अन्य पीएचए कैटगरी वाले ऐप्लिकेशन की तरह होता है (खास तौर पर ट्रोजन). इनमें मुख्य अंतर, नुकसान पहुंचाने वाली गतिविधि को अस्पष्ट बनाने के लिए इस्तेमाल होने वाली तकनीकों का होता है.

किसी दूसरे के नाम पर काम करना

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 आपका ऐप्लिकेशन किसी से जुड़ा नहीं है और न ही किसी ने इसे अनुमति दी है, तो इसका झूठा दावा न करें. इस बात का ध्यान रखें कि किसी ऐसी जानकारी का इस्तेमाल न करें जो लोगों को आपके ऐप्लिकेशन के किसी दूसरे व्यक्ति या किसी दूसरे ऐप्लिकेशन के साथ संबंध के बारे में गुमराह करती हो. इस जानकारी में ऐप्लिकेशन आइकॉन, ब्यौरे, शीर्षक या ऐप्लिकेशन के अंदर मौजूद दूसरी चीज़ें शामिल होती हैं.

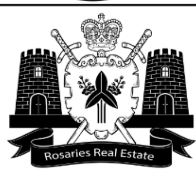
आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण यहां दिए गए हैं:

- ऐसे डेवलपर जो किसी अन्य कंपनी / डेवलपर / इकाई / संगठन 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.

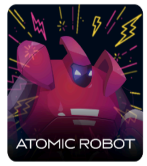
- ऐसे ऐप्लिकेशन जिनके आइकॉन और नाम से लगता है कि उनका संबंध किसी अन्य कंपनी / डेवलपर / इकाई / संगठन से है, जबकि यह सही नहीं होता.

✓		
✗	① 	②

①ऐप्लिकेशन में राष्ट्रीय प्रतीक का इस्तेमाल करके, लोगों को गुमराह कर यह भरोसा दिलाना कि ऐप्लिकेशन सरकार से जुड़ी हुई है.
②ऐप्लिकेशन में किसी कारोबारी इकाई के लोगो की नकल की जा रही है, ताकि झूठे तौर पर यह दिखाया जा सके कि वह उस कारोबारी इकाई का आधिकारिक ऐप्लिकेशन है.

- ऐसे ऐप्लिकेशन जिनके नाम और आइकॉन, पहले से मौजूद किसी प्रॉडक्ट या सेवाओं से मिलते-जुलते हैं. इससे, उपयोगकर्ता गुमराह हो सकते हैं.

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

✓		
✗	①	② 

①ऐप्लिकेशन के ऐप्लिकेशन आइकॉन में किसी मशहूर क्रिप्टो करंसी वेबसाइट का इस्तेमाल किया जा रहा है, ताकि ऐसा लगे कि वह आधिकारिक वेबसाइट है.
②ऐप्लिकेशन के ऐप्लिकेशन आइकॉन में किसी मशहूर टीवी शो के कैरेक्टर और नाम की नकल की जा रही है, ताकि उपयोगकर्ताओं को गुमराह कर यह भरोसा दिलाया जा सके कि ऐप्लिकेशन उस टीवी शो से जुड़ा हुआ है.

- ऐसे ऐप्लिकेशन जो 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.
- ऐसे ऐप्लिकेशन जो Android ब्रैंड के दिशा-निर्देशों का उल्लंघन करते हैं.

मोबाइल का अनचाहा सॉफ़्टवेयर

Google का मानना है कि अगर हम ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति पर ध्यान देंगे, तो बाकी सब भी अपने-आप बेहतर हो जाएगा. 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 स्टोर' के सिद्धांतों से Google की अनचाही सॉफ़्टवेयर नीति पर बनाई जाती 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.

पारदर्शी व्यवहार और साफ़ जानकारी

सभी कोड ऐसे होने चाहिए जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति से किए गए वादों के हिसाब से हों. ऐप्लिकेशन को सुविधाओं की सभी जानकारी देनी चाहिए. ऐप्लिकेशन, इस्तेमाल करने वालों को गुमराह न करने वाले होने 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
- सोशल इंजीनियरिंग

उपयोगकर्ता के डेटा और निजता को सुरक्षित रखना

उपयोगकर्ता 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 उपयोगकर्ता के डेटा से जुड़ी सभी ज़रूरी नीतियों का पालन करना चाहिए. साथ ही, डेटा की सुरक्षा के लिए सभी सावधानियां रखें.

- उपयोगकर्ताओं 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 ऐसी अन्य निजी और संवेदनशील जानकारी शामिल है जिसे उपयोगकर्ता को इकट्ठा किए जाने की उम्मीद नहीं होगी.
- उपयोगकर्ता का इकट्ठा किया गया निजी और संवेदनशील डेटा सुरक्षित तरीके से हैंडल किया जाना चाहिए. इसमें मॉर्डन क्रिप्टोग्राफ़ी (उदाहरण के लिए, एचटीटीपीएस पर) का इस्तेमाल करना भी शामिल है.
- मोबाइल ऐप्लिकेशन के साथ-साथ सॉफ़्टवेयर को उपयोगकर्ता के निजी और संवेदनशील डेटा को सिर्फ़ सर्वर पर भेजना चाहिए. ऐसा इसलिए, क्योंकि यह ऐप्लिकेशन की सुविधाओं से जुड़ा हुआ है.
- उपयोगकर्ताओं से डिवाइस की सुरक्षा सुविधाओं को बंद करने के लिए न तो अनुरोध करें और न ही उन्हें गुमराह करके ऐसा करवाएं. उदाहरण के लिए, Google Play Protect की सुविधा बंद करने के लिए, उपयोगकर्ताओं को ऐप्लिकेशन की अन्य सुविधाएं या इनाम ऑफ़र न करें.

उल्लंघनों के उदाहरण:

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

उपयोगकर्ता के डेटा से जुड़ी नीतियों का उदाहरण:

- Google Play के उपयोगकर्ता के डेटा से जुड़ी नीति
- GMS के उपयोगकर्ता के डेटा से जुड़ी नीति की ज़रूरी शर्तें
- Google API सेवा के उपयोगकर्ता के डेटा से जुड़ी नीति

मोबाइल पर ऐप्लिकेशन इस्तेमाल करने के अनुभव को खराब न करें

इस्तेमाल करने वाले व्यक्ति का अनुभव सरल, समझने में आसान, और उसकी पसंद पर आधारित होना चाहिए. इसे इस्तेमाल करने वाले व्यक्ति को खास बातें साफ़ तौर पर बतानी चाहिए. साथ ही, विज्ञापन में बताए गए और उपयोगकर्ता के पसंदीदा अनुभव में बदलाव नहीं करना 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 के काम करने के तरीके का बिना अनुमति इस्तेमाल करना या उसकी नकल करना

गलत चीज़ें डाउनलोड करने वाला मैलवेयर

ऐसा कोड जो खुद अनचाहा सॉफ़्टवेयर नहीं है, लेकिन मोबाइल के लिए अन्य अनचाहे सॉफ़्टवेयर (MUwS) को डाउनलोड करता है.

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

- ऐसा लगे कि इसे MUwS फैलाने के लिए बनाया गया है या इसने MUwS डाउनलोड किया है. इसके अलावा, इसमें ऐसा कोड शामिल है जो ऐप्लिकेशन इंस्टॉल और डाउनलोड कर सकता है या
- 500 ऐप्लिकेशन डाउनलोड करने वाले इस कोड से डाउनलोड किए गए, कम से कम 5% यानी 25 ऐप्लिकेशन MUwS हों.

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

- वे उपयोगकर्ता की अनुमति के बिना डाउनलोड नहीं करते और
- उपयोगकर्ताओं की अनुमति मिलने पर ही सभी सॉफ़्टवेयर डाउनलोड होते हैं.

विज्ञापनों से होने वाली धोखाधड़ी

विज्ञापनों से होने वाली 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. विज्ञापनों से होने वाली धोखाधड़ी तब हो सकती है, जब डेवलपर विज्ञापन दिखाने के लिए बिना अनुमति वाले तरीके इस्तेमाल करते हैं, जैसे कि छिपे हुए विज्ञापन दिखाना, उन पर अपने-आप क्लिक होना, जानकारी में बदलाव या उसमें छेड़छाड़ करना, और गैर-मानवीय कार्रवाइयों (स्पाइडर, बॉट वगैरह) का गलत तरीके से फ़ायदा लेना. साथ ही, अमान्य विज्ञापन ट्रैफ़िक लाने वाली मानव गतिविधि भी इनमें शामिल है. विज्ञापनों से होने वाली धोखाधड़ी और अमान्य ट्रैफ़िक से विज्ञापन देने वाले लोगों, डेवलपर, और ऐप्लिकेशन इस्तेमाल करने वाले लोगों को नुकसान पहुंचता है. इससे, लोग मोबाइल विज्ञापन नेटवर्क पर लंबे समय के लिए भरोसा खो देते हैं.

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

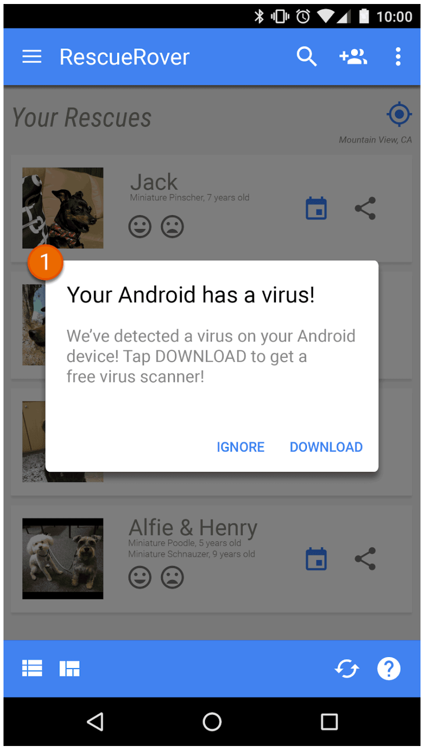
- ऐसा ऐप्लिकेशन जो लोगों को दिखाई न देने वाले विज्ञापन रेंडर करता है.
- ऐसा ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की इच्छा के बिना अपने-आप विज्ञापनों पर क्लिक करता है या धोखाधड़ी से विज्ञापनों पर क्लिक का क्रेडिट उपयोगकर्ता को देने के लिए, ऐसे किसी नेटवर्क का इस्तेमाल करता है.
- ऐसा ऐप्लिकेशन जो इंस्टॉल 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.
- विज्ञापन इन्वेंट्री को गलत तरीके से दिखाने वाला ऐप्लिकेशन. उदाहरण के लिए, ऐसा ऐप्लिकेशन जो विज्ञापन नेटवर्क कंपनी को दिखाता है कि यह iOS डिवाइस पर काम कर रहा है, जबकि असल में यह Android डिवाइस पर काम कर रहा होता है. साथ ही, ऐसा ऐप्लिकेशन जो कमाई करने वाले पैकेज के नाम को गलत तरीके से पेश करता है.

सिस्टम के काम करने के तरीके का बिना अनुमति इस्तेमाल करना या उसकी नकल करना

हम ऐसे ऐप्लिकेशन या विज्ञापनों की अनुमति नहीं देते हैं जो सूचना या चेतावनी जैसे सिस्टम के फ़ंक्शन की नकल करते हैं या उसमें दखल देते हैं. सिस्टम के लेवल पर मिलने वाली सूचनाओं (सिस्टम नोटिफ़िकेशन) का इस्तेमाल सिर्फ़ किसी ऐप्लिकेशन की ज़रूरी सुविधाओं के लिए किया जा सकता है. उदाहरण के लिए, कोई ऐसा एयरलाइन ऐप्लिकेशन जो लोगों को खास ऑफ़र के बारे में सूचना देता है या ऐसा गेम जो लोगों को गेम के अंदर किए जाने वाले प्रचार के बारे में सूचना देता है.

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

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



① इस ऐप्लिकेशन में दिखने वाली सिस्टम नोटिफ़िकेशन का इस्तेमाल विज्ञापन दिखाने के लिए किया जाता है.

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

सोशल इंजीनियरिंग

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों को गुमराह करने के मकसद से, किसी अन्य ऐप्लिकेशन की नकल करते हैं. इसके अलावा, वे इस तरीके से काम करते हैं कि उपयोगकर्ता को यह लगे कि वह सही और भरोसेमंद ऐप्लिकेशन का इस्तेमाल कर रहा है.

कमाई करना और विज्ञापन

Google Play, डेवलपर और उपयोगकर्ताओं के फ़ायदे के लिए कमाई करने के कई तरीके देता है. इनमें पैसे देकर खरीदे जाने वाले ऐप्लिकेशन वितरण, ऐप्लिकेशन के अंदर उत्पाद, सदस्यताएं, और अलग-अलग तरह के विज्ञापन मॉडल के हिसाब से ऐप्लिकेशन तैयार करने जैसे तरीके शामिल हैं. उपयोगकर्ताओं को बेहतर अनुभव देने के लिए, हम चाहते हैं कि आप इन नीतियों का पालन करें.

पैसे चुकाना

1. Google Play से ऐप्लिकेशन डाउनलोड करने के लिए लोगों से शुल्क लेने वाले डेवलपर को ऐसे लेन-देन के लिए, Google Play के बिलिंग सिस्टम का इस्तेमाल करना होगा.
2. Play पर मौजूद कुछ ऐप्लिकेशन की सुविधाओं या सेवाओं को ऐक्सेस करने के लिए पैसे चुकाने पड़ते हैं. जैसे, ऐप्लिकेशन की मुख्य सुविधाएं और उनके काम करने का तरीका, डिजिटल कॉन्टेंट या आइटम (इन्हें “इन-ऐप्लिकेशन खरीदारी” कहा जाता है). इनकी खरीदारी के दौरान होने वाले लेन-देन के लिए, ऐप्लिकेशन को Google Play के बिलिंग सिस्टम का ही इस्तेमाल करना होगा. हालांकि, इसके लिए ज़रूरी है कि ऐसे लेन-देन सेक्शन 3, सेक्शन 8 या सेक्शन 9 के दायरे में न आते हों.

   ऐप्लिकेशन की ऐसी सुविधाओं या सेवाओं के उदाहरण जिनके लिए Google Play के बिलिंग सिस्टम का इस्तेमाल करना ज़रूरी है. इनमें नीचे दी गई चीज़ों की इन-ऐप्लिकेशन खरीदारी शामिल है. हालांकि, और भी चीज़ें शामिल हो सकती हैं:

   - आइटम, जैसे कि वर्चुअल करंसी, खेलने के कुछ और मौके, खेलने के लिए कुछ और समय, ऐड-ऑन आइटम, किरदार, और अवतार;
   - सदस्यता सेवाएं, जैसे कि फ़िटनेस, गेम, डेटिंग, शिक्षा, संगीत, वीडियो, सेवा अपग्रेड, और अन्य कॉन्टेंट से जुड़ी सदस्यता सेवाएं;

- ऐप्लिकेशन की सुविधाएं या कॉन्टेंट, जैसे कि किसी ऐप्लिकेशन का ऐसा वर्शन जिस पर कोई विज्ञापन न दिखता हो या ऐसी नई सुविधाएं मिलती हों जो मुफ़्त वर्शन में न मिलें; और
- क्लाउड सॉफ़्टवेयर और सेवाएं, जैसे कि डेटा स्टोर करने वाली सेवाएं, कारोबार की उत्पादकता बढ़ाने वाला सॉफ़्टवेयर, और वित्तीय मामलों को मैनेज करने वाला सॉफ़्टवेयर.

3. उन मामलों में Google Play के बिलिंग सिस्टम का इस्तेमाल नहीं करना चाहिए जहां:
   a. असली मकसद इनके लिए पैसे चुकाना हो:
      - सामान खरीदने या किराये पर लेने के लिए, जैसे कि किराने का सामान, कपड़े, घरेलू सामान, इलेक्ट्रॉनिक सामान;
      - सेवाओं की खरीदारी के लिए, जैसे कि परिवहन सेवाएं, सफ़ाई से जुड़ी सेवाएं, हवाई किराया, जिम की सदस्यताएं, खाने की डिलीवरी, लाइव इवेंट के टिकट; या
      - क्रेडिट कार्ड या बिजली-पानी जैसी सुविधाओं के साथ-साथ, केबल और दूरसंचार सेवाओं के बिल चुकाने के लिए;
   b. पीयर-टू-पीयर पेमेंट और ऑनलाइन नीलामी वाले पेमेंट के साथ-साथ, ऐसे दान के लिए जिनमें टैक्स से छूट मिलती है;
   c. ऐसे कॉन्टेंट या सेवाओं का पेमेंट करने के लिए जो ऑनलाइन जुए से जुड़ी सुविधाएं देती हैं, जैसा कि असली पैसे दांव पर लगाकर खेले जाने वाले जुए, गेम, और प्रतियोगिताओं से जुड़ी नीति के जुआ खेलने की सुविधा देने वाले ऐप्लिकेशन सेक्शन में बताया गया है;
   d. ऐसी कैटगरी के प्रॉडक्ट का पेमेंट करने के लिए जिन्हें Google के पेमेंट सेंटर से जुड़ी कॉन्टेंट की नीति के तहत स्वीकार नहीं किया जाता.

   ध्यान दें: कुछ बाज़ारों में, हम ऐसे ऐप्लिकेशन के लिए Google Pay का विकल्प देते हैं जो सामान बेचते हैं और/या सेवाएं देते हैं. ज़्यादा जानकारी के लिए, कृपया हमारे Google Pay डेवलपर पेज पर जाएं.

4. सेक्शन 3, सेक्शन 8, सेक्शन 9 में बताई गई शर्तों को छोड़कर अन्य सभी स्थितियों में, ऐप्लिकेशन अपने उपयोगकर्ताओं को Google Play के बिलिंग सिस्टम के बजाय पेमेंट के किसी दूसरे तरीके पर नहीं ले जा सकते. उपयोगकर्ताओं को नीचे दिए गए तरीकों के ज़रिए पेमेंट के किसी दूसरे तरीके पर नहीं ले जाया जा सकता (ध्यान रखें कि यहां दिए गए उदाहरणों के अलावा, इसमें दूसरे मामले भी शामिल हो सकते हैं):
   - Google Play में ऐप्लिकेशन के स्टोर पेज;
   - खरीदे जा सकने वाले कॉन्टेंट का ऐप्लिकेशन में प्रमोशन;
   - इन-ऐप्लिकेशन वेबव्यू, बटन, लिंक, मैसेज सेवा, विज्ञापन या दूसरे कॉल-टू-ऐक्शन; और
   - खाता बनाने या साइन-अप करने जैसे इन-ऐप्लिकेशन यूज़र इंटरफ़ेस फ़्लो, जो उपयोगकर्ताओं को Google Play के बिलिंग सिस्टम के अलावा, पेमेंट के किसी दूसरे तरीके पर ले जाते हों.
5. इन-ऐप्लिकेशन वर्चुअल करंसी का इस्तेमाल, सिर्फ़ ऐसे ऐप्लिकेशन या गेम में किया जाना चाहिए जिसके लिए उन्हें खरीदा गया था.
6. डेवलपर के लिए ज़रूरी है कि वे लोगों को अपने ऐप्लिकेशन की शर्तों और कीमत के बारे में साफ़ और सही जानकारी दें. इसके अलावा, उनके ऐप्लिकेशन में खरीदने के लिए उपलब्ध, किसी भी इन-ऐप्लिकेशन सुविधा या सदस्यता के बारे में भी साफ़ और सही जानकारी देनी चाहिए. इन-ऐप्लिकेशन प्रॉडक्ट और सुविधाओं की कीमत, उपयोगकर्ता के लिए उपलब्ध Play Billing इंटरफ़ेस में दिख रही कीमत से मेल खानी चाहिए. अगर Google Play पर आपके प्रॉडक्ट की जानकारी में, ऐसी इन-ऐप्लिकेशन सुविधाओं के बारे में बताया गया हो जिनके लिए किसी खास या अतिरिक्त शुल्क की ज़रूरत हो सकती है, तो ऐप लिस्टिंग में लोगों को साफ़ तौर पर बताना चाहिए कि उन सुविधाओं का इस्तेमाल करने के लिए पैसे चुकाना ज़रूरी है.
7. कुछ ऐप्लिकेशन और गेम, ऐसे वर्चुअल आइटम खरीदने की सुविधा देते हैं जो किसी खास क्रम के हिसाब से नहीं दिए जाते हैं. इनमें "लूट बॉक्स" जैसी कई चीज़ें शामिल हो सकती हैं. ऐसे आइटम बेचने वाले ऐप्लिकेशन या गेम को, खरीदारी से पहले ही लोगों को साफ़ तौर पर बताना होगा कि इन आइटम को हासिल करने की संभावना कितनी है. साथ ही, यह भी बताना होगा कि उन्हें खरीदारी के कितने समय बाद ये आइटम मिलेंगे.
8. Play पर मौजूद ऐप्लिकेशन के डेवलपर इन देशों/इलाकों में उपयोगकर्ताओं को Google Play के बिलिंग सिस्टम के साथ-साथ अन्य बिलिंग सिस्टम की सुविधा दे सकते हैं. ऐसा उन ऐप्लिकेशन के लिए ही किया जा सकता है जिनमें इन-ऐप्लिकेशन खरीदारी के लिए उपयोगकर्ताओं से पैसे लिए जाते हैं या स्वीकार किए जाते हैं. इसके लिए डेवलपर को हर प्रोग्राम के लिए, बिलिंग सिस्टम का एलान करने वाला फ़ॉर्म भरना होगा और उसमें शामिल अन्य शर्तों और प्रोग्राम की शर्तों के लिए सहमति देनी होगी. हालांकि, यह ज़रूरी है कि ऐसे मामलों में सेक्शन 3 में बताई गई शर्तें लागू न होती हों.
9. Play पर मौजूद ऐप्लिकेशन के डेवलपर, यूरोपियन इकनॉमिक एरिया (ईईए) के लोगों को, ऐप्लिकेशन से बाहर किसी और पेज पर रीडायरेक्ट कर सकते हैं. जैसे, ऐप्लिकेशन में मौजूद सुविधाओं और सेवाओं के प्रमोशन के लिए वे ऐसा कर सकते हैं. ऐसे डेवलपर को प्रोग्राम के लिए एलान वाला फ़ॉर्म भरना होगा. साथ ही, उन्हें बताई गई अतिरिक्त शर्तों और प्रोग्राम की ज़रूरी शर्तों को स्वीकार करना होगा.

ध्यान दें: इस नीति से जुड़े अक्सर पूछे जाने वाले सवाल और समयावधि देखने के लिए, कृपया हमारे सहायता केंद्र पर जाएं.

विज्ञापन

उपयोगकर्ताओं को अच्छा अनुभव मिलता रहे, इसके लिए हम आपके विज्ञापन के कॉन्टेंट, ऑडियंस, उपयोगकर्ता अनुभव, और व्यवहार के साथ-साथ, सुरक्षा और निजता का भी ध्यान रखते हैं. हम विज्ञापनों और उनसे जुड़े ऑफ़र को आपके ऐप्लिकेशन का हिस्सा मानते हैं. इसलिए, यह ज़रूरी है कि वे भी Google Play की अन्य सभी नीतियों का पालन करें. अगर आपको Google Play पर मौजूद किसी ऐसे ऐप्लिकेशन से कमाई करना है जो बच्चों को टारगेट करता है, तो आपको विज्ञापन के लिए हमारी कुछ अन्य शर्तों को पूरा करना होगा.

ऐप्लिकेशन के प्रमोशन और स्टोर पेज की हमारी नीतियों के बारे में ज़्यादा जानकारी के लिए, यहां जाएं. साथ ही, यह भी जानें कि हम धोखाधड़ी से प्रमोशन करने के मामलों से कैसे निपटते हैं.

विज्ञापन का कॉन्टेंट

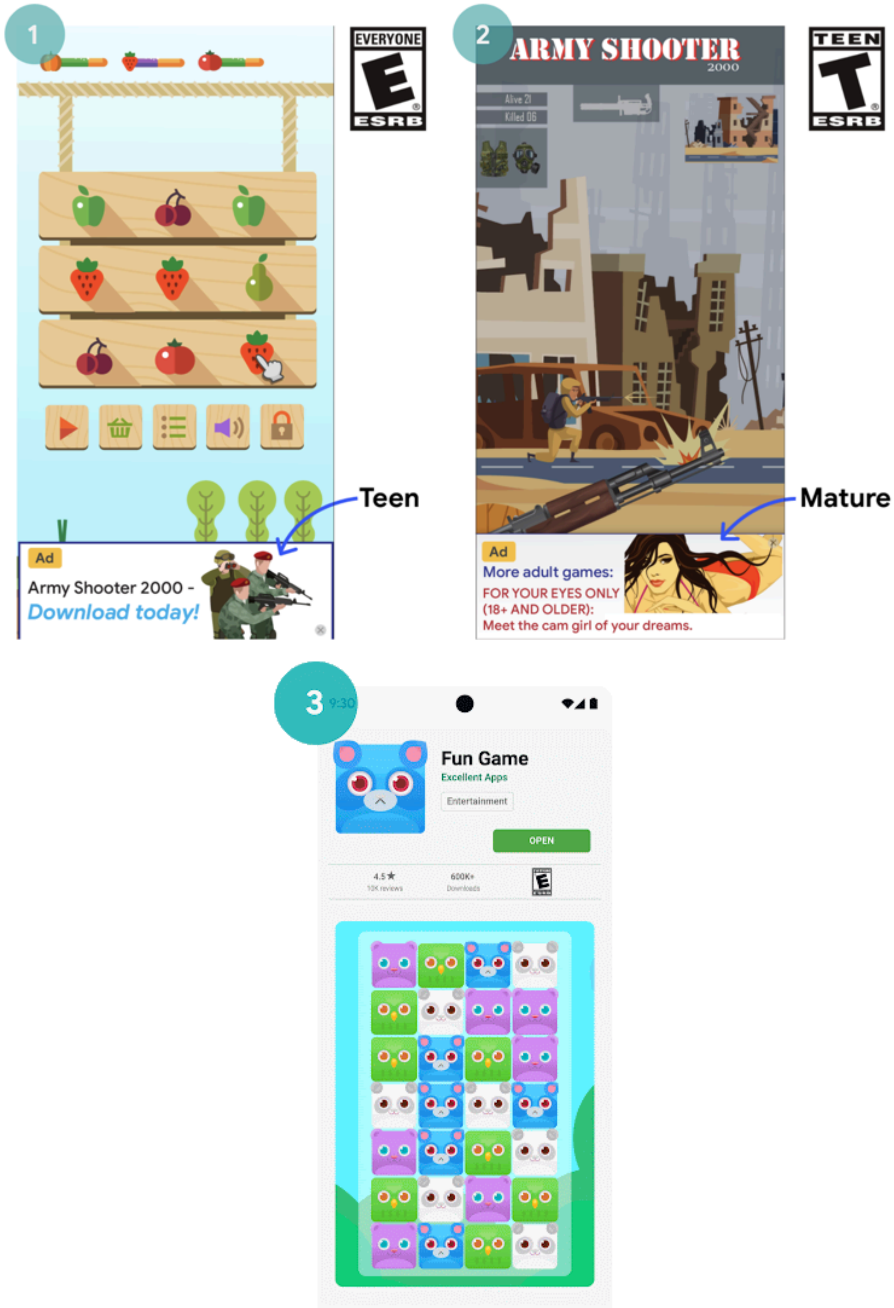
विज्ञापन और उनसे जुड़े ऑफ़र, आपके ऐप्लिकेशन का हिस्सा होते हैं. इसलिए, यह ज़रूरी है कि वे प्रतिबंधित कॉन्टेंट के लिए हमारी नीतियों के मुताबिक हों. अगर आपका ऐप्लिकेशन, जुआ खेलने की सुविधा देने वाला ऐप्लिकेशन है, तो आपको अन्य ज़रूरी शर्तों को भी पूरा करना होगा.

आपत्तिजनक विज्ञापन

आपके ऐप्लिकेशन के अंदर दिखाए जाने वाले विज्ञापन और उनसे जुड़े ऑफ़र (उदाहरण के लिए, विज्ञापन की मदद से अन्य ऐप्लिकेशन को डाउनलोड करने का प्रचार किया जाए) को आपके ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए सही होना चाहिए. भले ही, कॉन्टेंट हमारी अन्य पॉलिसी के मुताबिक हो.

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

- ऐसे विज्ञापन जो ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए सही नहीं हैं



① यह विज्ञापन (किशोर के लिए), ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए सही नहीं है (हर किसी के लिए)
② यह विज्ञापन (वयस्क के लिए), ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए सही नहीं है (किशोर के लिए)
③ विज्ञापन का ऑफ़र (वयस्क वाले ऐप्लिकेशन डाउनलोड करने को प्रमोट करता है), उस गेम ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए सही नहीं है जिसमें विज्ञापन दिखाया गया है (हर किसी के लिए)

परिवार नीतियों के मुताबिक विज्ञापन की शर्तें

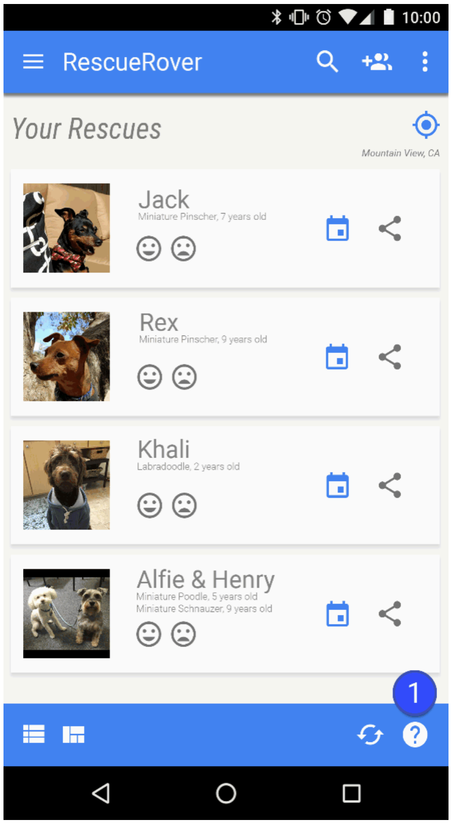
अगर आपको Google Play पर मौजूद किसी ऐसे ऐप्लिकेशन से कमाई करना है जो बच्चों को टारगेट करता है, तो यह ज़रूरी है कि आपका ऐप्लिकेशन परिवार नीतियों के मुताबिक, विज्ञापन और कमाई करने से जुड़ी विज्ञापन की शर्तों के मुताबिक हो.

धोखाधड़ी करने वाले विज्ञापन

विज्ञापनों को किसी भी ऐप्लिकेशन फ़ीचर के यूज़र इंटरफ़ेस, जैसे किसी ऑपरेटिंग सिस्टम की सूचनाएं या चेतावनियां देने के तरीकों की नकल नहीं करनी चाहिए या उनकी पहचान नहीं चुरानी चाहिए. उपयोगकर्ता को यह साफ़ तौर पर बताया जाना चाहिए कि हर विज्ञापन को कौनसा ऐप्लिकेशन उपलब्ध करा रहा है.

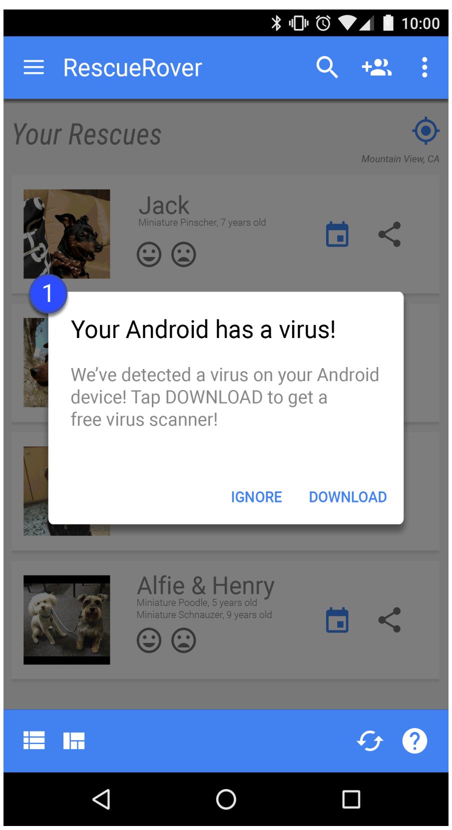
आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण यहां दिए गए हैं:

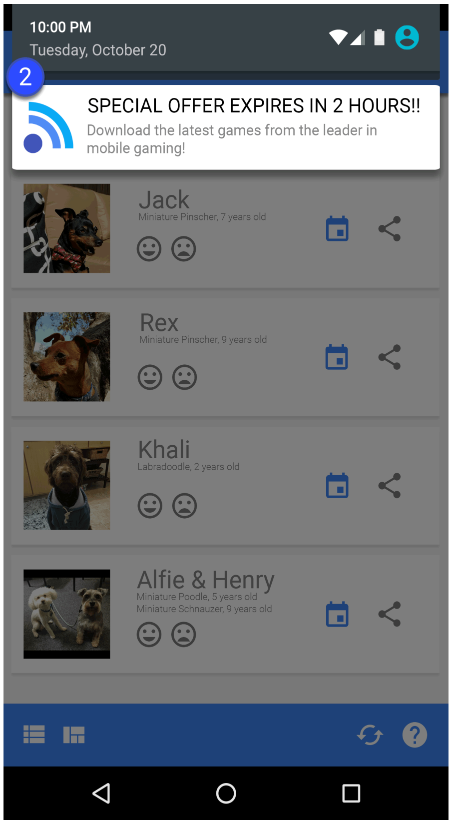
- ऐसे विज्ञापन जो किसी ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) की तरह दिखते हैं:



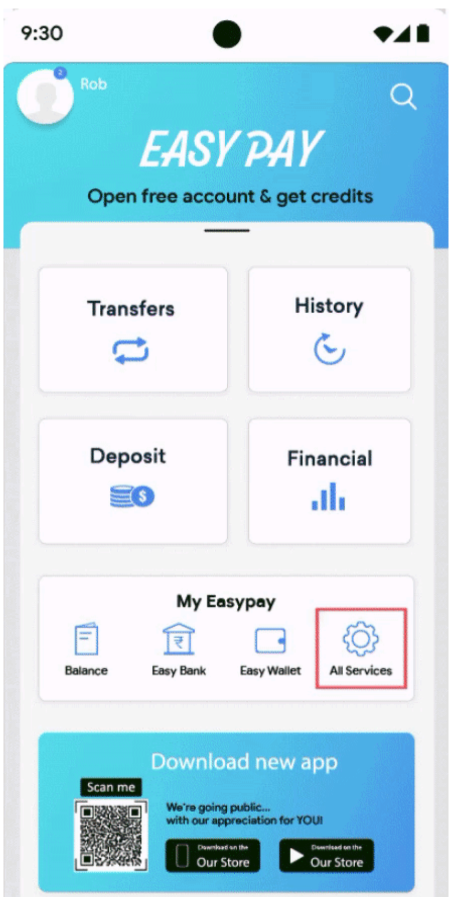
① इस ऐप्लिकेशन में, सवाल के निशान वाला जो आइकॉन दिख रहा है वह एक विज्ञापन है, जो उपयोगकर्ता को किसी बाहरी लैंडिंग पेज पर ले जाता है.

- ऐसे विज्ञापन जो सिस्टम से मिलने वाली सूचनाओं की तरह दिखते हैं:





① ② ऊपर दिए गए उदाहरणों में, कुछ ऐसे विज्ञापन दिए गए हैं जो सिस्टम से मिलने वाली अलग-अलग सूचनाओं जैसे दिखते हैं.



① ऊपर दिए गए उदाहरण में, ऐसे फ़ीचर सेक्शन के बारे में बताया गया है जो किसी अन्य फ़ीचर जैसा दिखता है. हालांकि, यह उपयोगकर्ता को सिर्फ़ किसी विज्ञापन या विज्ञापनों पर ले जाने का काम करता है.

परेशान करने वाले विज्ञापन

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

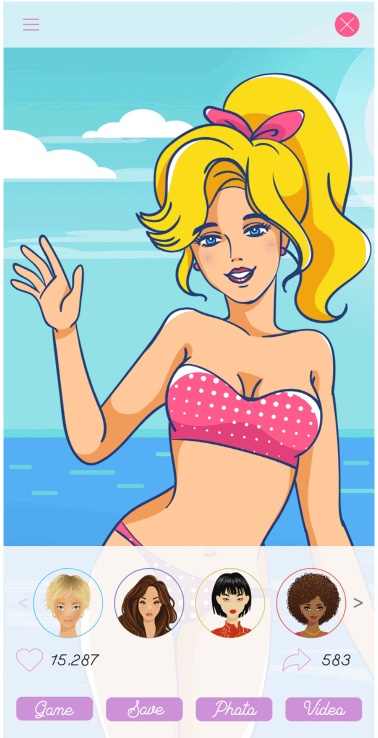
आपका ऐप्लिकेशन, विज्ञापन दिखाने के मकसद से उपयोगकर्ता को तब तक किसी विज्ञापन पर क्लिक करने या अपनी निजी जानकारी देने के लिए मजबूर नहीं कर सकता, जब तक वह ऐप्लिकेशन को पूरी तरह से इस्तेमाल नहीं करता है. साथ ही, विज्ञापन सिर्फ़ उसी ऐप्लिकेशन में दिखाए जा सकते हैं जिसमें वे मौजूद हैं. यह भी ज़रूरी है कि ये विज्ञापन, अन्य विज्ञापनों के दिखने या अन्य ऐप्लिकेशन, सिस्टम समेत डिवाइस या डिवाइस के बटन और पोर्ट के काम करने में रुकावट पैदा न करें. इसमें ओवरले, कंपैनियन फ़ंक्शन, और विजेट के तौर पर बनाई गई विज्ञापन यूनिट शामिल हैं. अगर आपका ऐप्लिकेशन, पेज पर अचानक दिखने वाले विज्ञापन या ऐसे अन्य विज्ञापन दिखाता है जो सामान्य इस्तेमाल में रुकावट डालते हैं, तो उन्हें ऐसा होना चाहिए कि पेनल्टी के बिना आसानी से हटाया जा सके.

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

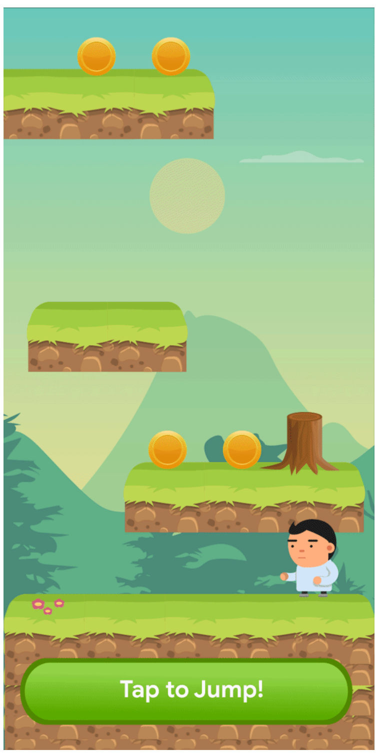
- ऐसे विज्ञापन जो पूरी स्क्रीन को घेर लेते हैं या ऐप्लिकेशन के सामान्य इस्तेमाल में रुकावट डालते हैं. साथ ही, इस तरह के विज्ञापन को हटाने के लिए साफ़ तौर पर कोई तरीका उपलब्ध नहीं कराया जाता:

① इस विज्ञापन को हटाने का कोई बटन नहीं है.

- ऐसे विज्ञापन जिन्हें बंद करने के लिए, गलत बटन पर क्लिक करने के लिए मजबूर किया जाता है या ऐसे विज्ञापन जो उन जगहों पर अचानक दिखते हैं जहां उपयोगकर्ता आम तौर पर अन्य फ़ंक्शन के लिए टैप करता है:

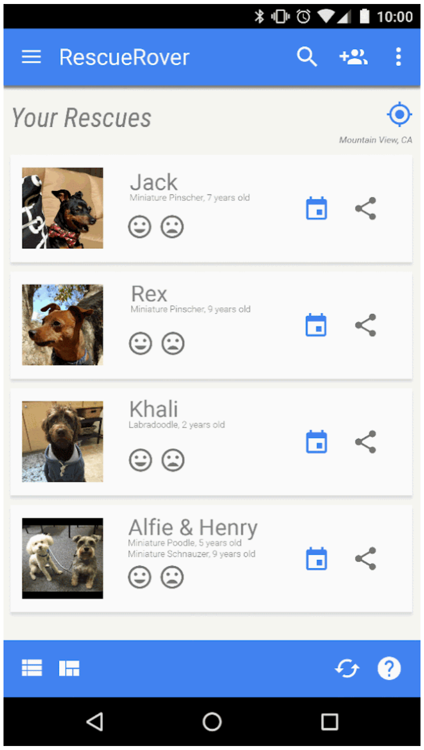


① इस विज्ञापन को हटाने के लिए दिया गया बटन, गुमराह करने वाला है.



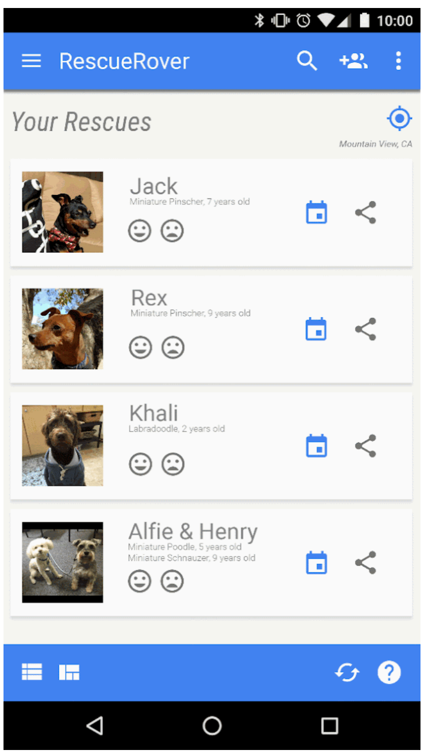
② यह विज्ञापन, अचानक उस जगह पर दिखने लगता है जहां उपयोगकर्ता, ऐप्लिकेशन की सुविधाओं के लिए आम तौर पर टैप करता है.

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



① जब उपयोगकर्ता इस ऐप्लिकेशन से होम स्क्रीन पर जाता है, तो उसे होम स्क्रीन पर अचानक एक विज्ञापन दिखने लगता है.

- ऐसे विज्ञापन जो होम बटन पर टैप करने या ऐप्लिकेशन से बाहर जाने के लिए खास तौर पर बनाई गई सुविधाओं से ट्रिगर होते हैं:



① उपयोगकर्ता, ऐप्लिकेशन से बाहर निकलने और होम स्क्रीन पर जाने की कोशिश करता है. हालांकि, किसी विज्ञापन की वजह से ऐसा करने में रुकावट आ जाती है.

बेहतर विज्ञापन अनुभव

डेवलपर को विज्ञापन से जुड़े नीचे बताए गए दिशा-निर्देशों का पालन करना होगा. इससे, यह पक्का किया जा सकेगा कि Google Play ऐप्लिकेशन का इस्तेमाल करने पर, उपयोगकर्ताओं को बढ़िया अनुभव मिले. ऐसा हो सकता है कि आपके विज्ञापन नीचे बताए गए अनचाहे तरीके से नहीं दिखाए जाएं:

- फ़ुल स्क्रीन पर, अनचाहे तौर पर अचानक दिखने वाले (इंटरस्टीशियल) विज्ञापनों की अनुमति नहीं है. चाहे वे किसी भी फ़ॉर्मैट में हों. जैसे, वीडियो, GIF, स्टैटिक (स्क्रीन पर लगातार दिखने वाले अनचाहे विज्ञापन) वगैरह. ये विज्ञापन उपयोगकर्ताओं को आम तौर पर

तब दिखते हैं, जब वे कुछ और करने की कोशिश कर रहे होते हैं.

- ऐसे विज्ञापनों की अनुमति नहीं है जो कॉन्टेंट वाले किसी हिस्से के शुरू होने या गेम खेलने के दौरान, किसी लेवल की शुरुआत में दिखते हैं.
- फ़ुल स्क्रीन पर, वीडियो के तौर पर अचानक दिखने वाले (इंटरस्टीशियल) ऐसे विज्ञापनों की अनुमति नहीं है जो किसी ऐप्लिकेशन की लोडिंग स्क्रीन (स्प्लैश स्क्रीन) पर दिखते हैं.

- फ़ुल स्क्रीन पर अचानक दिखने वाले (इंटरस्टीशियल) ऐसे विज्ञापनों की अनुमति नहीं है जिन्हें 15 सेकंड के बाद भी बंद नहीं किया जा सकता. भले ही, वे किसी भी फ़ॉर्मैट में हों. फ़ुल स्क्रीन पर अचानक दिखने वाले (इंटरस्टीशियल) ऐसे विज्ञापन 15 सेकंड से ज़्यादा समय तक दिख सकते हैं जिन्हें ऑप्ट-इन किया गया है या फ़ुल स्क्रीन पर अचानक दिखने वाले (इंटरस्टीशियल) ऐसे विज्ञापन भी 15 सेकंड से ज़्यादा समय तक दिख सकते हैं जो उपयोगकर्ताओं की कार्रवाइयों में रुकावट नहीं डालते. उदाहरण के लिए, किसी गेम ऐप्लिकेशन में स्कोर स्क्रीन के बाद.

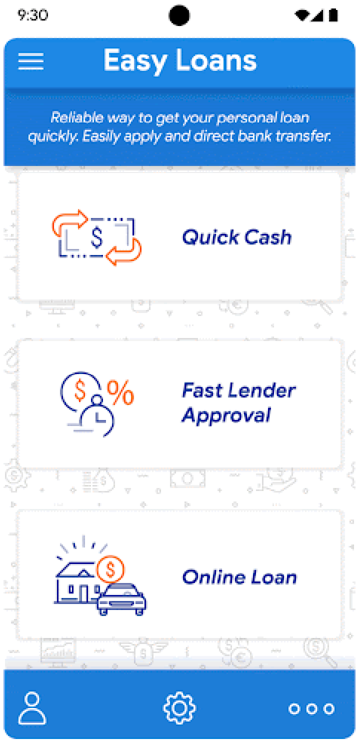
यह नीति इनाम वाले ऐसे विज्ञापनों पर लागू नहीं होती जिन्हें उपयोगकर्ता ऑप्ट-इन करते हैं. उदाहरण के लिए, ऐसा विज्ञापन जिसे कोई डेवलपर, कॉन्टेंट या गेम की किसी सुविधा को अनलॉक करने के बदले उपयोगकर्ता को ऑफ़र करता है. यह नीति ऐसे विज्ञापन और कमाई करने से जुड़े कॉन्टेंट पर भी लागू नहीं होती जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट नहीं डालता. उदाहरण के लिए, विज्ञापन से जुड़ा वीडियो कॉन्टेंट, ऐसे बैनर विज्ञापन जो पूरी स्क्रीन पर नहीं आते.

ये दिशा-निर्देश Better Ads Standards - मोबाइल ऐप्लिकेशन के इस्तेमाल के अनुभव से जुड़े दिशा-निर्देशों पर आधारित हैं. Better Ads Standards के बारे में ज़्यादा जानकारी के लिए, कृपया Coalition of Better Ads पर जाएं.

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

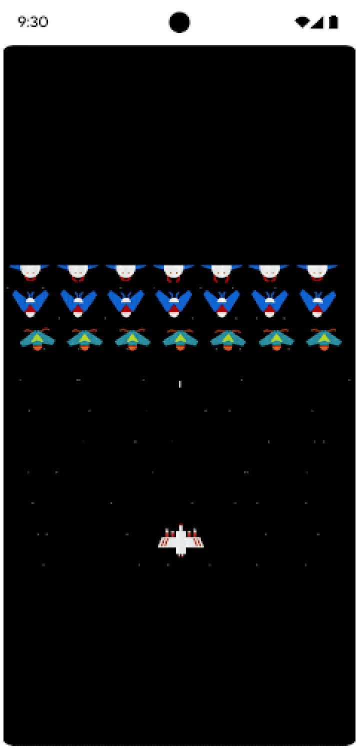
- ऐसे अनचाहे विज्ञापनों की अनुमति नहीं है जो गेम खेलने के दौरान या कॉन्टेंट सेगमेंट के शुरू होने पर दिखते हैं. उदाहरण के लिए, किसी बटन पर उपयोगकर्ता के क्लिक करने के बाद और बटन पर क्लिक करने से होने वाली कार्रवाई से ठीक पहले. ये विज्ञापन उपयोगकर्ताओं के लिए अनचाहे होते हैं, क्योंकि उपयोगकर्ताओं को उम्मीद होती है कि इसकी जगह, कोई गेम या कॉन्टेंट खुलेगा.

① स्क्रीन पर लगातार दिखने वाले अनचाहे विज्ञापन, गेम खेलने के दौरान किसी लेवल की शुरुआत में दिखते हैं.



② अनचाहे वीडियो विज्ञापन, कॉन्टेंट सेगमेंट के शुरू होने पर दिखते हैं.

- फ़ुल स्क्रीन पर आने वाला विज्ञापन गेम खेलने के दौरान दिखता है. इसे, 15 सेकंड के बाद बंद नहीं किया जा सकता है.



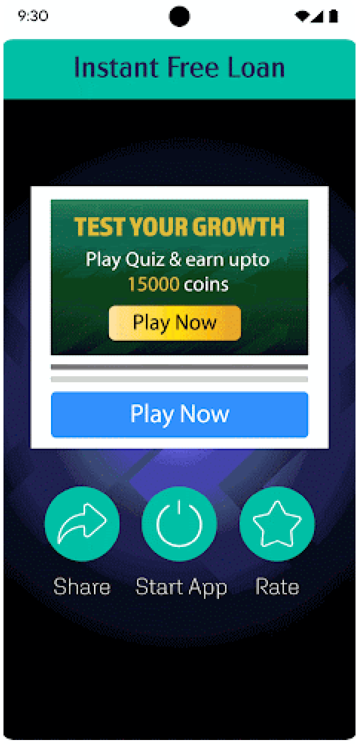
① अचानक दिखने वाले (इंटरस्टीशियल) विज्ञापन, गेम खेलने के दौरान दिखते हैं. इन्हें 15 सेकंड के अंदर बंद करके, आगे बढ़ने का विकल्प नहीं मिलता.

विज्ञापन के लिए बनाए गए ऐप्लिकेशन

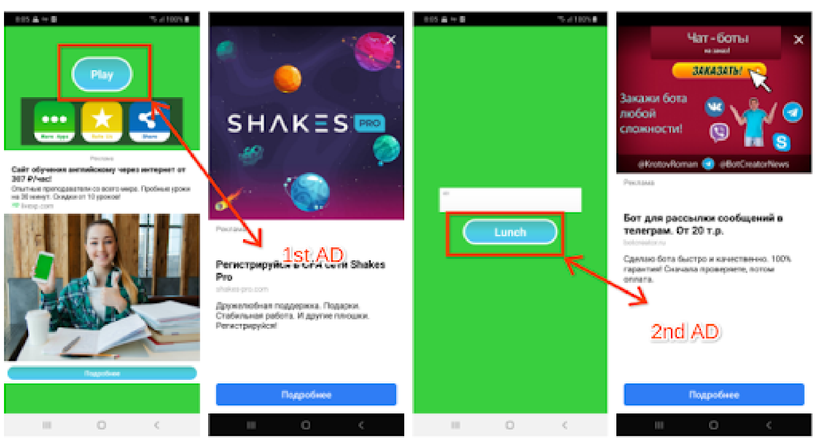
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो उपयोगकर्ताओं का ध्यान खींचने के लिए बार-बार उन्हें अचानक दिखने वाले (इंटरस्टीशियल) विज्ञापन दिखाते हैं. इससे, उपयोगकर्ता को ऐप्लिकेशन से इंटरैक्ट करने और ऐप्लिकेशन के अंदर कोई टास्क पूरा करने में रुकावट होती है.

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

- ऐसे ऐप्लिकेशन जिनमें उपयोगकर्ता की कार्रवाई (इसमें, क्लिक, स्वाइप वगैरह के अलावा, और भी चीज़ें शामिल हो सकती हैं) के बाद, लगातार अचानक दिखने वाला (इंटरस्टीशियल) विज्ञापन आते रहते हैं.



① ऐप्लिकेशन के अंदर मौजूद पहले पेज में इंटरैक्ट करने के लिए कई बटन हों. जब उपयोगकर्ता, ऐप्लिकेशन इस्तेमाल करने के लिए, **ऐप्लिकेशन चालू करें** पर क्लिक करता है, तो अचानक दिखने वाला (इंटरस्टीशियल) विज्ञापन पॉप-अप होता है. विज्ञापन बंद होने के बाद, उपयोगकर्ता ऐप्लिकेशन पर वापस आता है और सेवा का इस्तेमाल शुरू करने के लिए, **सेवा** पर क्लिक करता है, लेकिन अचानक दिखने वाला दूसरा (इंटरस्टीशियल) विज्ञापन नज़र आने लगता है.



② पहले पेज पर, उपयोगकर्ता को **Play** पर क्लिक करने के लिए ले जाया जाता है, क्योंकि ऐप्लिकेशन का इस्तेमाल करने के लिए सिर्फ़ यह बटन उपलब्ध होता है. जब उपयोगकर्ता उस पर क्लिक करता है, तो अचानक दिखने वाला (इंटरस्टीशियल) विज्ञापन नज़र आता है. विज्ञापन बंद होने के बाद, उपयोगकर्ता **Launch** पर क्लिक करता है, क्योंकि ऐप्लिकेशन से इंटरैक्ट करने के लिए सिर्फ़ यह बटन उपलब्ध होता है. फिर, अचानक दिखने वाला (इंटरस्टीशियल) दूसरा विज्ञापन पॉप अप होता है.

लॉकस्क्रीन पर कमाई करने की सुविधा

जब तक कि ऐप्लिकेशन किसी खास मकसद के लिए लॉकस्क्रीन का इस्तेमाल न करे, तब तक ऐप्लिकेशन पर ऐसे विज्ञापन या फ़ीचर को पेश नहीं किया जा सकता जो किसी डिवाइस के लॉक किए गए डिसप्ले पर कमाई करें.

विज्ञापन से होने वाली धोखाधड़ी

विज्ञापन से होने वाली धोखाधड़ी पर पूरी तरह से पाबंदी है. ज़्यादा जानकारी के लिए, विज्ञापनों से होने वाली धोखाधड़ी के ख़िलाफ़ हमारी नीति पर जाएं.

विज्ञापनों के लिए जगह की जानकारी के डेटा का इस्तेमाल

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

- ऐप्लिकेशन के उपयोगकर्ता 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 प्राइवेसी पॉलिसी में दस्तावेज़ के रूप में दर्ज होनी चाहिए. इसके अलावा, इस जानकारी को विज्ञापन नेटवर्क की प्राइवेसी पॉलिसी से भी लिंक किया जाना चाहिए जिसमें जगह की जानकारी के डेटा के इस्तेमाल के बारे में बताया गया हो.
- जगह की जानकारी की अनुमतियों के ऐक्सेस की ज़रूरतों के मुताबिक, जगह की जानकारी की अनुमतियों की मांग सिर्फ़ ऐप्लिकेशन में मौजूदा सुविधाओं और सेवाओं को लागू करने के लिए की जा सकती है, लेकिन सिर्फ़ विज्ञापनों के लिए नहीं की जा सकती.

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 के लिए आइडेंटिफ़ायर का इस्तेमाल, सिर्फ़ विज्ञापन और उपयोगकर्ता के के एनालिटिक्स के लिए किया जाना चाहिए. हर बार आईडी ऐक्सेस करने पर, "पसंद के हिसाब से विज्ञापन दिखाने की सुविधा से ऑप्ट आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन दिखाने की सुविधा से ऑप्ट आउट करने" की सेटिंग की स्थिति की पुष्टि की जानी चाहिए.
- **व्यक्तिगत पहचान से जुड़ी जानकारी या दूसरे आइडेंटिफ़ायर से जुड़ाव**.
  - विज्ञापन का इस्तेमाल: विज्ञापन के लिए आइडेंटिफ़ायर को विज्ञापन के मकसद के लिए डिवाइस के आइडेंटिफ़ायर (उदाहरण के लिए: SSAID, MAC का पता, IMEI वगैरह) से लगातार नहीं जोड़ा जा सकता. विज्ञापन के लिए आइडेंटिफ़ायर को उपयोगकर्ता की साफ़ तौर पर सहमति के बाद ही, व्यक्तिगत पहचान से जुड़ी जानकारी के साथ जोड़ा जा सकता है.
  - आंकड़ों के तौर पर इस्तेमाल करने के लिए: विज्ञापन के लिए आइडेंटिफ़ायर को आंकड़े के तौर पर इस्तेमाल करने के लिए, व्यक्तिगत पहचान से जुड़ी जानकारी या किसी डिवाइस आइडेंटिफ़ायर (उदाहरण के लिए: SSAID, MAC पता, IMEI वगैरह) के साथ लगातार नहीं जोड़ा जा सकता. डिवाइस के स्थायी आइडेंटिफ़ायर से जुड़े अन्य दिशा-निर्देशों के लिए, कृपया उपयोगकर्ता के डेटा से जुड़ी पॉलिसी को पढ़ें.
- **उपयोगकर्ताओं की पसंद का ध्यान रखते हुए**.
  - अगर रीसेट किया जाता है, तो विज्ञापन के नए आइडेंटिफ़ायर को उपयोगकर्ता की साफ़ तौर पर सहमति के बिना, विज्ञापन के किसी पिछले आइडेंटिफ़ायर या विज्ञापन के पिछले आइडेंटिफ़ायर से मिले हुए डेटा से नहीं जोड़ा जाना चाहिए.
  - साथ ही, "पसंद के हिसाब से विज्ञापन दिखाने की सुविधा से ऑप्ट आउट करने" या "दिलचस्पी के मुताबिक विज्ञापन दिखाने की सुविधा से ऑप्ट आउट करने" की सेटिंग के हिसाब से काम करना चाहिए. अगर किसी उपयोगकर्ता ने इस सेटिंग को चालू किया है, तो विज्ञापन के मकसद से उपयोगकर्ता की प्रोफ़ाइलें बनाने या पसंद को ध्यान में रखते हुए विज्ञापन बनाकर उपयोगकर्ताओं को टारगेट करने के लिए, विज्ञापन के लिए आइडेंटिफ़ायर का इस्तेमाल नहीं किया जा सकता. जिन गतिविधियों की अनुमति दी गई है उनमें प्रासंगिक विज्ञापन, फ़्रीक्वेंसी कैपिंग, कन्वर्ज़न ट्रैकिंग, रिपोर्टिंग, और सुरक्षा से जुड़े खतरे और धोखाधड़ी की पहचान करना शामिल है.
  - जब कोई उपयोगकर्ता नए डिवाइसों पर, Android विज्ञापन के लिए आइडेंटिफ़ायर को मिटाता है, तब उस आइडेंटिफ़ायर को हटा दिया जाएगा. अगर आइडेंटिफ़ायर को ऐक्सेस करने की कोशिश की जाती है, तो इसके बजाय कई शून्य दिखेंगे. किसी डिवाइस में विज्ञापन के लिए आइडेंटिफ़ायर न होने पर उसे विज्ञापन के पिछले आइडेंटिफ़ायर से जुड़े या उससे मिले डेटा से नहीं जोड़ा जाना चाहिए.
- **ऐप्लिकेशन इस्तेमाल करने वाले लोगों के लिए साफ़ तौर पर जानकारी देनी चाहिए**. विज्ञापन के लिए आइडेंटिफ़ायर का संग्रह, इसके इस्तेमाल और इन शर्तों को पूरा करने के वादों को कानूनी तौर पर जारी निजता से जुड़ी सूचना से ज़ाहिर किया जाना चाहिए. निजता मानकों के बारे में ज़्यादा जानकारी के लिए, कृपया उपयोगकर्ता के डेटा की पॉलिसी देखें.
- **इस्तेमाल करने की शर्तों को मानना** विज्ञापन के लिए आइडेंटिफ़ायर का इस्तेमाल सिर्फ़ Google Play के डेवलपर कार्यक्रम (Google Play डेवलपर प्रोग्राम) की पॉलिसी के मुताबिक किया जा सकता है. इसके अलावा, इसे कोई ऐसा पक्ष भी इस्तेमाल कर सकता है जिसके साथ कारोबार के हिस्से के तौर पर यह शेयर किया जाए. Google Play पर अपलोड या पब्लिश किए गए सभी ऐप्लिकेशन को विज्ञापन से जुड़े किसी भी मकसद के लिए, डिवाइस के लिए किसी अन्य आइडेंटिफ़ायर के बजाय विज्ञापन आईडी (डिवाइस पर उपलब्ध होने पर) का इस्तेमाल करना होगा.

ज़्यादा जानकारी के लिए, उपयोगकर्ता के डेटा से जुड़ी हमारी नीति पर जाएं.

सदस्यताएं

डेवलपर के तौर पर, अपने ऐप्लिकेशन में दी जाने वाली किसी सदस्यता सेवा या कॉन्टेंट के बारे में, लोगों को गुमराह नहीं करना चाहिए. साथ ही, ऐप्लिकेशन के अंदर किए जाने वाले किसी भी प्रमोशन या स्प्लैश स्क्रीन में ऑफ़र से जुड़ी जानकारी साफ़ तौर पर देना ज़रूरी है. हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जिनमें उपयोगकर्ताओं के साथ खरीदारी में धोखा किया जाता है या उन्हें खरीदारी के लिए गुमराह किया जाता है. इन खरीदारी में सदस्यताएं या इन-ऐप्लिकेशन खरीदारी भी शामिल हैं.

आपको अपने ऑफ़र के बारे में साफ़ तौर पर बताना होगा. इसमें, अपने ऑफ़र की शर्तें, सदस्यता शुल्क, और बिलिंग साइकल के बारे में साफ़ तौर पर जानकारी देना शामिल है. इसके अलावा, आपको यह भी बताना होगा कि ऐप्लिकेशन इस्तेमाल करने के लिए सदस्यता ज़रूरी है या नहीं. लोगों को इस तरह की जानकारी देखने के लिए कोई और कार्रवाई करने की ज़रूरत नहीं होनी चाहिए.

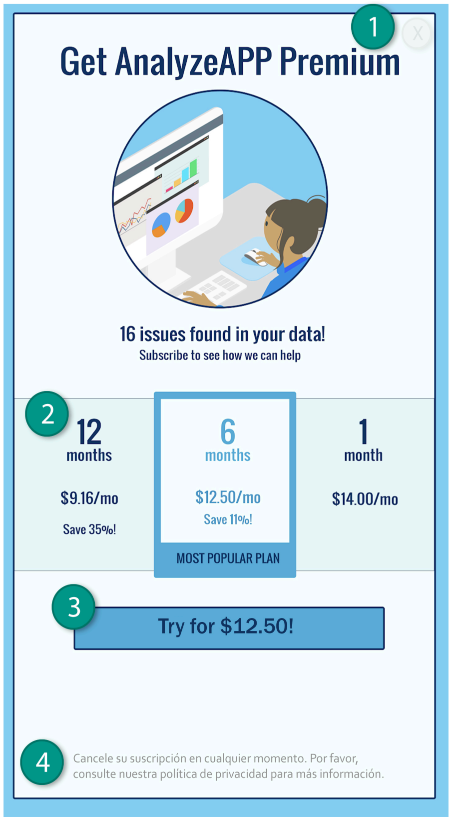
सदस्यताओं के साथ ऑफ़र किए जाने वाले फ़ायदे, सदस्यता चालू रहने के दौरान उपयोगकर्ताओं को लगातार या तय अवधि पर बार-बार देने होंगे. ऐसे फ़ायदे ऑफ़र नहीं किए जाने चाहिए जिनका इस्तेमाल उपयोगकर्ता सिर्फ़ एक बार कर सकते हों. उदाहरण के लिए, ऐसे SKUs जिनके साथ ऐप्लिकेशन के अंदर एकमुश्त क्रेडिट/मुद्रा मिलती हो या एक ही बार इस्तेमाल किए जाने वाले ऐसे टूल मिलते हों जिनसे गेम में परफ़ॉर्मेंस बेहतर की जा सकती है. आपकी सदस्यता के साथ, प्रमोशन के लिए दिए जाने वाले बोनस या अन्य फ़ायदे ऑफ़र किए जा सकते हैं. हालांकि, ये उन फ़ायदों से अलग होंगे जो सदस्यता चालू रहने के दौरान, लगातार या तय अवधि पर बार-बार दिए जाते हैं**.** जिन प्रॉडक्ट के साथ लगातार या तय अवधि पर बार-बार मिलने वाले फ़ायदे ऑफ़र नहीं किए जाते उन्हें ऐप्लिकेशन में खरीदने के लिए उपलब्ध प्रॉडक्ट के तौर पर ऑफ़र करना होगा. उन्हें शुल्क लेकर सदस्यता देने वाले प्रॉडक्ट के तौर पर ऑफ़र नहीं किया जा सकता.

उपयोगकर्ताओं को गलत जानकारी देकर या फ़र्ज़ी खूबियां बताकर, एक ही बार इस्तेमाल किए जा सकने वाले फ़ायदों को सदस्यताओं के तौर पर ऑफ़र नहीं किया जा सकता. इसमें उपयोगकर्ता के सदस्यता खरीद लेने के बाद, सदस्यता में बदलाव करके उसे एक ही बार इस्तेमाल किए जा सकने वाले ऑफ़र में बदल देना शामिल है. उदाहरण के लिए, बार-बार मिलने वाले फ़ायदों को रद्द कर देना, रोक देना या उनकी संख्या को कम कर देना.

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

- हर महीने की ऐसी सदस्यताएं जिनके लिए लोगों को यह जानकारी नहीं मिलती कि उनकी सदस्यता अपने-आप रिन्यू हो जाएगी और उसके लिए हर महीने पैसे देने होंगे.
- ऐसी सालाना सदस्यताएं जो अपने शुल्क को, प्रमुखता से हर महीने के खर्च के तौर पर दिखाती हैं.
- सदस्यता शुल्क और शर्तों के बारे में स्थानीय भाषा में पूरी जानकारी नहीं दी गई हो.
- ऐप्लिकेशन के अंदर किए जाने वाले ऐसे प्रमोशन जिनमें साफ़ तौर पर यह नहीं बताया जाता कि कोई उपयोगकर्ता, बिना सदस्यता लिए भी (अगर यह सुविधा उपलब्ध है) कॉन्टेंट ऐक्सेस कर सकता है.
- SKU के ऐसे नाम जिनसे सदस्यता के बारे में सही जानकारी नहीं मिलती. उदाहरण के लिए, "मुफ़्त में आज़माना" या "प्रीमियम सदस्यता आज़माएं-तीन दिनों के लिए मुफ़्त में”. इनका ऐसी सदस्यता के लिए इस्तेमाल करना जिसके लिए अपने-आप बार-बार शुल्क लगता है.
- परचेज़ फ़्लो में एक साथ कई स्क्रीन का दिखना, जिसकी वजह से लोग अनजाने में 'सदस्यता लें' बटन पर क्लिक कर देते हैं.
- ऐसी सदस्यताएं जिनके साथ लगातार या तय अवधि पर बार-बार फ़ायदे नहीं दिए जाते. उदाहरण के लिए, पहले महीने 1000 जेम ऑफ़र किए जाएं. फिर, सदस्यता के बाद के महीनों में इस फ़ायदे को घटाकर 1 जेम कर दिया जाए.
- इस तरह कि शर्त रखना कि एक ही बार इस्तेमाल किया जा सकने वाला कोई फ़ायदा पाने के लिए, उपयोगकर्ता को अपने-आप रिन्यू होने वाली सदस्यता के लिए साइन अप करना होगा. साथ ही, खरीदारी के बाद उपयोगकर्ता के अनुरोध के बिना ही उसकी सदस्यता रद्द कर देना.

उदाहरण 1:



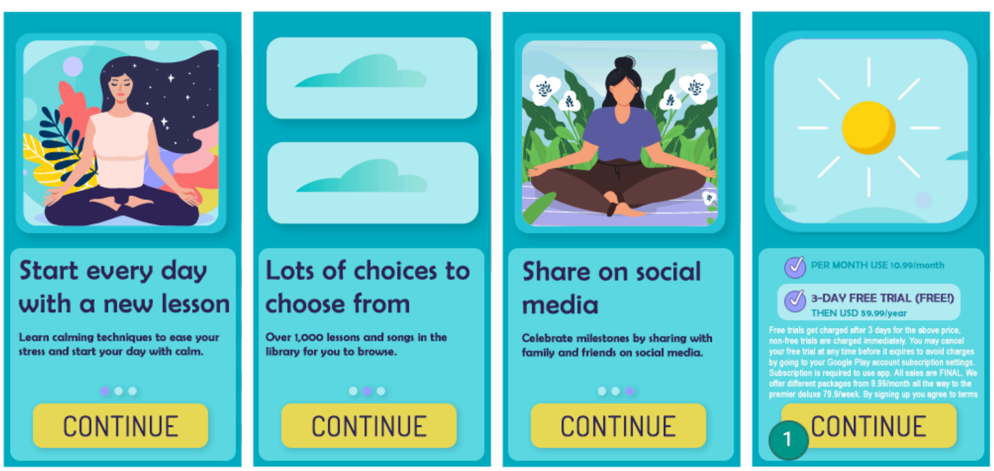
① जब 'खारिज करें' बटन साफ़ तौर पर न दिखे, जिससे लोग यह न समझ पाएं कि वे सदस्यता का ऑफ़र स्वीकार किए बिना भी ऐप्लिकेशन की सुविधाएं ऐक्सेस कर सकते हैं.

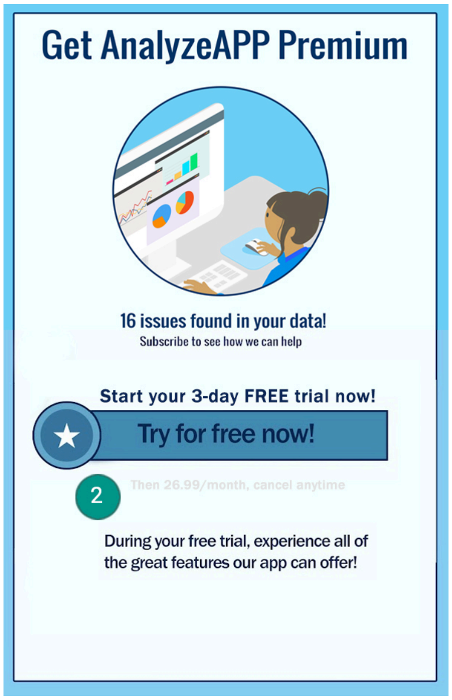
② जब सदस्यता के ऑफ़र में सिर्फ़ महीने का शुल्क दिखे, जिससे लोग यह न समझ पाएं कि सदस्यता लेते समय उनसे छह महीने का शुल्क लिया जाएगा.

③ जब सदस्यता के ऑफ़र में सिर्फ़ उसकी शुरुआती कीमत दिखे, जिससे लोग यह न समझ पाएं कि शुरुआती कीमत की अवधि खत्म होने पर, उनसे अपने-आप कितना सदस्यता शुल्क ले लिया जाएगा.

④ ऑफ़र की जानकारी उसी स्थानीय भाषा में होनी चाहिए जिसमें उसके नियम और शर्तें हैं. इससे उपयोगकर्ताओं को ऑफ़र को पूरी तरह समझने में मदद मिलेगी.

उदाहरण 2:





① एक ही बटन की जगह पर बार-बार क्लिक होने से, अनजाने में उस बटन पर क्लिक हो जाना जो सदस्यता लेने की प्रक्रिया में आखिरी “जारी रखें” बटन होता है और जिस पर क्लिक करने से सदस्यता चालू हो सकती है.

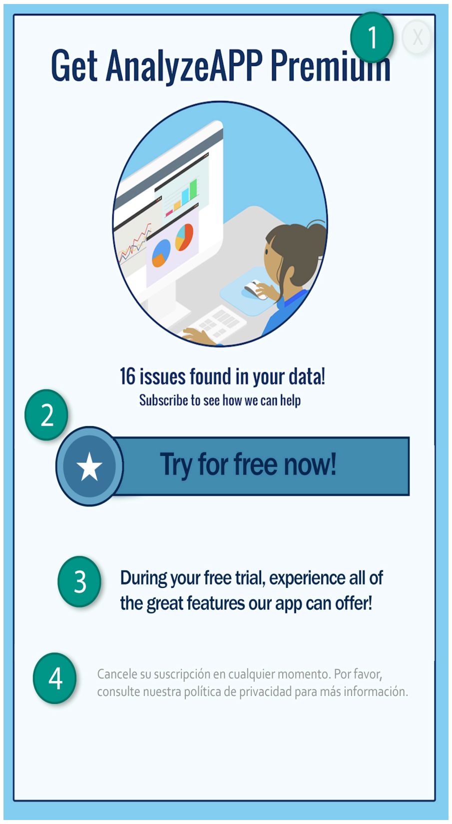
② पढ़कर यह पता लगाना मुश्किल होता है कि मुफ़्त में आज़माने की अवधि खत्म होने पर उपयोगकर्ताओं से कितनी रकम ली जाएगी. इससे, उपयोगकर्ताओं को ऐसा लग सकता है कि प्लान मुफ़्त है

मुफ़्त में आज़माने की अवधि और शुरुआती ऑफ़र

किसी उपयोगकर्ता के आपके ऐप्लिकेशन की सदस्यता के लिए नाम दर्ज कराने से पहले: आपको ऑफ़र से जुड़ी शर्तों के बारे में लोगों को साफ़ तौर पर और सटीक तरीके से बताना चाहिए. इन शर्तों में ऑफ़र की अवधि, कीमत, और कॉन्टेंट या सेवाओं को ऐक्सेस करने की जानकारी शामिल होती 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.

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

- ऐसे ऑफ़र जिनमें साफ़ तौर से यह नहीं बताया जाता है कि मुफ़्त में आज़माने की अवधि या शुरुआती कीमत पर ली गई सदस्यता की अवधि कब खत्म होगी.
- ऐसे ऑफ़र जिनमें साफ़ तौर पर यह नहीं बताया जाता कि ऑफ़र की अवधि खत्म होने पर, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति का नाम उस सदस्यता के लिए अपने-आप दर्ज हो जाएगा जो पैसे देकर ली जाती है.
- ऐसे ऑफ़र जिनमें साफ़ तौर पर यह नहीं बताया जाता कि ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति बिना किसी ट्रायल (उपलब्ध होने पर) के भी कॉन्टेंट ऐक्सेस कर सकता है.
- ऑफ़र की कीमत और वे शर्तें जिन्हें पूरी तरह से स्थानीय भाषा में नहीं बताया गया है.



① जब 'खारिज करें' बटन साफ़ तौर से न दिखे और लोगों को यह समझने में परेशानी हो कि वे मुफ़्त में आज़माने की सुविधा के लिए साइन अप किए बिना भी ऐप्लिकेशन की सुविधाएं ऐक्सेस कर सकते हैं.

② जब ऑफ़र में सदस्यता को मुफ़्त में आज़माने पर ज़ोर दिया जाए और लोगों को यह समझने में परेशानी हो कि मुफ़्त में आज़माने की अवधि खत्म होने पर, उनसे अपने-आप सदस्यता शुल्क ले लिया जाएगा.

③ जब ऑफ़र में सदस्यता को मुफ़्त में आज़माने की अवधि की जानकारी न दी गई हो और लोगों को यह समझने में परेशानी हो कि वे कितने समय के लिए सदस्यता का कॉन्टेंट मुफ़्त में ऐक्सेस कर सकते हैं.

④ ऑफ़र की जानकारी उसी स्थानीय भाषा में होनी चाहिए जिसमें उसके नियम और शर्तें हैं. इससे लोगों को ऑफ़र को पूरी तरह समझने में मदद मिलेगी.

सदस्यताएं मैनेज करना, उन्हें रद्द करना और उनका रिफ़ंड पाना

अगर आपके ऐप्लिकेशन में सदस्यताएं बेची जाती हैं, तो आपको यह पक्का करना होगा कि सदस्यता को मैनेज करने या रद्द करने का तरीका, आपके ऐप्लिकेशन में साफ़ तौर पर ज़ाहिर किया जाए. आपको अपने ऐप्लिकेशन में, सदस्यताएं रद्द करने के लिए ऐसे ऑनलाइन तरीके का ऐक्सेस भी देना चाहिए जिसे आसानी से इस्तेमाल किया जा सके. इस ज़रूरी शर्त को पूरा करने के लिए, अपने ऐप्लिकेशन के खाते की सेटिंग में:

- Google Play के सदस्यता केंद्र का एक लिंक शामिल किया जा सकता है. यह उन ऐप्लिकेशन के लिए है जिनमें Google Play के बिलिंग सिस्टम का इस्तेमाल किया जाता है; और/या
- सदस्यता को रद्द करने की प्रक्रिया को ऐक्सेस करने की सुविधा शामिल की जा सकती है.

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

कॉन्टेंट या ऐक्सेस देने वाले के रूप में अपने उपयोगकर्ताओं के साथ सीधे ऐसी रिफ़ंड नीति लागू की जा सकती है जो ज़्यादा सुविधाजनक हो. 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 के मुताबिक हों.

परिवार के लिए बने कार्यक्रम में शामिल ऐप्लिकेशन में खुद से प्रमाणित किए हुए, विज्ञापन दिखाने के लिए इस्तेमाल होने वाले SDK टूल

अगर आपके ऐप्लिकेशन में विज्ञापन दिखाए जाते हैं और ऐप्लिकेशन की टारगेट ऑडियंस में सिर्फ़ बच्चे शामिल हैं, जैसा कि परिवार नीति में बताया गया है, तो आपको विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल के ऐसे वर्शन ही इस्तेमाल करने होंगे जिन्होंने यह खुद से प्रमाणित किया हो कि वे Google Play की नीतियों के मुताबिक हैं. इनमें नीचे दी गईं, Families Self-Certified Ads SDK Program की ज़रूरी शर्तें भी शामिल हैं.

अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे और वयस्क दोनों शामिल हैं, तो आपको यह पक्का करना होगा कि बच्चों को विज्ञापन दिखाने के लिए, खुद से प्रमाणित किए गए किसी विज्ञापन SDK टूल का ही इस्तेमाल किया जाए. उदाहरण के लिए, न्यूट्रल एज स्क्रीन का तरीका इस्तेमाल करके.

ध्यान दें कि यह पक्का करना आपकी ज़िम्मेदारी है कि आपके ऐप्लिकेशन में इस्तेमाल किए जाने वाले विज्ञापन SDK टूल, लागू होने वाली सभी नीतियों, स्थानीय कानूनों, और नियमों के मुताबिक हों. इनमें, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले खुद से प्रमाणित किए गए SDK टूल भी शामिल हैं. Google न तो इसकी कोई ज़िम्मेदारी लेता है और न ही कोई गारंटी देता है कि खुद से प्रमाणित करने की प्रक्रिया के तहत, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल जो जानकारी देते हैं वह कितनी सही है.

Families Self-Certified Ads SDK Program में शामिल SDK टूल का इस्तेमाल करना सिर्फ़ तब ज़रूरी होता है, जब बच्चों को विज्ञापन दिखाने के लिए SDK टूल इस्तेमाल किए जाते हैं. नीचे बताई गई परिस्थितियों में Google Play पर, विज्ञापन SDK टूल को खुद से प्रमाणित करने की ज़रूरत नहीं होती. हालांकि, इस बात को पक्का करने की ज़िम्मेदारी अब भी आपकी है कि विज्ञापन का कॉन्टेंट और डेटा इकट्ठा करने के तरीके, Play की उपयोगकर्ता के डेटा से जुड़ी नीति और परिवार नीति के मुताबिक हों:

- इन-हाउस विज्ञापन दिखाना. इसमें, SDK टूल इस्तेमाल करके, अपने ऐप्लिकेशन या अपने मालिकाना हक वाले अन्य मीडिया और चीज़ों के, दूसरी जगहों पर किए जा रहे प्रमोशन को मैनेज किया जाता है.
- विज्ञापन देने वालों के साथ सीधे तौर पर डील करना. इसमें SDK टूल इस्तेमाल करके, इन्वेंट्री मैनेज की जाती है.

Families Self-Certified Ads SDK Program की ज़रूरी शर्तें

- तय करें कि किस तरह के विज्ञापन और व्यवहार आपत्तिजनक हैं. उन पर विज्ञापन SDK टूल की शर्तों या नीतियों के मुताबिक पाबंदी लगाएं. परिभाषाएं, Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक हों.
- अपने विज्ञापन क्रिएटिव को रेटिंग देने का एक तरीका बनाएं. यह तरीका उम्र के हिसाब से बने अलग-अलग ग्रुप के मुताबिक हो. इन ग्रुप में, 'सभी के लिए' और 'वयस्क' दोनों तरह के ग्रुप शामिल होने चाहिए. रेटिंग देने का तरीका, Google के उस तरीके के मुताबिक होना चाहिए जो वह SDK टूल को देता है. ऐसा तब होता है, जब डेवलपर पसंद बताने के लिए नीचे दिया गया फ़ॉर्म भरता है.
- पब्लिशर को हर अनुरोध या हर ऐप्लिकेशन के आधार पर, विज्ञापन देने के लिए बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव का अनुरोध करने दें. इस तरह के बर्ताव, लागू कानूनों और नियमों, जैसे कि अमेरिका में लागू बच्चों की ऑनलाइन निजता और संरक्षण नियम (कोपा) और ईयू (यूरोपीय संघ) में लागू सामान्य डेटा से जुड़े सुरक्षा कानून (जीडीपीआर) के मुताबिक होने चाहिए. बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव लागू करने के लिए, Google Play को विज्ञापन SDK टूल की ज़रूरत होती है. इससे वह लोगों के हिसाब से बनाए गए विज्ञापन, रुचि के हिसाब से बनाए गए विज्ञापन, और रीमार्केटिंग को बंद कर पाता है.
- पब्लिशर को ऐसे विज्ञापन फ़ॉर्मैट चुनने की अनुमति दें जो Google Play की परिवारों के लिए विज्ञापन और कमाई करने की नीति के मुताबिक हों और Teacher Approved program की शर्तें पूरी करते हों.
- पक्का करें कि जब रीयल-टाइम बिडिंग की प्रक्रिया का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए किया जाए, तो क्रिएटिव की समीक्षा की जाए. साथ ही, निजता बनाए रखने के संकेत, बिडिंग करने वालों को दिए जाएं.
- इस बात की पुष्टि करने के लिए Google को ज़रूरी जानकारी उपलब्ध कराएं कि विज्ञापन SDK टूल, खुद प्रमाणित करने से जुड़ी सभी ज़रूरी शर्तों के मुताबिक हैं. उदाहरण के लिए, जांच वाला ऐप्लिकेशन और नीचे दिए गए दिलचस्पी दिखाने वाले फ़ॉर्म में बताई गई जानकारी सबमिट करना. साथ ही, बाद में जानकारी के लिए किए जाने वाले अन्य अनुरोधों का समय पर जवाब दें. उदाहरण के लिए, इस बात की पुष्टि के लिए रिलीज़ का नया वर्शन सबमिट करना कि विज्ञापन SDK टूल, खुद प्रमाणित करने से जुड़ी सभी ज़रूरी शर्तों के मुताबिक हैं. साथ ही, जांच वाला ऐप्लिकेशन उपलब्ध कराना.
- खुद से प्रमाणित करें कि सभी नई वर्शन रिलीज़ Google Play के डेवलपर कार्यक्रम की नई नीतियों और परिवार नीति की ज़रूरी शर्तों के मुताबिक भी हों.

ध्यान दें: Families Self-Certified Ads SDK Program में इस्तेमाल होने वाले SDK टूल में ऐसे विज्ञापन देने की सुविधा होनी चाहिए जो उनके पब्लिशर पर लागू होने वाले, बच्चों से जुड़े सभी ज़रूरी कानूनों और नियमों के मुताबिक हों.

वॉटरमार्क वाले विज्ञापन क्रिएटिव और टेस्ट ऐप्लिकेशन सबमिट करने के लिए, ज़्यादा जानकारी यहां पाई जा सकती है.

बच्चों को विज्ञापन दिखाते समय, विज्ञापन दिखाने वाले प्लैटफ़ॉर्म पर लागू होने वाली मीडिएशन की ज़रूरी शर्तें:

- Families Self-Certified Ads SDKs Program या सुरक्षा के ज़रूरी उपाय लागू करें, ताकि यह पक्का किया जा सके कि मीडिएशन से दिखाए जाने वाले सभी विज्ञापन इन शर्तों के मुताबिक हैं; और

- विज्ञापन की रेटिंग और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव के लिए मीडिएशन प्लैटफ़ॉर्म को ज़रूरी जानकारी दें.

डेवलपर, यहां Families Self-Certified Ads SDK Program में इस्तेमाल होने वाले SDK टूल की सूची देख सकते हैं जिन्हें खुद से प्रमाणित करना होता है. साथ ही, वे यह भी देख सकते हैं कि विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले इन SDK टूल का कौनसा वर्शन, परिवार के मुताबिक बनाए गए ऐप्लिकेशन में इस्तेमाल करने के लिए खुद से प्रमाणित किया गया है.

इसके अलावा डेवलपर, दिलचस्पी दिखाने वाला फ़ॉर्म भी उन विज्ञापन SDK टूल के साथ शेयर कर सकते हैं जिन्हें खुद से प्रमाणित करना है.

स्टोर पेज और प्रचार

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

ऐप्लिकेशन का प्रचार

हम उन ऐप्लिकेशन को अनुमति नहीं देते जो सीधे तौर पर या किसी अन्य तरीके से गलत तरह के प्रचार में शामिल होते हैं या उससे फ़ायदा पाते हैं. ये ऐसे प्रचार होते हैं जो लोगों या डेवलपर के साथ धोखाधड़ी करते हैं या उन्हें नुकसान पहुंचाते हैं. विज्ञापनों से भी इस तरह का प्रचार किया जा सकता है. प्रचार के ऐसे तरीकों को धोखाधड़ी करने वाला या नुकसान पहुंचाने वाला माना जाता है जिनका व्यवहार या कॉन्टेंट, डेवलपर कार्यक्रम की नीतियों का उल्लंघन करता है.

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

- वेबसाइट, ऐप्लिकेशन या अन्य प्रॉपर्टी पर, धोखाधड़ी वाले विज्ञापनों का इस्तेमाल करना. इनमें सिस्टम से मिलने वाली सूचनाओं और चेतावनी जैसी सूचनाएं भी शामिल हैं.
- अश्लील विज्ञापनों का इस्तेमाल करके, लोगों को Google Play में अपने ऐप्लिकेशन के स्टोर पेज पर भेजना, ताकि वे ऐप्लिकेशन को डाउनलोड करें.
- ऐप्लिकेशन का प्रमोशन या उन्हें 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.
- एसएमएस सेवाओं का इस्तेमाल करके अनचाहा प्रमोशन करना.
- ऐप्लिकेशन के नाम, आइकॉन या डेवलपर के नाम में ऐसा कोई भी टेक्स्ट या इमेज नहीं होना चाहिए जिससे स्टोर पेज की परफ़ॉर्मेंस या रैंकिंग दिखती हो. इसके अलावा, कीमत या प्रमोशन की जानकारी दिखती हो या फिर किसी मौजूदा Google Play कार्यक्रम से जुड़े सुझाव दिखते हों.

यह पक्का करना आपकी ज़िम्मेदारी है कि आपके ऐप्लिकेशन से जुड़ी विज्ञापन नेटवर्क कंपनियां, सहयोगी कंपनियां या विज्ञापन इन नीतियों का पालन करते हों.

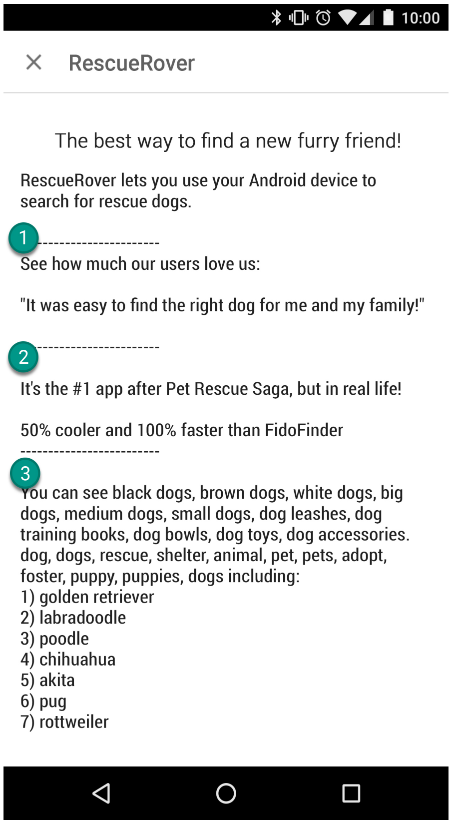
मेटाडेटा

उपयोगकर्ता को आपके ऐप्लिकेशन के मुख्य फ़ंक्शन और मकसद के बारे में, ऐप्लिकेशन के ब्यौरे से जानकारी मिलती है. हम उन ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह करने वाला, गलत तरीके से फ़ॉर्मैट किया गया, बिना किसी जानकारी वाला, ग़ैर-ज़रूरी, ज़रूरत से ज़्यादा या गलत मेटाडेटा होता है. इसमें ऐप्लिकेशन की जानकारी, डेवलपर का नाम, ऐप्लिकेशन का नाम, आइकॉन, स्क्रीनशॉट, और प्रमोशन से जुड़ी इमेज के अलावा, और भी चीज़ें शामिल हो सकती हैं. डेवलपर को अपने ऐप्लिकेशन के बारे में साफ़ तौर पर और सही तरीके से लिखी जानकारी देनी चाहिए. हम ऐप्लिकेशन के बारे में दी गई जानकारी में, उन टेस्टिमोनियल को शामिल करने की अनुमति नहीं देते जिन्हें किसी व्यक्ति ने पहचान छिपाकर लिखा हो या जिन्हें लिखने वाले के बारे में कुछ पता न हो.

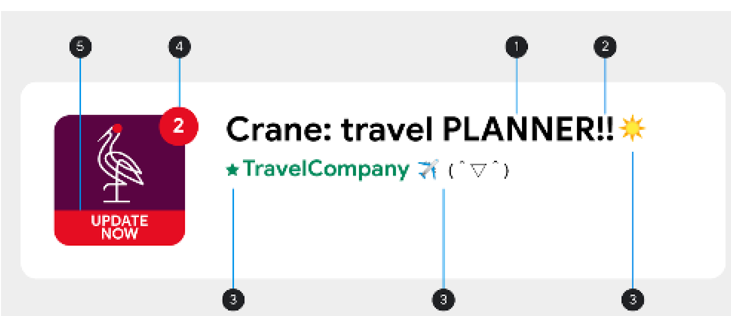
उपयोगकर्ता को ऐप्लिकेशन का टाइटल, आइकॉन, और डेवलपर के नाम से, आपके ऐप्लिकेशन को खोजने और उसके बारे में जानने में मदद मिलती है. इसलिए, इन मेटाडेटा में इमोजी और इमोटिकॉन का इस्तेमाल न करें. इसके अलावा, खास वर्णों का भी बार-बार इस्तेमाल न करें. सिर्फ़ बड़े अक्षर लिखने से बचें. ऐसा तब ही करें, जब आपके ब्रैंड के नाम में शामिल सभी अक्षर बड़े हों. ऐप्लिकेशन आइकॉन में गुमराह करने वाले सिंबल इस्तेमाल करने की अनुमति नहीं है. उदाहरण के लिए, कोई नया मैसेज न होने के बाद भी नए मैसेज होने का संकेत दिखना या ऐप्लिकेशन के डाउनलोडिंग कॉन्टेंट से न जुड़े होने के बावजूद डाउनलोड/इंस्टॉल के सिंबल दिखना. आपके ऐप्लिकेशन का नाम 30 या उससे कम वर्णों का होना चाहिए. ऐप्लिकेशन के नाम, आइकॉन या डेवलपर के नाम में ऐसा कोई भी टेक्स्ट या इमेज का इस्तेमाल न करें जिससे स्टोर पेज की परफ़ॉर्मेंस या रैंकिंग दिखती हो. इसके अलावा, कीमत या प्रमोशन की जानकारी दिखती हो या फिर किसी मौजूदा Google Play कार्यक्रम से जुड़े सुझाव दिखते हों.

यहां बताई गई ज़रूरी शर्तों के अलावा, Google Play की खास डेवलपर नीतियों के लिए आपको मेटाडेटा से जुड़ी ज़्यादा जानकारी देने की ज़रूरत हो सकती है.

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

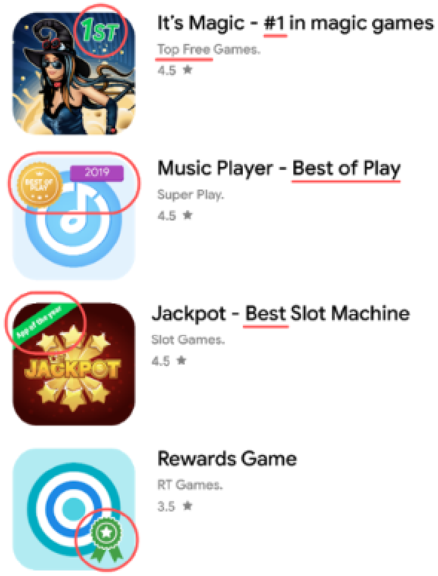


① बिना पहचान के या पहचान छिपाकर दिए गए उपयोगकर्ता टेस्टिमोनियल
② ऐप्लिकेशन या ब्रैंड के डेटा की तुलना
③ वर्ड ब्लॉक और वर्टिकल (ऊपर-नीचे)/हॉरिज़ॉन्टल (दाएं-बाएं) वर्ड लिस्ट

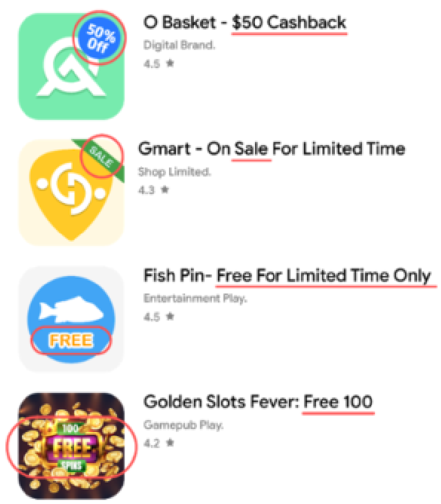


① ब्रैंड के नाम में शामिल न होने के बावजूद, सिर्फ़ बड़े अक्षरों का इस्तेमाल
② खास वर्ण के क्रम, जो ऐप्लिकेशन के लिए किसी काम के नहीं
③ इमोजी, इमोटिकॉन (जैपनीज़ काओमोजी शामिल), और खास वर्णों का इस्तेमाल
④ गुमराह करने वाला सिंबल
⑤ गुमराह करने वाला टेक्स्ट

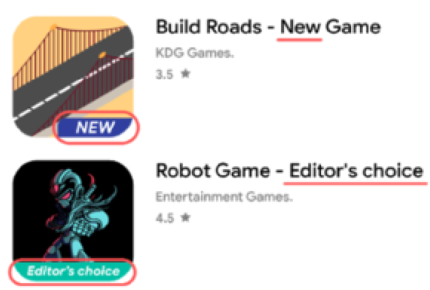
- ऐसी इमेज या टेक्स्ट जिससे स्टोर पेज की परफ़ॉर्मेंस या रैंकिंग के बारे में पता चलता हो. जैसे, 'साल का सबसे अच्छा ऐप्लिकेशन,' '#1,' 'साल 20XX में Google Play का सबसे अच्छा ऐप्लिकेशन,' 'लोकप्रिय,' अवॉर्ड आइकॉन वगैरह.



- ऐसी इमेज या टेक्स्ट जिससे प्रमोशन से जुड़ी जानकारी और कीमत के बारे में पता चलता हो. उदाहरण के लिए, '10% छूट,' '50 डॉलर कैशबैक,' 'सिर्फ़ कुछ समय के लिए मुफ़्त' वगैरह.



- ऐसी इमेज या टेक्स्ट जिससे Google Play programs के बारे में पता चलता हो. उदाहरण के लिए, 'संपादक की पसंद,' 'नया' वगैरह.



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

- ऐसी तस्वीरें या वीडियो जिनमें सेक्शुअल ऐक्ट से जुड़ा कॉन्टेंट शामिल हो. उन अश्लील इमेज से बचें जिनमें स्तन, कूल्हे, जननांग या ऐसा ही कोई दूसरा आकर्षित करने वाला अंग या कॉन्टेंट शामिल हो. भले ही, उसे तस्वीर के तौर पर दिखाया गया हो या असल रूप में.
- ऐप्लिकेशन के स्टोर पेज पर ऐसी भाषा का इस्तेमाल करना जिसमें अपशब्दों का इस्तेमाल हुआ हो, अश्लील हो या आम तौर पर लोगों के लिए सही न हो.
- ऐप्लिकेशन आइकॉन, प्रचार से जुड़ी इमेज या वीडियो में खास तौर पर दिखाया गया दिल दहलाने वाला 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:

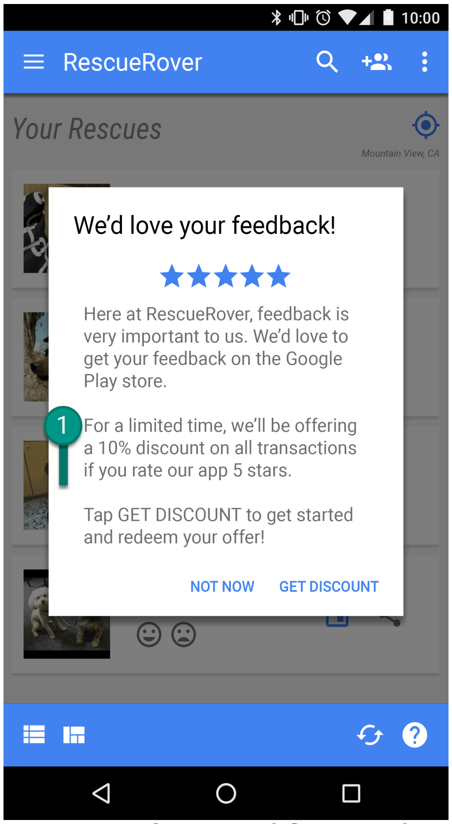
- अपने ऐप्लिकेशन की सबसे अच्छी बातों को हाइलाइट करें. दिलचस्प और मज़ेदार जानकारी शेयर करें, ताकि लोगों को यह पता चल सके कि आपके ऐप्लिकेशन में क्या खास है.
- पक्का करें कि आपके ऐप्लिकेशन का टाइटल और ब्यौरा, ऐप्लिकेशन के फ़ंक्शन के बारे में सही जानकारी देता हो.
- दोहराए जाने वाले या बेवजह के कीवर्ड या रेफ़रंस 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, बहुत ज़्यादा विस्तार से दी गई जानकारी, 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.

उपयोगकर्ता रेटिंग, समीक्षाएं, और इंस्टॉल की संख्या

डेवलपर को Google Play में किसी भी ऐप्लिकेशन के प्लेसमेंट में गलत तरीके से बदलाव करने की कोशिश नहीं करनी चाहिए. इसमें, बढ़ा-चढ़ाकर दी गई प्रॉडक्ट रेटिंग, समीक्षाएं या अमान्य तरीके से इंस्टॉल किए गए ऐप्लिकेशन की संख्या (जैसे कि धोखाधड़ी से या लालच में हुए डाउनलोड, समीक्षाएं, और रेटिंग) शामिल है. इसके अलावा, ऐप्लिकेशन के मुख्य फ़ंक्शन के तौर पर, उपयोगकर्ताओं को किसी तरह का फ़ायदा देकर अन्य ऐप्लिकेशन इंस्टॉल करने का बढ़ावा देना भी शामिल है. साथ ही, इसमें और भी बातें शामिल हो सकती हैं.

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

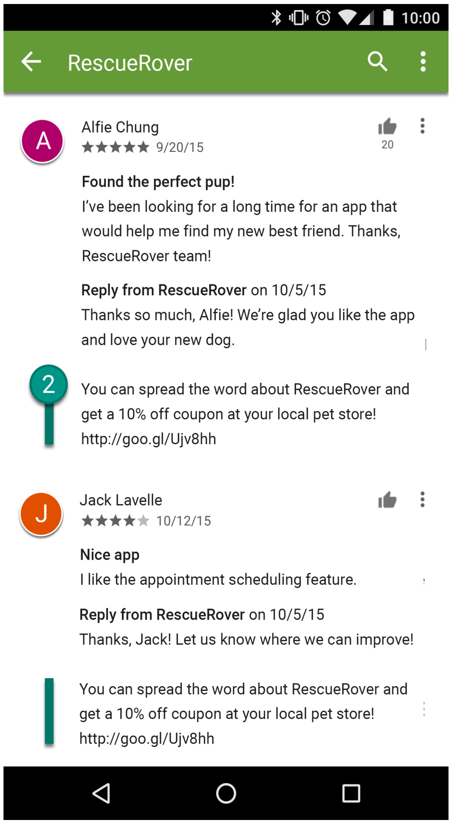
- कुछ फ़ायदा पहुंचाते हुए, लोगों से अपने ऐप्लिकेशन को रेटिंग देने के लिए कहना:



① इस सूचना में बताया गया है कि अगर उपयोगकर्ता ऐप्लिकेशन को पूरी यानी कि फ़ाइव स्टार रेटिंग देते हैं, तो उन्हें बदले में छूट दी जाएगी.

- Google Play पर ऐप्लिकेशन के प्लेसमेंट में बदलाव करने के लिए, उपयोगकर्ताओं के तौर पर बार-बार रेटिंग सबमिट करना.

- आपत्तिजनक कॉन्टेंट वाली समीक्षाएं सबमिट करना या उपयोगकर्ताओं को ऐसी समीक्षाएं सबमिट करने के लिए बढ़ावा देना. आपत्तिजनक कॉन्टेंट में सहयोगी (अफ़िलिएट) कंपनियों के नाम, कूपन, गेम के कोड, ईमेल पते, और वेबसाइट या अन्य ऐप्लिकेशन के लिंक शामिल होते हैं:



② यह समीक्षा, उपयोगकर्ताओं को एक कूपन का ऑफ़र देकर, RescueRover ऐप्लिकेशन का प्रमोशन करने के लिए बढ़ावा देती है.

रेटिंग और समीक्षाएं, ऐप्लिकेशन की क्वालिटी के मानदंड हैं. ऐप्लिकेशन कितना भरोसेमंद है और कितने काम का है, यह जानने के लिए उपयोगकर्ता रेटिंग और समीक्षाओं की मदद लेते हैं. उपयोगकर्ताओं की समीक्षाओं के जवाब देने के लिए, यहां सबसे सही तरीके बताए गए हैं:

- अपने जवाब में, उपयोगकर्ता की टिप्पणियों में बताई गई समस्याओं को हल करने पर ध्यान दें, न कि ज़्यादा रेटिंग की मांग करें.

- अपने जवाब में, अक्सर पूछे जाने वाले सवालों के पेज या सहायता उपलब्ध कराने के लिए ईमेल पते जैसे मददगार संसाधनों को शामिल करें.

कॉन्टेंट रेटिंग

Google Play पर कॉन्टेंट रेटिंग देने का काम इंटरनैशनल एज रेटिंग कोअलिशन (आईएआरसी) करता है. ये रेटिंग इस तरह दी जाती हैं कि डेवलपर को ऐप्लिकेशन इस्तेमाल करने वाले लोगों तक, उनकी जगह के हिसाब से रेटिंग पहुंचाने में मदद मिलती है. क्षेत्रीय आईएआरसी एजेंसी उन दिशा-निर्देशों को बनाए रखती हैं जिनसे यह तय होता है कि ऐप्लिकेशन का कॉन्टेंट किस उम्र के हिसाब से सही है. हम Google Play पर बिना कॉन्टेंट रेटिंग वाले ऐप्लिकेशन की अनुमति नहीं देते.

कॉन्टेंट रेटिंग का इस्तेमाल कैसे किया जाता है

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

कॉन्टेंट रेटिंग किस तरह दी जाती हैं

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

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

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

रेटिंग देने वाली अलग-अलग एजेंसी के बारे में ज़्यादा जानने और कॉन्टेंट रेटिंग से जुड़े सवालों की सूची में मौजूद सभी सवालों के जवाब देने का तरीका जानने के लिए, सहायता केंद्र पर जाएं.

रेटिंग से जुड़ी अपील

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

समाचार

किसी ऐप्लिकेशन को समाचार ऐप्लिकेशन तब माना जाता है, जब:

- उसके बारे में Google Play Console में यह एलान किया जाता है कि वह "समाचार" ऐप्लिकेशन है
- उसे Google Play Store पर मौजूद “समाचार और पत्रिका” कैटगरी में शामिल किया जाता है. साथ ही, ऐप्लिकेशन के नाम, आइकॉन, डेवलपर के नाम या ब्यौरे में उसे “समाचार” ऐप्लिकेशन बताया जाता है.

“समाचार और पत्रिका” कैटगरी में शामिल, ऐसे ऐप्लिकेशन के उदाहरण जो समाचार ऐप्लिकेशन की शर्तों के मुताबिक होते हैं:

- ऐसे ऐप्लिकेशन जिनके ब्यौरों में यह बताया जाता है कि वे “समाचार” ऐप्लिकेशन हैं. इसमें नीचे बताई गई चीज़ों से जुड़े ऐप्लिकेशन के अलावा, और भी ऐप्लिकेशन शामिल हो सकते हैं:
  - हाल की खबरें
  - अखबार
  - ताज़ा खबर
  - स्थानीय खबरें
  - रोज़ की खबरें
- ऐसे ऐप्लिकेशन जिनके नाम, आइकॉन या डेवलपर के नाम में “समाचार” शब्द का इस्तेमाल किया गया हो.

हालांकि, जिन ऐप्लिकेशन में मुख्य तौर पर यूज़र जनरेटेड कॉन्टेंट होता है (जैसे कि सोशल मीडिया ऐप्लिकेशन) उन्हें समाचार ऐप्लिकेशन के तौर पर पेश नहीं करना चाहिए. ऐसे किसी भी ऐप्लिकेशन को समाचार ऐप्लिकेशन नहीं माना जाएगा.

कुछ समाचार ऐप्लिकेशन इस्तेमाल करने के लिए, उपयोगकर्ता को उनकी सदस्यता खरीदनी पड़ती है. ऐसे ऐप्लिकेशन की सदस्यता खरीदे जाने से पहले, यह ज़रूरी है कि लोगों को उनके अंदर मौजूद कॉन्टेंट की झलक दिखाई जाए.

समाचार ऐप्लिकेशन के लिए ज़रूरी है कि:

- उनमें ऐप्लिकेशन के मालिकाना हक और समाचार वाले लेखों के स्रोत की जानकारी उपलब्ध कराई जाए. इसमें, हर लेख के असली पब्लिशर या लेखक से जुड़ी जानकारी के अलावा, और भी चीज़ें शामिल हो सकती हैं. सभी लेखों के लेखकों की सूची उपलब्ध न कराने की छूट किसी समाचार ऐप्लिकेशन को सिर्फ़ तब होती है, जब वह लेखों का असली पब्लिशर हो. कृपया ध्यान दें कि लेखक या पब्लिशर की जानकारी के तौर पर, सोशल मीडिया खातों के लिंक देना काफ़ी नहीं होता.
- ऐप्लिकेशन के लिए कोई वेबसाइट या ऐप्लिकेशन के अंदर लेबल किया गया कोई ऐसा पेज होना चाहिए जिसमें संपर्क जानकारी दी गई हो और वह आसानी से मिल जाए (उदाहरण के लिए, उसे होम पेज में सबसे नीचे या साइट नेविगेशन बार में लिंक किया गया हो). इसके अलावा, उसमें समाचार पब्लिशर की सही संपर्क जानकारी दी गई हो. इसमें, संपर्क के लिए ईमेल पता या फ़ोन नंबर शामिल होना चाहिए. कृपया ध्यान दें कि लेखक या पब्लिशर की जानकारी के तौर पर, सोशल मीडिया खातों के लिंक देना काफ़ी नहीं होता.

समाचार ऐप्लिकेशन के लिए ज़रूरी है कि:

- उनमें वर्तनी और/या व्याकरण से जुड़ी अहम गड़बड़ियां न हों,
- उनमें सिर्फ़ स्टैटिक कॉन्टेंट (उदाहरण के लिए, तीन महीनों से ज़्यादा पुराना कॉन्टेंट) न हो या
- उनका मुख्य मकसद अफ़िलिएट मार्केटिंग या विज्ञापन से कमाई करना न हो.

कृपया ध्यान दें कि जिन समाचार ऐप्लिकेशन का मुख्य मकसद प्रॉडक्ट और सेवाएं बेचना या विज्ञापन से होने वाली आय जनरेट करना नहीं है वे कमाई करने के लिए, विज्ञापनों और मार्केटिंग के अन्य तरीकों का इस्तेमाल *कर सकते हैं*.

जो समाचार ऐप्लिकेशन, पब्लिशिंग के अलग-अलग स्रोतों से कॉन्टेंट इकट्ठा करते हैं उन्हें ऐप्लिकेशन में पब्लिश 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 के मुताबिक होना चाहिए.

मांगी गई जानकारी देने का सबसे बेहतर तरीका जानने के लिए, कृपया यह लेख पढ़ें .

स्पैम, ऐप्लिकेशन की सुविधाएं, और उपयोगकर्ता अनुभव

ऐप्लिकेशन के ज़रिए लोगों को बेहतर सुविधाओं के साथ-साथ ऐसा कॉन्टेंट दिया जाना चाहिए जिससे उन्हें दिलचस्प अनुभव मिले. ऐसे ऐप्लिकेशन जो क्रैश होते रहते हैं और सही उपयोगकर्ता अनुभव नहीं देते उनका Google Play पर कोई काम नहीं होता. Google Play पर और उपयोगकर्ताओं में स्पैम फैलाने वाले ऐप्लिकेशन भी किसी काम के नहीं माने जाते.

स्पैम

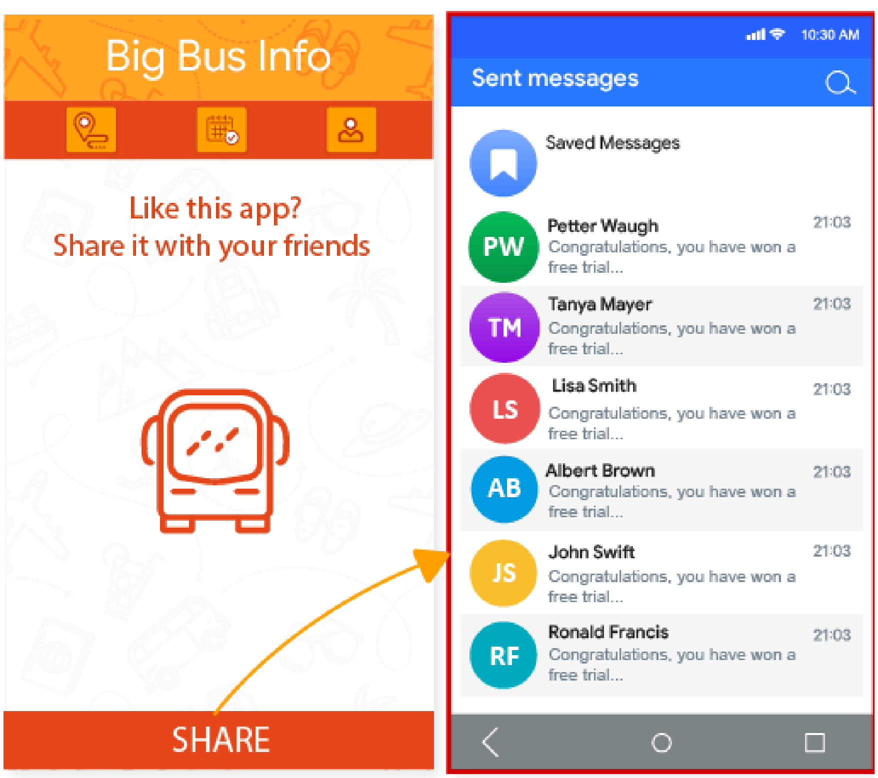
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो ऐप्लिकेशन इस्तेमाल करने वाले लोगों को या Google Play को स्पैम भेजते हैं, जैसे कि वे ऐप्लिकेशन जो लोगों को अनचाहे मैसेज भेजते हैं या ऐसे ऐप्लिकेशन जो बार-बार एक ही चीज़ दिखाते हैं या जिनकी क्वालिटी कम अच्छी होती है.

मैसेज स्पैम

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

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

- जब उपयोगकर्ता 'शेयर करें' बटन दबाता है, तो ऐप्लिकेशन उसकी तरफ़ से मैसेज भेजता है. उपयोगकर्ता को यह सुविधा नहीं दी जाती कि मैसेज भेजे जाने से पहले वह कॉन्टेंट और पाने वाले लोगों के नाम की पुष्टि कर सके:

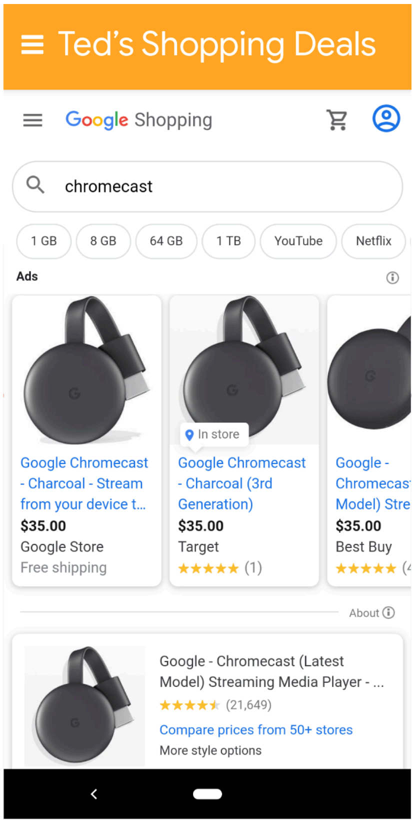


वेबव्यू और उससे जुड़े स्पैम

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

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

- ऐसा ऐप्लिकेशन जिसका मुख्य उद्देश्य रेफ़रल ट्रैफ़िक को किसी वेबसाइट पर भेजना होता है, ताकि वह उस वेबसाइट पर उपयोगकर्ता 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:



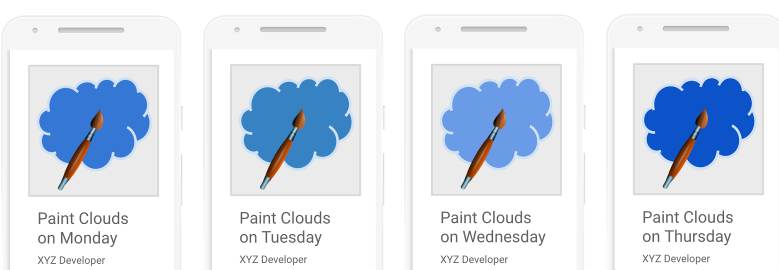
① इस ऐप्लिकेशन को "Ted's shopping Deals" कहा जाता है और यह सामान्य तौर पर Google Shopping का वेबव्यू दिखाता है.

बार-बार एक ही तरह के कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो Google Play पर पहले से मौजूद दूसरे ऐप्लिकेशन के जैसा ही अनुभव देते हों. ऐप्लिकेशन ऐसे होने चाहिए जो सबसे अलग कॉन्टेंट या सेवाएं देकर लोगों के लिए फ़ायदेमंद साबित हों.

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

- कोई मूल कॉन्टेंट या उसमें कुछ नया जोड़े बिना दूसरे ऐप्लिकेशन से कॉन्टेंट कॉपी करना.
- इसके अलावा, ऐसे कई सारे ऐप्लिकेशन बनाना जिनका काम करने का तरीका, कॉन्टेंट, और ऐप्लिकेशन को इस्तेमाल करने का अनुभव बहुत ही मिलता-जुलता हो. अगर इनमें से हर ऐप्लिकेशन पर कम कॉन्टेंट है, तो डेवलपर को सभी कॉन्टेंट के लिए एक ही ऐप्लिकेशन बनाना चाहिए.



ऐप्लिकेशन की सुविधाएं, कॉन्टेंट, और उपयोगकर्ता अनुभव

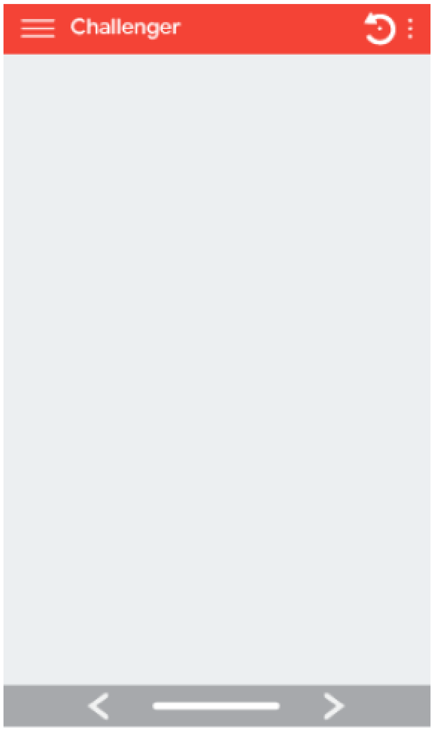
यह ज़रूरी है कि ऐप्लिकेशन, उपयोगकर्ता को भरोसेमंद, रिस्पॉन्सिव, और दिलचस्प अनुभव देते हों. Google Play पर ऐसे ऐप्लिकेशन को अनुमति नहीं दी जाती जो क्रैश हो जाते हैं और जिनमें मोबाइल ऐप्लिकेशन से जुड़ी बुनियादी सुविधाएं और दिलचस्प कॉन्टेंट मौजूद नहीं है. इसके अलावा, उन ऐप्लिकेशन को अनुमति नहीं दी जाती है जिन्हें इस्तेमाल करने पर उपयोगकर्ता को दिलचस्प और अच्छा अनुभव नहीं मिलता.

सीमित सुविधाएं और कॉन्टेंट

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें तय मानकों से कम सुविधाएं और कॉन्टेंट मौजूद होता है.

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

- ऐसे ऐप्लिकेशन जिनमें उपयोगकर्ताओं के कार्रवाई करने के लिए कोई खास सुविधाएं उपलब्ध नहीं होती हैं. जैसे, सिर्फ़ टेक्स्ट या PDF फ़ाइल वाले ऐप्लिकेशन
- ऐसे ऐप्लिकेशन जिनमें बहुत कम कॉन्टेंट उपलब्ध होता है और जो उपयोगकर्ता को दिलचस्प अनुभव नहीं देते हैं. जैसे, सिर्फ़ एक वॉलपेपर की सुविधा देने वाले ऐप्लिकेशन
- ऐसे ऐप्लिकेशन जिन्हें बेवजह बनाया गया है या जिनमें कोई सुविधा नहीं है



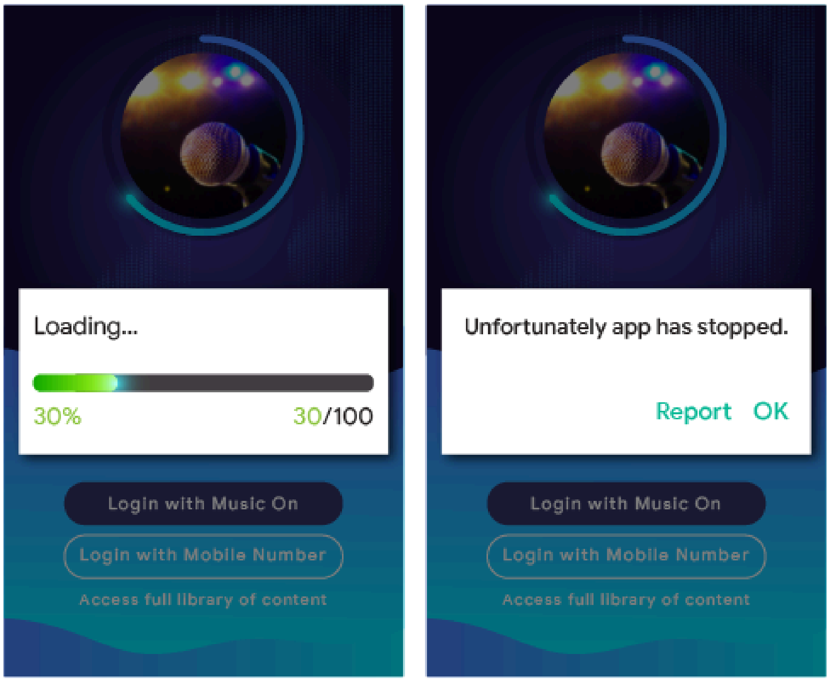
अधूरी सुविधाएं

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो क्रैश हो जाते हैं, ज़बरदस्ती बंद हो जाते हैं, फ़्रीज़ हो जाते हैं या फिर असामान्य तरह से काम करते हैं.

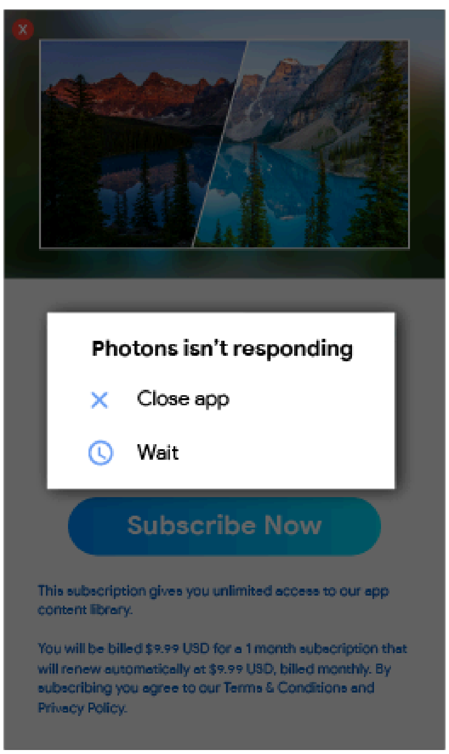
आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण यहां दिए गए हैं:

- 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**



अन्य कार्यक्रम

Android से जुड़े दूसरे अनुभव देने के लिए बनाए गए और Google Play पर सभी लोगों को उपलब्ध कराए गए ऐप्लिकेशन पर, इस नीति केंद्र में कहीं भी दी गई सामग्री नीतियां लागू होती हैं. इनके अलावा, उन पर किसी कार्यक्रम के लिए खास तौर पर बनाई गई नीति से

जुड़ी ज़रूरी शर्तें भी लागू हो सकती हैं. नीचे दी गई सूची को देखकर यह पक्का करें कि इनमें से कोई नीति आपके ऐप्लिकेशन पर लागू होती है या नहीं.

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

पहचान

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

लिंक देकर मदद करना

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

तकनीकी जानकारी

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

ऐप्लिकेशन इंस्टॉल करने की सुविधा का ऑफ़र देना

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

- मटीरियल डिज़ाइन वाला "ऐप्लिकेशन डाउनलोड करें" आइकॉन और इंस्टॉल करने वाले बटन के लिए, "इंस्टॉल करें" लेबल इस्तेमाल करना चाहिए.
- अपने झटपट ऐप्लिकेशन में, किसी ऐप्लिकेशन को इंस्टॉल करने के दो या तीन से ज़्यादा अनुरोध शामिल नहीं करने चाहिए.
- 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, उपयोगकर्ता को बेहतर अनुभव देने के सबसे सही तरीके पर जा कर देखे जा सकते हैं.

डिवाइस में बदलाव करने की स्थिति

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

ऐप्लिकेशन कैसा दिखेगा

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

डिवाइस पहचानकर्ता

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

डिवाइस पहचानकर्ता भी शामिल हो सकते हैं:

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

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

नेटवर्क ट्रैफ़िक

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

Android के लिए इमोजी नीति

हमारी इमोजी नीति को ऐसे तैयार किया गया है जिससे कि इन्हें, हर कोई एक ही तरीके से इस्तेमाल कर सके. इस लक्ष्य को पूरा करने के लिए, सभी ऐप्लिकेशन के लिए यह ज़रूरी है कि जब उन्हें Android 12 के बाद के वर्शन पर चलाया जाए, तो वे यूनिकोड की अनुमति वाले इमोजी के नए वर्शन के मुताबिक काम करें.

कुछ ऐप्लिकेशन जब Android 12 के बाद के वर्शन पर चलते हैं, तो उनमें यूनिकोड की अनुमति वाले इमोजी के नए वर्शन का इस्तेमाल किया जाता है. इनमें, वे ऐप्लिकेशन शामिल हैं जिनमें मनमुताबिक कोई इमोजी लागू किए बिना, Android वाले इमोजी डिफ़ॉल्ट तौर पर इस्तेमाल किए जाते हैं.

यह ज़रूरी है कि जब कुछ ऐप्लिकेशन को Android 12 के बाद के वर्शन पर चलाया जाए, तो वे यूनिकोड की अनुमति वाले इमोजी के नए वर्शन के मुताबिक पूरी तरह काम करें. यूनिकोड की अनुमति वाले नए इमोजी को रिलीज़ होने के चार महीने के अंदर ऐसा करना होगा. इनमें, वे ऐप्लिकेशन शामिल हैं जिनमें मनमुताबिक इमोजी लागू किए गए हैं. इसके अलावा, उन इमोजी को भी लागू किया गया है जिन्हें तीसरे पक्ष की लाइब्रेरी उपलब्ध कराती हैं.

ऐप्लिकेशन को नए इमोजी के मुताबिक बनाने का तरीका सीखने के लिए, इस गाइड की मदद लें.

परिवार

Google Play, डेवलपर के लिए बेहतरीन प्लैटफ़ॉर्म मुहैया कराता है, ताकि वे अपना अच्छी क्वालिटी वाला और उम्र के मुताबिक बनाया गया कॉन्टेंट पूरे परिवार को दिखा सकें. 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, इंटरैक्टिव चेकलिस्ट भी देखें.

Google Play की परिवार से जुड़ी नीतियां

परिवारों की ज़िंदगी बेहतर बनाने के टूल के तौर पर टेक्नोलॉजी का इस्तेमाल बढ़ता जा रहा है. अभिभावक अपने बच्चों से शेयर करने के लिए, सुरक्षित और अच्छी क्वालिटी के कॉन्टेंट खोज रहे हैं. हो सकता है कि खास तौर पर बच्चों के लिए ऐप्लिकेशन बनाए जा 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. अपने कानूनी सलाहकार से पूछा जा सकता है 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.

Google Play परिवार की नीतियों का पालन करने वाले सभी ऐप्लिकेशन, Teacher Approved program के लिए रेट किए जाने की प्रक्रिया में शामिल हो सकते हैं. हालांकि, हम इस बात की गारंटी नहीं दे सकते कि आपका ऐप्लिकेशन Teacher Approved program में शामिल कर ही लिया जाएगा.

Play Console से जुड़ी ज़रूरी शर्तें

टारगेट ऑडियंस और कॉन्टेंट

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

आपको अपने ऐप्लिकेशन की टारगेट ऑडियंस के लिए एक से ज़्यादा उम्र समूह तभी चुनने चाहिए, जब आपने ऐप्लिकेशन को उन चुने हुए उम्र समूह (समूहों) के लोगों को ध्यान में रखकर बनाया हो. साथ ही, आप पक्के तौर पर यह जानते हो कि आपका ऐप्लिकेशन उनके लिए पूरी तरह सही है. उदाहरण के लिए, अगर आपका ऐप्लिकेशन बच्चों, छोटे बच्चों, और प्रीस्कूल में पढ़ने वाले बच्चों के लिए है, तो उम्र समूह टारगेट करते समय "पांच साल और उससे कम" उम्र का समूह ही चुनना चाहिए. अगर आपका ऐप्लिकेशन स्कूल के किसी खास 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 अपडेट कर सकते हैं. Google Play Store पर यह जानकारी दिखाई देने से पहले ऐप्लिकेशन अपडेट ज़रूरी है. हालांकि, आप Google Play Console के इस सेक्शन में जो भी बदलाव करेंगे उनकी समीक्षा ऐप्लिकेशन अपडेट सबमिट किए जाने से पहले भी यह देखने के लिए की जा सकती है कि वे नीति का पालन करते हैं या नहीं.

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

Play Console में गलत तरीके से पेश करना

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

परिवार नीति से जुड़ी ज़रूरी शर्तें

अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो आपको इन शर्तों का पालन करना होगा. इन ज़रूरी शर्तों को पूरा न करने पर, ऐप्लिकेशन को हटाया या निलंबित किया जा सकता है.

1. **ऐप्लिकेशन का कॉन्टेंट:** आपके ऐप्लिकेशन का वह कॉन्टेंट बच्चों की उम्र के हिसाब से सही होना चाहिए जिसे वे ऐक्सेस कर सकते हैं. अगर आपके ऐप्लिकेशन में ऐसा कॉन्टेंट है जिसे पूरी दुनिया में हर जगह सही नहीं माना जाता, लेकिन वह कॉन्टेंट किसी खास देश/इलाके के बच्चों के लिए सही माना जाता है, तो ऐप्लिकेशन को उसी देश/इलाके (सीमित देश/इलाके) में उपलब्ध कराया जा सकता है. हालांकि, वह अन्य देशों/इलाकों में उपलब्ध नहीं रहेगा.
2. **ऐप्लिकेशन की मुख्य सुविधाएं और उनके काम करने का तरीका:** आपके ऐप्लिकेशन में सिर्फ़ किसी वेबसाइट का वेबव्यू नहीं दिखाया जाना चाहिए या ऐप्लिकेशन का मुख्य मकसद, वेबसाइट के मालिक या एडमिन की अनुमति के बिना, अफ़िलिएट मार्केटिंग से आने वाले ट्रैफ़िक को किसी वेबसाइट पर भेजना नहीं होना चाहिए.
3. **Play Console में सवालों के जवाब:** आपको Google Play Console में अपने ऐप्लिकेशन से जुड़े सवालों के सही जवाब देने चाहिए. साथ ही, ऐप्लिकेशन में कोई भी बदलाव होने पर, जवाबों को अपडेट भी कर देना चाहिए. इनमें 'टारगेट ऑडियंस और कॉन्टेंट' सेक्शन, डेटा की सुरक्षा वाले सेक्शन, और कॉन्टेंट रेटिंग के लिए आईएआरसी के सवालों की सूची में, आपके ऐप्लिकेशन के बारे में पूछे गए सवालों के सटीक जवाब भी शामिल हैं. इनके अलावा, इसमें और भी जानकारी हो सकती है.
4. **डेटा इस्तेमाल करने के तरीके:** अगर आपके ऐप्लिकेशन में बच्चों की किसी भी तरह की निजी और संवेदनशील जानकारी को इकट्ठा किया जाता है, तो इस बारे में आपको बताना होगा. इसमें, एपीआई और SDK टूल की मदद से मिलने वाली जानकारी भी शामिल है. यहां उन एपीआई और SDK टूल की बात हो रही है जिन्हें या तो आपके ऐप्लिकेशन में इस्तेमाल किया गया है या जिनकी मदद से आपका ऐप्लिकेशन जानकारी जुटाता है. बच्चों से इकट्ठा की जाने वाली संवेदनशील जानकारी में पहचान की पुष्टि करने की जानकारी, माइक्रोफ़ोन और कैमरा सेंसर का डेटा, डिवाइस का डेटा, Android आईडी, और विज्ञापन से जुड़े डेटा की जानकारी शामिल है. इसके अलावा, इसमें और भी जानकारी शामिल हो सकती है. आपको यह भी पक्का करना होगा कि आपका ऐप्लिकेशन नीचे दिए गए, डेटा इस्तेमाल करने के तरीकों का पालन करता हो:
   - सिर्फ़ बच्चों को टारगेट करने वाले ऐप्लिकेशन को Android विज्ञापन के लिए आइडेंटिफ़ायर (AAID), सिम का सीरियल नंबर, बिल्ड का सीरियल नंबर, BSSID, एमएसी, SSID, IMEI, और/या IMSI को शेयर नहीं करना चाहिए.
     - सिर्फ़ बच्चों के लिए बनाए गए ऐप्लिकेशन को Android एपीआई 33 या उसके बाद के वर्शन को टारगेट करने पर, AD_ID अनुमति के लिए अनुरोध नहीं करना चाहिए.

- बच्चों और बड़ों, दोनों को टारगेट करने वाले ऐप्लिकेशन को बच्चों या उन उपयोगकर्ताओं से मिली जानकारी को शेयर नहीं करना चाहिए जिनकी उम्र के बारे में पता नहीं है. इस जानकारी में, Android विज्ञापन के लिए आइडेंटिफ़ायर (AAID), सिम का सीरियल नंबर, बिल्ड का सीरियल नंबर, BSSID, MAC, SSID, IMEI, और/या IMSI शामिल हैं.
- Android एपीआई के TelephonyManager से, डिवाइस के फ़ोन नंबर के लिए अनुरोध नहीं किया जाना चाहिए.
- सिर्फ़ बच्चों को टारगेट करने वाले ऐप्लिकेशन को न तो जगह की जानकारी का अनुरोध करना चाहिए और न ही जगह की सटीक जानकारी को इकट्ठा, इस्तेमाल, और शेयर करना चाहिए.
- ब्लूटूथ कनेक्शन का अनुरोध करते समय ऐप्लिकेशन को कंपैनियन डिवाइस मैनेजर (सीडीएम) का इस्तेमाल करना ज़रूरी है. हालांकि, अगर आपका ऐप्लिकेशन ऐसे डिवाइस ऑपरेटिंग सिस्टम (ओएस) वर्शन को टारगेट करता है जो सीडीएम के साथ काम नहीं करते, तो ऐसा करना ज़रूरी 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 ऐसे एपीआई या SDK टूल नहीं होने चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल करने की मंज़ूरी न मिली हो.
     - जैसे, पहचान की पुष्टि और अनुमति देने के लिए OAuth टेक्नोलॉजी का इस्तेमाल करने वाली ऐसी एपीआई सेवा जिसकी सेवा की शर्तों में बताया गया है कि इसे, बच्चों के लिए बनी सेवाओं में इस्तेमाल करने की मंज़ूरी नहीं मिली है.
   - बच्चों और बड़ों, दोनों को टारगेट करने वाले ऐप्लिकेशन में ऐसे एपीआई या SDK टूल का इस्तेमाल नहीं किया जाना चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी नहीं मिली है. इनका इस्तेमाल, सिर्फ़ न्यूट्रल एज स्क्रीन के तहत या इस तरह किया जाना चाहिए जिससे कि बच्चों की निजी या संवेदनशील जानकारी को इकट्ठा न किया जा सके. बच्चों और बड़ों, दोनों को टारगेट करने वाले ऐप्लिकेशन में ऐसे एपीआई या SDK टूल से लोगों को कॉन्टेंट ऐक्सेस करने के लिए नहीं कहना चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी न मिली हो.
6. **ऑगमेंटेड रिएलिटी (एआर):** अगर आपके ऐप्लिकेशन में ऑगमेंटेड रिएलिटी (एआर) का इस्तेमाल किया गया है, तो आपको सुरक्षा से जुड़ी चेतावनी शामिल करनी होगी. यह चेतावनी, एआर सेक्शन नज़र आने के तुरंत बाद दिखनी चाहिए. चेतावनी में नीचे दी गई जानकारी शामिल होनी चाहिए:
   - माता-पिता की निगरानी की अहमियत के बारे में सही मैसेज.
   - असली दुनिया के असली खतरों से सजग रहने का रिमाइंडर. उदाहरण के लिए, अपने आस-पास की घटनाओं के बारे में सजग रहना.
   - आपके ऐप्लिकेशन को इस्तेमाल करने लिए ऐसे डिवाइस की ज़रूरत नहीं होनी चाहिए जो बच्चों के इस्तेमाल के लिए सही नहीं है. उदाहरण के लिए, Daydream और Oculus.
7. **सोशल मीडिया ऐप्लिकेशन और उनकी सुविधाएं:** अगर आपके ऐप्लिकेशन में उपयोगकर्ताओं को जानकारी शेयर करने या उसके लेन-देन की अनुमति है, तो आपको Play Console पर मौजूद कॉन्टेंट रेटिंग से जुड़े सवालों की सूची में इसके बारे में ठीक-ठीक जानकारी देनी होगी.
   - सोशल मीडिया ऐप्लिकेशन: सोशल मीडिया ऐप्लिकेशन वह ऐप्लिकेशन होता है जिसमें मुख्य तौर पर, उपयोगकर्ताओं को बिना कॉपीराइट वाला कॉन्टेंट शेयर करने या बड़े पैमाने पर लोगों से बातचीत करने की सुविधा उपलब्ध होती है. बच्चों को अपनी टारगेट ऑडियंस में शामिल करने वाले सभी सोशल मीडिया ऐप्लिकेशन के लिए ज़रूरी है कि उनमें रिमाइंडर की सुविधा उपलब्ध कराई जाए. इस सुविधा की मदद से, बच्चों को बिना कॉपीराइट वाले मीडिया या जानकारी के लेन-देन की अनुमति देने से पहले, यह याद दिलाना होगा कि उन्हें ऑनलाइन रहने के दौरान अपनी सुरक्षा का ध्यान रखना होगा. इसके अलावा, उन्हें इस बात को भी ध्यान में रखना होगा कि ऑनलाइन बातचीत का असल दुनिया में क्या जोखिम हो सकता है. बच्चों को उनकी निजी जानकारी के लेन-देन की सुविधा उपलब्ध कराने से पहले, आपको वयस्क होने की पुष्टि करने की कार्रवाई को ज़रूरी शर्तों में शामिल करना होगा.
   - सोशल मीडिया ऐप्लिकेशन से जुड़ी सुविधाएं: सोशल मीडिया ऐप्लिकेशन से जुड़ी सुविधा, किसी ऐप्लिकेशन की मुख्य सुविधाओं के अलावा, उसमें शामिल की गई ऐसी सुविधाएं होती हैं जिनकी मदद से, उपयोगकर्ता बिना कॉपीराइट वाला कॉन्टेंट शेयर कर सकते हैं या बड़े पैमाने पर लोगों के साथ बातचीत कर सकते हैं. बच्चों को अपनी टारगेट ऑडियंस में शामिल करने वाले ऐसे ऐप्लिकेशन जो सोशल मीडिया वाली सुविधाएं देते हैं उनमें रिमाइंडर की सुविधा उपलब्ध कराना ज़रूरी है. इसकी मदद से, बच्चों को बिना कॉपीराइट वाले मीडिया या जानकारी के लेन-देन की अनुमति देने से पहले, यह याद दिलाना होगा कि उन्हें ऑनलाइन रहने के दौरान अपनी सुरक्षा का ध्यान रखना होगा. इसके अलावा, उन्हें इस बात को भी ध्यान में रखना होगा कि ऑनलाइन बातचीत का असल दुनिया में क्या जोखिम हो सकता है. आपको एक ऐसा तरीका भी उपलब्ध कराना होगा जिसका इस्तेमाल करके वयस्क, बच्चों के लिए दी गई सोशल मीडिया वाली सुविधाओं को मैनेज कर सकें. इसमें, सोशल मीडिया वाली सुविधा को चालू/बंद करना या सुविधा के अलग-अलग लेवल को चुनने के अलावा, और भी चीज़ें शामिल हो सकती हैं. आखिर में, बच्चों को उनकी निजी जानकारी का लेन-देन करने की अनुमति देने वाली सुविधाएं शुरू करने से पहले, आपको वयस्क होने की पुष्टि करने की कार्रवाई को ज़रूरी शर्तों में शामिल करना होगा.
   - वयस्क होने की पुष्टि करने की कार्रवाई, एक ऐसा तरीका है जिसकी मदद से यह पुष्टि की जा सकती है कि उपयोगकर्ता बच्चा नहीं है. इससे, बच्चे अपनी उम्र के बारे में झूठ बोलकर, आपके ऐप्लिकेशन के उन हिस्सों को ऐक्सेस नहीं कर सकेंगे जो वयस्कों के

लिए डिज़ाइन किए गए हैं. इस तरीके में, वयस्क होने की पुष्टि करने से जुड़ा पिन, पासवर्ड, जन्म की तारीख, ईमेल पते की पुष्टि, फ़ोटो आईडी, क्रेडिट कार्ड या SSN जैसी जानकारी शामिल हो सकती है.

- ऐसे सोशल मीडिया ऐप्लिकेशन को बच्चों को टारगेट नहीं करना चाहिए जो खास तौर पर, अनजान लोगों के साथ चैट करने की सुविधा उपलब्ध कराते हैं. उदाहरण के लिए: chat roulette जैसे ऐप्लिकेशन, डेटिंग ऐप्लिकेशन, बच्चों पर फ़ोकस करने वाले ओपन चैट रूम वगैरह.

8. **कानून का पालन:** आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन, अमेरिका में लागू चिल्ड्रंस ऑनलाइन प्राइवसी ऐंड प्रोटेक्शन ऐक्ट (कोपा), ईयू (यूरोपीय संघ) में लागू जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर), और किसी भी अन्य लागू कानून या नियम का पालन करता हो. साथ ही, ऐसे सभी एपीआई या SDK टूल भी इन नियमों का पालन करते हों जिन्हें आपके ऐप्लिकेशन में इस्तेमाल किया गया है या जिनसे आपका ऐप्लिकेशन जानकारी जुटाता है.

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

- ऐसे ऐप्लिकेशन जो अपने स्टोर पेज में प्रमोशन करते हैं कि वे बच्चों के खेलने के लिए 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 डराने-चौंकाने वाला कॉन्टेंट ऐसा कॉन्टेंट शामिल है जो बच्चों के लिए सही नहीं है.
- डेटिंग सेवाएं देने वाले या ऐसे ऐप्लिकेशन जो सेक्शुअल या शादीशुदा ज़िंदगी से जुड़ी सलाह देते हैं.
- ऐसे ऐप्लिकेशन जिनमें उन वेबसाइटों के लिंक होते हैं जो Google Play की डेवलपर कार्यक्रम की नीतियों का उल्लंघन करने वाले कॉन्टेंट उपलब्ध कराते हैं.
- ऐसे ऐप्लिकेशन जो बच्चों को बड़ों के लिए बनाए गए विज्ञापन दिखाते हैं. जैसे- हिंसक कॉन्टेंट, सेक्शुअल कॉन्टेंट, और जुआ खेलने से जुड़ा कॉन्टेंट.

विज्ञापन और कमाई करना

अगर आप किसी ऐसे ऐप्लिकेशन से कमाई करना चाहते हैं जो Google Play पर बच्चों को टारगेट करता है, तो आपके लिए यह अहम है कि आपका ऐप्लिकेशन, परिवार के लिए विज्ञापन और कमाई करने की नीति से जुड़ी नीचे दी गई ज़रूरी शर्तों के मुताबिक हो.

नीचे दी गई नीतियां आपके ऐप्लिकेशन में मौजूद सभी विज्ञापन और कमाई करने से जुड़ा हर तरह का कॉन्टेंट पर लागू होंगी. इसमें विज्ञापन, और जगहों पर प्रमोशन (आपके ऐप्लिकेशन और तीसरे पक्ष के ऐप्लिकेशन के लिए), इन-ऐप्लिकेशन खरीदारी के लिए ऑफ़र या किसी भी तरह का व्यावसायिक कॉन्टेंट शामिल है (जैसे कि पेड प्रॉडक्ट प्लेसमेंट). इन ऐप्लिकेशन में मौजूद सभी विज्ञापन और कमाई करने से जुड़ा हर तरह का कॉन्टेंट, सभी लागू नियमों और कानूनों (इसमें खुद पर लागू किए जाने वाले नियम या उद्योग से जुड़े उचित दिशा-निर्देश शामिल हैं) के मुताबिक होना चाहिए.

Google Play के पास यह अधिकार है कि वह, व्यावसायिक फ़ायदे के लिए बहुत ज़्यादा आक्रामक विज्ञापन दिखाने वाले ऐप्लिकेशन को खारिज कर दे, हटा दे या निलंबित कर दे.

विज्ञापन से जुड़ी शर्तें

अगर आपका ऐप्लिकेशन बच्चों या ऐसे लोगों को विज्ञापन दिखाता है जिनकी उम्र के बारे में पता नहीं है, तो आपको:

- ऐसे उपयोगकर्ताओं को विज्ञापन दिखाने के लिए Google Play के Families self-certified ads SDKs Program में शामिल SDK टूल का इस्तेमाल करना होगा;
- यह पक्का करना होगा कि उन लोगों को दिखने वाले विज्ञापनों में, दिलचस्पी के हिसाब से दिखाए जाने वाले या रीमार्केटिंग करने वाले विज्ञापन शामिल न हों. दिलचस्पी के हिसाब से दिखाए जाने वाले विज्ञापन वे होते हैं जो ऑनलाइन ब्राउज़िंग व्यवहार के हिसाब से लोगों को टारगेट करके दिखाए जाते हैं. वहीं, रीमार्केटिंग करने वाले विज्ञापन, किसी ऐप्लिकेशन या वेबसाइट के साथ पिछले इंटरैक्शन के हिसाब से लोगों को टारगेट करके दिखाए जाते हैं;
- यह पक्का करें कि उन लोगों को दिखाए गए विज्ञापनों का कॉन्टेंट 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 फ़ॉर्मैट की शर्तों के मुताबिक हो; और
- यह भी पक्का करना होगा कि बच्चों को विज्ञापन दिखाने से जुड़े, सभी लागू कानूनों और इंडस्ट्री स्टैंडर्ड का पालन किया जा रहा हो.

विज्ञापन फ़ॉर्मैट की ज़रूरी शर्तें

आपके ऐप्लिकेशन में कमाई करने और विज्ञापन दिखाने के लिए, ऐसे कॉन्टेंट का इस्तेमाल नहीं किया जाना चाहिए जो लोगों को गुमराह करने वाला हो. साथ ही, कॉन्टेंट को इस तरह से डिज़ाइन भी न किया गया हो कि बच्चे (नाबालिग उपयोगकर्ता) उस पर अनजाने में क्लिक कर दें.

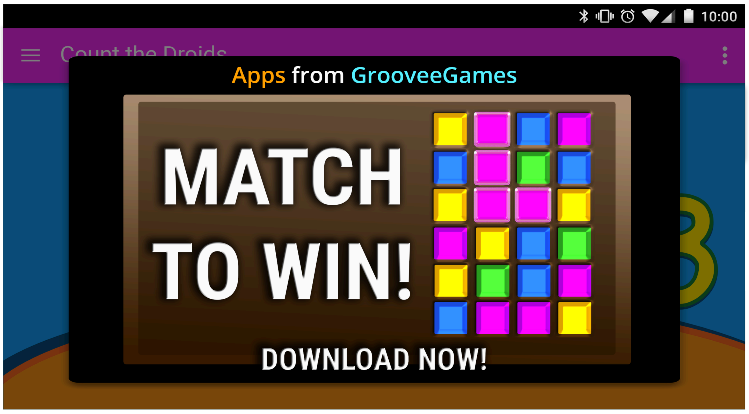
अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस सिर्फ़ बच्चे हैं, तो इन चीज़ों पर पाबंदी है. अगर बच्चे और बड़े, दोनों आपके ऐप्लिकेशन की टारगेट ऑडियंस हैं, तो बच्चों या जिन लोगों की उम्र का पता नहीं है उन्हें विज्ञापन दिखाते समय कुछ चीज़ों और कॉन्टेंट पर पाबंदियां लागू होती हैं. ये पाबंदियां यहां दी गई हैं:

- कमाई करने और विज्ञापन दिखाने के लिए, ऐसे कॉन्टेंट का इस्तेमाल नहीं किया जाना चाहिए जिससे लोगों को परेशानी हो. इनमें, ऐसे विज्ञापन और कमाई करने के लिए दिखाया जाने वाला ऐसा कॉन्टेंट शामिल है जो पूरी स्क्रीन को घेर लेता है या ऐप्लिकेशन के सामान्य इस्तेमाल में रुकावट डालता है. साथ ही, इस तरह के विज्ञापन या कॉन्टेंट को हटाने के लिए साफ़ तौर पर कोई तरीका भी उपलब्ध नहीं कराया जाता. जैसे, विज्ञापन वॉल.
- कमाई करने और विज्ञापन दिखाने के लिए इस्तेमाल किया जाने वाला ऐसा कॉन्टेंट जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट डालता है. इनमें, इनाम वाले या ऑप्ट-इन करने का विकल्प दिखाने वाले ऐसे विज्ञापन भी शामिल हैं जिन्हें पांच सेकंड के बाद भी हटाया नहीं जा सकता.
- कमाई करने और विज्ञापन दिखाने के लिए इस्तेमाल किया जाने वाला ऐसा कॉन्टेंट जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट तो नहीं डालता, लेकिन वह पांच सेकंड से ज़्यादा समय तक दिखता है. जैसे, विज्ञापनों से जुड़ा वीडियो कॉन्टेंट.
- कमाई करने और विज्ञापन दिखाने के लिए इस्तेमाल किया जाने वाला ऐसा कॉन्टेंट जो ऐप्लिकेशन लॉन्च होते ही दिखता है.
- किसी पेज पर कई विज्ञापनों को दिखाया जाना. जैसे, बैनर वाले ऐसे विज्ञापन जिनमें एक प्लेसमेंट में कई विज्ञापन दिखते हैं. इसके अलावा, एक से ज़्यादा बैनर या वीडियो विज्ञापन दिखाने की अनुमति भी नहीं है.
- कमाई करने और विज्ञापन दिखाने के लिए इस्तेमाल किया जाने वाला ऐसा कॉन्टेंट जो आपके ऐप्लिकेशन के कॉन्टेंट से साफ़ तौर पर मिलता-जुलता हो. जैसे, ऑफ़रवॉल और ध्यान खींचने वाले अन्य विज्ञापन.
- विज्ञापन व्यू या इन-ऐप्लिकेशन खरीदारी बढ़ाने के लिए, चौंकाने वाले या भावनात्मक तौर पर गुमराह करने वाले तरीकों का इस्तेमाल करना.
- धोखाधड़ी वाले ऐसे विज्ञापन जिन्हें बंद करने के लिए, गलत बटन पर क्लिक करने के लिए मजबूर किया जाता है या ऐसे विज्ञापन जो उन जगहों पर अचानक दिखते हैं जहां उपयोगकर्ता आम तौर पर अन्य फ़ंक्शन के लिए टैप करता है.
- इन-ऐप्लिकेशन खरीदारी करने के लिए, वर्चुअल गेम के सिक्कों और असली पैसों के बीच फ़र्क़ न दिखाना.

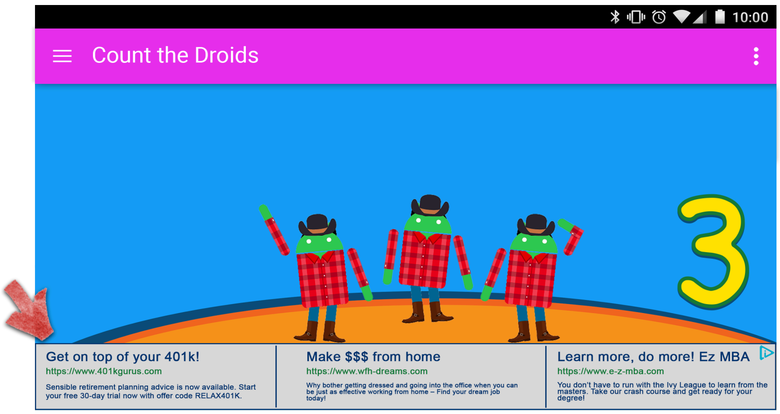
आम तौर पर होने वाले उल्लंघनों के कुछ उदाहरण यहां दिए गए हैं:

- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जिसे बंद करने की कोशिश करते ही, वह उपयोगकर्ता की पहुंच से दूर हो जाता है
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जिसमें किसी ऑफ़र के शुरू होने के पांच (5) सेकंड बाद भी, उपयोगकर्ता को उसे हटाने का तरीका नहीं बताया जाता, जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:

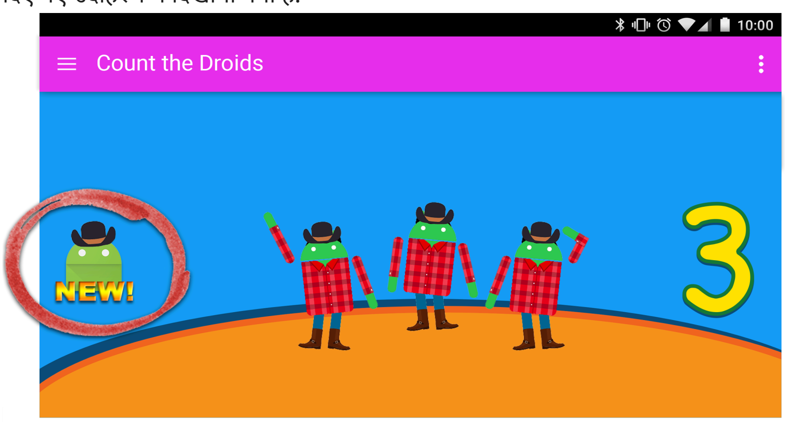
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जो उपयोगकर्ता को विज्ञापन हटाने का तरीका साफ़ तौर पर बताए बिना, डिवाइस की पूरी स्क्रीन या उसके ज़्यादातर हिस्से पर दिखने लगता है, जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



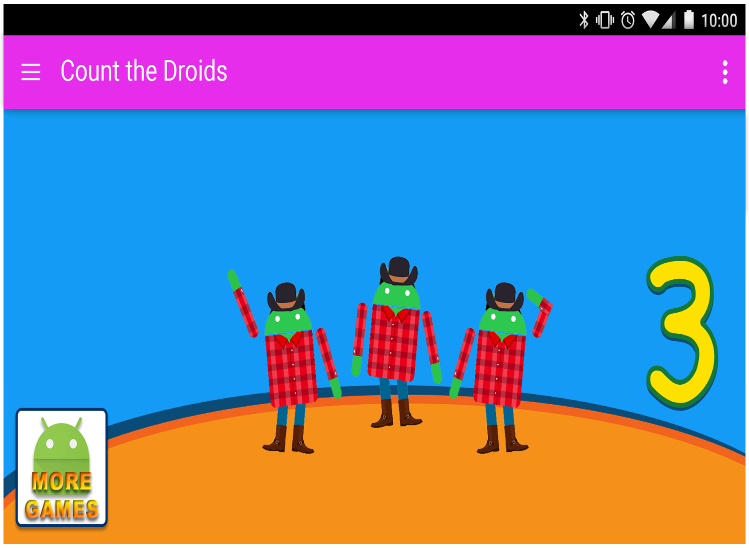
- एक से ज़्यादा ऑफ़र दिखाने वाले बैनर विज्ञापन. जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जिसे उपयोगकर्ता, गलती से ऐप्लिकेशन का कॉन्टेंट समझ सकता है. जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



- ऐसे बटन, विज्ञापन या अन्य कॉन्टेंट जो आपके Google Play store के अन्य पेज का प्रमोशन करता है, लेकिन जिसे देखकर यह पता नहीं चल सकता कि वह आपके ऐप्लिकेशन के कॉन्टेंट से अलग है. इसका उदाहरण नीचे दिखाया गया है:



यहां गलत कॉन्टेंट वाले विज्ञापनों के कुछ उदाहरण दिए गए हैं, जिन्हें बच्चों को नहीं दिखाना चाहिए.

- **आपत्तिजनक मीडिया कॉन्टेंट**: टीवी शो, फ़िल्में, म्यूजिक एल्बम या कोई दूसरे मीडिया आउटलेट के विज्ञापन जो बच्चों के लिए ठीक नहीं हैं.
- **आपत्तिजनक वीडियो गेम और डाउनलोड करने लायक सॉफ़्टवेयर**: डाउनलोड करने लायक सॉफ़्टवेयर और इलेक्ट्रॉनिक वीडियो गेम के विज्ञापन जो बच्चों के लिए सही नहीं हैं.
- **पाबंदी वाली नशीली दवाएं या नुकसान पहुंचाने वाली चीज़ें**: शराब, तंबाकू, पाबंदी वाली नशीली दवाएं या नुकसान पहुंचाने वाली किसी और चीज़ के विज्ञापन.
- **जुआ**: असली में जुआ खेलने जैसा अनुभव देने वाले विज्ञापन, प्रतियोगिता या लॉटरी के प्रचार, भले ही उसमें शामिल होने के लिए कोई शुल्क न मांगा जाए.
- **वयस्क और सेक्शुअल ऐक्ट से जुड़ा कॉन्टेंट**: ऐसे विज्ञापन जिनमें सेक्शुअल, सेक्शुअल ऐक्ट से जुड़ा, और मैच्योर कॉन्टेंट हो.
- **डेटिंग या संबंध**: डेटिंग या वयस्क संबंध वाली वेबसाइट के विज्ञापन.
- **हिंसा से जुड़ा कॉन्टेंट**: ऐसे विज्ञापन जिनमें हिंसा से जुड़ा और दिल दहलाने वाला ऐसा कॉन्टेंट हो जो बच्चों के लिए सही नहीं है.

विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDKs टूल

अगर आपके ऐप्लिकेशन में विज्ञापन दिखाए जाते हैं और आपकी टारगेट ऑडियंस में सिर्फ़ बच्चे शामिल हैं, तो आपको सिर्फ़ Families Self-Certified Ads SDK Program में शामिल SDK टूल के वर्शन इस्तेमाल करने चाहिए. अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में दोनों, बच्चे और वयस्क उपयोगकर्ता शामिल हैं, तो आपको उम्र का पता लगाने वाले तरीके इस्तेमाल करने होंगे. उदाहरण के लिए, न्यूट्रल एज स्क्रीन . साथ ही, यह पक्का करना होगा कि बच्चों को दिखने वाले विज्ञापनों में खास तौर पर, Google Play से खुद प्रमाणित किए गए किसी विज्ञापन SDK टूल वाले वर्शन इस्तेमाल किए जाएं.

इन ज़रूरी शर्तों के बारे में ज़्यादा जानकारी के लिए, कृपया Families Self-Certified Ads SDK Program की नीति पेज पर जाएं. साथ ही, Families Self-Certified Ads SDK Program में शामिल SDK टूल के वर्शन की मौजूदा सूची देखने के लिए, यहां जाएं.

अगर आप AdMob के उपयोगकर्ता हैं, तो उनके प्रॉडक्ट के बारे में ज़्यादा जानने के लिए AdMob के सहायता केंद्र पर जाएं.

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

परिवार के लिए विज्ञापन कार्यक्रम में शामिल, खुद से प्रमाणित किए विज्ञापन दिखाने में इस्तेमाल होने वाले SDK टूल से जुड़ी नीति

Google Play यह ज़िम्मेदारी लेता है कि परिवारों और बच्चों को सुरक्षित अनुभव मिले. इसके तहत, हम यह पक्का करते हैं कि बच्चों को सिर्फ़ ऐसे विज्ञापन दिखें जो उनकी उम्र के हिसाब से सही हों और उनके डेटा का रखरखाव सही तरीके से किया जा रहा हो. हम यह ज़िम्मेदारी पूरी कर सकें, इसके लिए यह ज़रूरी है कि विज्ञापन दिखाने में इस्तेमाल किए जाने वाले SDK टूल और मीडिएशन प्लैटफ़ॉर्म खुद से यह प्रमाणित करें कि वे बच्चों के लिए सही हैं और Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक हैं. साथ ही,

उन्हें यह भी प्रमाणित करना होगा कि वे Google Play की परिवार नीतियों के साथ-साथ Families Self-Certified Ads SDK Program की ज़रूरी शर्तों का भी पालन करते हैं.

Google Play Families Self-Certified Ads SDK Program, डेवलपर के लिए यह पता लगाने का अहम तरीका है कि किन विज्ञापन SDK टूल और मीडिएशन प्लैटफ़ॉर्म ने खुद से प्रमाणित किया है कि वे बच्चों के लिए खास तौर पर बनाए जाने वाले ऐप्लिकेशन के लिए सही हैं.

SDK टूल के बारे में कोई भी जानकारी गलत तरीके से पेश करने की वजह से, आपके SDK टूल को Families Self-Certified Ads SDK Program से निलंबित किया जा सकता है. इसलिए, सही जानकारी देना ज़रूरी है. इसमें आवेदन के समय दिलचस्पी दिखाने वाले फ़ॉर्म में डाली गई जानकारी भी शामिल है.

नीति से जुड़ी ज़रूरी शर्तें

अगर आपके SDK टूल या मीडिएशन प्लैटफ़ॉर्म का इस्तेमाल उन ऐप्लिकेशन में किया जा रहा है जो Google Play Families Program में शामिल हैं, तो आपको डेवलपर के लिए बनाई गई Google Play की सभी नीतियों का पालन करना होगा. साथ ही, यहां दी गई ज़रूरी शर्तें भी पूरी करनी होंगी. किसी नीति का पालन न करने या ज़रूरी शर्त को पूरा न करने पर, आपके SDK टूल या मीडिएशन प्लैटफ़ॉर्म को Families Self-Certified Ads SDK Program से हटाया या निलंबित किया जा सकता है.

यह पक्का करना आपकी ज़िम्मेदारी है कि आपका SDK टूल या मीडिएशन प्लैटफ़ॉर्म सभी ज़रूरी शर्तें पूरी करता हो. इसलिए, कृपया Google Play Developer Program की नीतियों, Google Play की परिवार से जुड़ी नीतियों, और Families Self-Certified Ads SDK Program की ज़रूरी शर्तों को ठीक से पढ़ लें.

1. **विज्ञापन का कॉन्टेंट:** बच्चों को दिखाए जाने वाले विज्ञापन का कॉन्टेंट, उनकी उम्र के हिसाब से सही होना चाहिए.
   - आपको (i) यह तय करना होगा कि किस तरह के विज्ञापन और व्यवहार आपत्तिजनक हैं और (ii) उन पर पाबंदी लगाने के लिए शर्तें या नीतियां तय करनी होंगी. कॉन्टेंट की परिभाषाएं, उन पर रोक लगाने के लिए तय की जाने वाली शर्तें और नीतियां, Google Play Developer Program की नीतियों के मुताबिक होनी चाहिए.
   - आपको अपने विज्ञापन क्रिएटिव को रेटिंग देने का तरीका भी तय करना होगा. यह तरीका उम्र के हिसाब से बने अलग-अलग ग्रुप के मुताबिक सही होना चाहिए. इन ग्रुप में 'सभी के लिए' और 'वयस्क', दोनों तरह के ग्रुप शामिल होने चाहिए. रेटिंग देने का तरीका, Google के तरीके के हिसाब से होना चाहिए. SDK टूल के लिए लागू होने वाले तरीके की जानकारी एक लिंक से मिलती है, जो दिलचस्पी दिखाने वाला फ़ॉर्म भरने के बाद जनरेट होता है.
   - आपको यह पक्का करना होगा कि जब रीयल-टाइम बिडिंग की प्रक्रिया का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए किया जाए, तो उससे पहले क्रिएटिव की समीक्षा की गई हो और वे ऊपर बताई गई ज़रूरी शर्तों के मुताबिक हों.
   - इसके अलावा, आपके पास आपकी इन्वेंट्री से आने वाले क्रिएटिव को देखकर पहचानने का तरीका भी होना चाहिए. उदाहरण के लिए, विज्ञापन के क्रिएटिव पर आपकी कंपनी के लोगो या उसके जैसी ही किसी अन्य चीज़ से वॉटरमार्किंग की गई हो, जो साफ़ तौर पर दिखे.

2. **विज्ञापन फ़ॉर्मैट:** आपको यह पक्का करना होगा कि नाबालिग उपयोगकर्ताओं को दिखाए जाने वाले सभी विज्ञापन, परिवार के लिए बनाए गए विज्ञापन फ़ॉर्मैट की ज़रूरी शर्तों के मुताबिक हों. साथ ही, आपको डेवलपर को ऐसे विज्ञापन फ़ॉर्मैट चुनने की भी अनुमति देनी होगी जो Google Play की परिवार नीति का पालन करते हों.
   - विज्ञापन, गुमराह करने वाले नहीं होने चाहिए. साथ ही, उन्हें इस तरह से डिज़ाइन किया गया हो कि नाबालिग उपयोगकर्ता उन पर अनजाने में क्लिक न करें. धोखाधड़ी वाले ऐसे विज्ञापन जिन्हें बंद करने के लिए, खारिज करने के बटन पर क्लिक करने के लिए मजबूर किया जाता है या ऐसे विज्ञापन जो उन जगहों पर अचानक दिखते हैं जहां उपयोगकर्ता आम तौर पर अन्य फ़ंक्शन के लिए टैप करता है:
   - परेशान करने वाले विज्ञापनों को अनुमति नहीं दी जाती. इनमें ऐसे विज्ञापन शामिल होते हैं जो पूरी स्क्रीन घेर लेते हैं या डिवाइस के सामान्य इस्तेमाल में रुकावट डालते हैं. साथ ही, इनमें विज्ञापन हटाने का तरीका भी साफ़ तौर पर नहीं दिया गया होता है. विज्ञापन वॉल, इस तरह के विज्ञापनों का एक उदाहरण है.
   - ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट डालने वाले विज्ञापन ऐसे होने चाहिए कि उन्हें पांच सेकंड तक चलने के बाद बंद किया जा सके. इनमें, इनाम देने वाले या ऑप्ट-इन करने का विकल्प दिखाने वाले विज्ञापन भी शामिल हैं.
   - किसी पेज पर एक से ज़्यादा विज्ञापन प्लेसमेंट की अनुमति नहीं है. उदाहरण के लिए, ऐसे बैनर विज्ञापन की अनुमति नहीं है जो एक प्लेसमेंट में एक से ज़्यादा ऑफ़र दिखाते हैं या एक से ज़्यादा बैनर या वीडियो विज्ञापन दिखाने की अनुमति नहीं है.
   - विज्ञापन ऐसे होने चाहिए जिन्हें ऐप्लिकेशन के कॉन्टेंट से अलग साफ़ तौर पर पहचाना जा सके. ऐसे Offerwall और ध्यान खींचने वाले ऐसे विज्ञापनों की अनुमति नहीं है जिन्हें बच्चे, विज्ञापन के तौर पर न पहचान सकें.
   - विज्ञापन व्यू बढ़ाने के लिए, विज्ञापन में भावनात्मक रूप से गुमराह करने या चौंकाने वाले तरीकों का इस्तेमाल नहीं करना चाहिए.

3. **आईबीए/रीमार्केटिंग:** आपको यह पक्का करना होगा कि नाबालिग उपयोगकर्ताओं को दिखाए जाने वाले विज्ञापनों में, दिलचस्पी के आधार पर दिखाए जाने वाले या रीमार्केटिंग करने वाले विज्ञापन शामिल न हों. दिलचस्पी के हिसाब से दिखाए जाने वाले विज्ञापन वे

होते हैं जो ऑनलाइन ब्राउज़िंग व्यवहार के हिसाब से लोगों को टारगेट करके दिखाए जाते हैं. वहीं, रीमार्केटिंग करने वाले विज्ञापन, किसी ऐप्लिकेशन या वेबसाइट के साथ पिछले इंटरैक्शन के हिसाब से लोगों को टारगेट करके दिखाए जाते हैं.

4. **डेटा इस्तेमाल करने के तरीके:** आपको यानी SDK टूल की सेवा देने वाली कंपनी को साफ़ तौर पर उपयोगकर्ता को यह जानकारी देनी होगी कि उनके डेटा को किस तरह मैनेज किया जाता है. उदाहरण के लिए, आपको बताना होगा कि किसी उपयोगकर्ता से या उसके बारे में इकट्ठा किया गया डेटा कैसे मैनेज किया जाता है. इसमें, डिवाइस की जानकारी के इस्तेमाल के बारे में बताना भी शामिल है. इसका मतलब है कि आपको उपयोगकर्ता को यह बताना होगा कि SDK टूल के ज़रिए, उनकी कौनसी जानकारी ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर की जा सकती है. साथ ही, यह भी बताना होगा कि SDK टूल आपके बताए गए कामों के अलावा, किसी और काम के लिए इस डेटा का इस्तेमाल नहीं करता है. निजता और डेटा की सुरक्षा के लागू कानूनों में बताई गई ज़रूरी शर्तों के साथ-साथ Google Play की इन ज़रूरी शर्तों को पूरा करना भी ज़रूरी है. आपको अपने ऐप्लिकेशन में, बच्चों से मिली किसी भी तरह की निजी और संवेदनशील जानकारी इकट्ठा करने के बारे में बताना होगा. बच्चों से मिली संवेदनशील जानकारी में पहचान की पुष्टि करने की जानकारी, माइक्रोफ़ोन और कैमरा सेंसर का डेटा, डिवाइस का डेटा, Android आईडी, और विज्ञापन देखने से जुड़े डेटा की जानकारी शामिल है. इसमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.
   - डेवलपर को हर अनुरोध या हर ऐप्लिकेशन के आधार पर, विज्ञापन देने के लिए बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव का अनुरोध करने दें. इस तरह के बर्ताव, लागू कानूनों और नियमों, जैसे कि अमेरिका में लागू चिल्ड्रंस ऑनलाइन प्राइवसी प्रोटेक्शन ऐक्ट (कोपा) और ईयू (यूरोपीय संघ) में लागू जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) के मुताबिक होने चाहिए.
     - बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव लागू करने के लिए Google Play को, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल की ज़रूरत होती है. इससे वह दिलचस्पी के मुताबिक दिखाए जाने वाले विज्ञापन और रीमार्केटिंग को बंद कर पाता है.
   - आपको यह पक्का करना होगा कि जब रीयल-टाइम बिडिंग की प्रक्रिया का इस्तेमाल बच्चों को विज्ञापन दिखाने के लिए किया जाए, तो बिडिंग करने वालों को निजता बनाए रखने के संकेत दिखें.
   - आपको बच्चों या उन उपयोगकर्ताओं से मिली जानकारी को शेयर नहीं करना चाहिए जिनकी उम्र के बारे में पता नहीं है. इस जानकारी में, AAID, सिम का सीरियल नंबर, बिल्ड का सीरियल नंबर, BSSID, एमएसी, SSID, IMEI, और/या IMSI शामिल है.
5. **मीडिएशन प्लैटफ़ॉर्म**: बच्चों को विज्ञापन दिखाते समय, आपको ये काम ज़रूर करने होंगे:
   - Families Self-Certified Ads SDKs Program या सुरक्षा के ज़रूरी उपाय लागू करें, ताकि यह पक्का किया जा सके कि मीडिएशन से दिखाए जाने वाले सभी विज्ञापन इन शर्तों के मुताबिक हैं; और
   - विज्ञापन की रेटिंग और बच्चों को ध्यान में रखते हुए व्यवहार/बर्ताव दिखाने के लिए, मीडिएशन प्लैटफ़ॉर्म को ज़रूरी जानकारी दें.
6. **अपने SDK टूल खुद प्रमाणित करना और उससे जुड़े नियमों का पालन:** आपको कुछ ज़रूरी जानकारी Google को देनी होगी, ताकि इस बात की पुष्टि की जा सके कि विज्ञापन दिखाने के लिए इस्तेमाल किया जाने वाला SDK टूल, खुद प्रमाणित करने से जुड़ी सभी ज़रूरी शर्तों के मुताबिक है. जैसे, दिलचस्पी दिखाने वाले फ़ॉर्म में दी गई जानकारी. इसमें इनके अलावा, और भी जानकारी शामिल हो सकती है:
   - आपको अपने SDK टूल या मीडिएशन प्लैटफ़ॉर्म की सेवा की शर्तों, निजता नीति, और पब्लिशर इंटिग्रेशन गाइड का अंग्रेज़ी वर्शन देना होगा
   - टेस्ट ऐप्लिकेशन का नमूना सबमिट करना होगा. इस नमूने में, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल का ऐसा वर्शन मौजूद होना चाहिए जो नया हो और नीति के मुताबिक हो. टेस्ट ऐप्लिकेशन के नमूने को पूरी तरह तैयार और ऐसे एक्ज़ीक्यूटेबल Android APK के तौर पर सबमिट करना चाहिए जिसमें SDK टूल की सभी सुविधाओं का इस्तेमाल किया जा रहा हो. टेस्ट ऐप्लिकेशन से जुड़ी ज़रूरी शर्तें:
     - टेस्ट ऐप्लिकेशन को पूरी तरह तैयार और ऐसे एक्ज़ीक्यूटेबल Android APK के तौर पर सबमिट करना ज़रूरी है जिसे किसी भी तरह के फ़ोन पर चलाया जा सके.
     - ज़रूरी है कि इसमें, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल का हाल ही में रिलीज़ हुआ या जल्द ही रिलीज़ होने वाला वर्शन इस्तेमाल किया गया हो और वह Google Play की नीतियों के मुताबिक हो.
     - ज़रूरी है कि इसमें, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले आपके SDK टूल की सभी सुविधाओं का इस्तेमाल किया गया हो. इन सुविधाओं में, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल की मदद से विज्ञापनों को फिर से ढूंढना और दिखाना भी शामिल है.
     - ज़रूरी है कि टेस्ट ऐप्लिकेशन के पास, नेटवर्क पर मौजूद लाइव/दिखाई जा रही सभी विज्ञापन इन्वेंट्री का पूरा ऐक्सेस हो. यह ऐक्सेस उन क्रिएटिव की मदद से मिलता है जिनका अनुरोध टेस्ट ऐप्लिकेशन करता है.
     - भौगोलिक जगह के हिसाब से, टेस्ट ऐप्लिकेशन पर रोक नहीं लगानी चाहिए.
     - अगर आपकी इन्वेंट्री कई तरह के दर्शकों के लिए है, तो ज़रूरी है कि आपका टेस्ट ऐप्लिकेशन यह पता लगा सके कि विज्ञापन क्रिएटिव के लिए अनुरोध पूरी इन्वेंट्री से मिले हैं या सिर्फ़ उस इन्वेंट्री से जो बच्चों या सभी उम्र समूहों के लिए सही है.
     - अगर न्यूट्रल एज स्क्रीन आपके टेस्ट ऐप्लिकेशन को कंट्रोल नहीं करती है, तो इसे इन्वेंट्री के खास विज्ञापनों तक सीमित नहीं करना चाहिए.

7. जानकारी पाने के लिए किए गए किसी भी अनुरोध का जवाब, आपको समय पर देना होगा. साथ ही, आपको यह खुद प्रमाणित करना होगा कि इस वर्शन की सभी नई रिलीज़, Google Play Developer Program की नई नीतियों और परिवार नीति की ज़रूरी शर्तों के मुताबिक हैं.
8. **कानून का पालन:** परिवार को खुद से प्रमाणित किए गए विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल में ऐसे विज्ञापन देने की सुविधा होनी चाहिए जो उनके पब्लिशर पर लागू होने वाले, बच्चों से जुड़े सभी ज़रूरी कानूनों और नियमों के मुताबिक हों.
   - आपको यह पक्का करना होगा कि आपका SDK टूल या मीडिएशन प्लैटफ़ॉर्म अमेरिका में लागू चिल्ड्रंस ऑनलाइन प्राइवसी प्रोटेक्शन ऐक्ट (कोपा), ईयू में लागू जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर), और किसी भी अन्य लागू कानून या नियम के मुताबिक हो.

     ध्यान दें: अलग-अलग भाषाओं और कॉन्टेक्स्ट में "बच्चे" शब्द के अलग-अलग मतलब हो सकते हैं. यह ज़रूरी है कि आप अपने कानूनी सलाहकार से पूछें कि आपके ऐप्लिकेशन पर किस तरह की कानूनी जवाबदेही और/या उम्र से जुड़ी पाबंदियां लागू हो सकती हैं. आपका ऐप्लिकेशन किस तरह काम करता 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.

इस कार्यक्रम की ज़्यादा जानकारी पाने के लिए, कृपया Families Self-Certified Ads SDK Program पेज पर जाएं.

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 उल्लंघन दिखता है या उल्लंघन को प्रबंधित करने के बारे में आपके कोई 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, ये नीतियां आपके डेवलपर खाते के ऐसे किसी भी कॉन्टेंट पर लागू होती हैं जो Google Play में सार्वजनिक रूप से दिखता है. इसमें डेवलपर का नाम और सूची में शामिल आपकी डेवलपर वेबसाइट का लैंडिंग पेज भी शामिल है.

हम ऐसे किसी ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जो उपयोगकर्ताओं को उनके डिवाइस पर दूसरे ऐप्लिकेशन इंस्टॉल करने की अनुमति देते हैं. कुछ ऐप्लिकेशन लोगों को दूसरे ऐप्लिकेशन, गेम या सॉफ़्टवेयर का ऐक्सेस उन्हें इंस्टॉल किए बिना ही दे देते हैं और साथ ही, तीसरे पक्ष की दी हुई सुविधाएं और उनसे जुड़े अनुभव भी देते हैं. ऐसे ऐप्लिकेशन के लिए यह पक्का करना ज़रूरी है कि वे जिस कॉन्टेंट का ऐक्सेस देते हैं वह Google Play की नीतियों के मुताबिक हो. साथ ही, उस पर नीति की अन्य समीक्षाएं भी लागू हो सकती 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, ज़रूरी है कि आपके ऐप्लिकेशन का कॉन्टेंट हमारे कॉन्टेंट रेटिंग से जुड़े दिशा-निर्देश के मुताबिक रेट किया जाए.

हम ऐसे ऐप्लिकेशन या ऐप्लिकेशन के कॉन्टेंट को अनुमति नहीं देते जो Google Play नेटवर्क में उपयोगकर्ता के भरोसे को कम करता है. Google Play में किसी ऐप्लिकेशन को शामिल करना या हटाना, कुछ बातों के मुताबिक तय किया जाता है. इनमें नुकसान पहुंचाने वाले या बुरे बर्ताव और यौन शोषण के अलावा, और भी चीज़ें शामिल हो सकती हैं. हम ऐप्लिकेशन और डेवलपर के हिसाब से शिकायतें, समाचार रिपोर्टिंग, पहले हुए उल्लंघनों की जानकारी, और ऐप्लिकेशन इस्तेमाल करने वाले लोगों की शिकायतों, सुझाव या राय की मदद से बुरा बर्ताव होने के खतरे की पहचान करते हैं. साथ ही, इसके लिए हम लोकप्रिय ब्रैंड, उससे जुड़े लोगों की जानकारी, और अन्य एसेट जैसी चीज़ों का इस्तेमाल भी करते हैं. इनमें इनके अलावा, और भी चीज़ें शामिल हो सकती हैं.

Google Play Protect के काम करने का तरीका

जब आप ऐप्लिकेशन को इंस्टॉल करते हैं, तब Google Play Protect 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 हटाया जाता है, तो Google Play Protect आपको इस बारे में चेतावनी भेजेगा. ऐसा इसलिए किया जाता है, क्योंकि ऐप्लिकेशन आपकी निजी जानकारी ऐक्सेस करने की कोशिश कर सकता है. साथ ही, चेतावनी मिलने पर आप ऐप्लिकेशन को अनइंस्टॉल भी कर सकते हैं.

नीति उल्लंघन ठीक करने के तरीके को लागू करने की प्रक्रिया

कॉन्टेंट या खातों की समीक्षा करते समय, कॉन्टेंट या खाते गैर-कानूनी हैं या नहीं या हमारी नीतियों का उल्लंघन करते हैं या नहीं, यह तय करने के लिए हम कई बातों को ध्यान में रखते हैं. इनमें, ऐप्लिकेशन का मेटाडेटा (उदाहरण के लिए, ऐप्लिकेशन का नाम और ब्यौरा), इन-ऐप्लिकेशन अनुभव, खाते की जानकारी (उदाहरण के लिए, नीति के उल्लंघन के पुराने मामले), और शिकायत करने के खास तरीकों (जहां भी लागू हो) और मैन्युअल तरीके से की गई समीक्षाओं का इस्तेमाल करके दी गई अन्य जानकारी शामिल है.

अगर आपका ऐप्लिकेशन या डेवलपर खाता हमारी किसी भी नीति का उल्लंघन करता है, तो हम उसके हिसाब से सही कार्रवाई करेंगे. इस बारे में नीचे बताया गया है. इसके अलावा, हम जो कार्रवाई करेंगे उसकी जानकारी आपको ईमेल से भेजी जाएगी. अगर आपको लगता है कि हमने गलत कार्रवाई की है, तो अपील करने का तरीका भी इस ईमेल में बताया जाएगा.

कृपया ध्यान दें, हो सकता है कि एडमिनिस्ट्रेटिव नोटिस या कॉन्टेंट हटाने से जुड़े नोटिस में, आपके खाते, ऐप्लिकेशन या आपके सभी ऐप्लिकेशन के कैटलॉग में हुए हर उल्लंघन के बारे में पूरी जानकारी न दी गई हो. नीति से जुड़ी किसी भी समस्या का जवाब देने और उसे हल करने के लिए, अन्य ज़रूरी कार्रवाई करने की ज़िम्मेदारी डेवलपर की होती है. इन कार्रवाइयों से डेवलपर यह पक्का करते हैं कि उनका पूरा ऐप्लिकेशन या खाता, सभी नीतियों का पालन करता हो. अपने खाते या सभी ऐप्लिकेशन में, किसी भी नीति के उल्लंघन को ठीक करने में असफल रहने पर, आपको नीति उल्लंघन ठीक करने के तरीके (एनफ़ोर्समेंट) से जुड़ी अन्य कार्रवाइयों का सामना करना पड़ सकता है.

इन नीतियों या डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट (डीडीए) के बार-बार होने वाले या गंभीर उल्लंघनों की वजह से, किसी व्यक्ति के Google Play डेवलपर खाते या उससे जुड़े सभी Google Play डेवलपर खातों को बंद कर दिया जाएगा. इन उल्लंघनों में मैलवेयर, धोखाधड़ी, और उपयोगकर्ता या डिवाइस को नुकसान पहुंचाने वाले ऐप्लिकेशन शामिल हैं.

नीति के उल्लंघन की वजह से की जाने वाली कार्रवाईयां

नीति उल्लंघन ठीक करने के तरीके (एनफ़ोर्समेंट) से जुड़ी अलग-अलग कार्रवाइयां, आपके ऐप्लिकेशन पर अलग-अलग असर डाल सकती हैं. ऐप्लिकेशन और उसके कॉन्टेंट की समीक्षा के लिए, हम ऑटोमेटेड और मैन्युअल, दोनों तरीकों का इस्तेमाल करते हैं. इनसे, हम नीतियों का उल्लंघन करने वाले ऐसे कॉन्टेंट का पता लगाते हैं और उसकी जांच करते हैं जो उपयोगकर्ताओं और Google Play के पूरे ईकोसिस्टम के लिए नुकसानदेह है. हम ऑटोमेटेड मॉडल का इस्तेमाल, तेज़ी से ज़्यादा उल्लंघनों का पता लगाने और संभावित समस्याओं की जांच की प्रक्रिया को पूरा करने के लिए करते हैं. इससे, Google Play को सभी के लिए सुरक्षित बनाए रखने में मदद मिलती है. हमारा ऑटोमेटेड मॉडल, नीति का उल्लंघन करने वाले कॉन्टेंट को हटा देता है या किसी कॉन्टेंट के लिए बेहतर जांच की ज़रूरत पड़ने पर, उसे समीक्षा के लिए फ़्लैग कर देता है. कॉन्टेंट की समीक्षा ऐसे ऑपरेटर और ऐनलिस्ट करते हैं जिन्हें खास तौर पर इसकी ट्रेनिंग दी गई है. ऐसा इसलिए किया जाता है, क्योंकि अलग-अलग तरह के कॉन्टेंट को समझने के लिए, उससे जुड़ी जानकारी की ज़रूरत होती है. इसके बाद, मैन्युअल तरीके से की गई इन समीक्षाओं के नतीजों का इस्तेमाल करके, ट्रेनिंग का डेटा बनाया जाता है. इस डेटा से, हमें मशीन लर्निंग मॉडल को और बेहतर बनाने में मदद मिलती है.

नीचे दिए गए सेक्शन में, Google Play की ओर से की जाने वाली कार्रवाइयों की जानकारी दी गई है. इसमें यह भी बताया गया है कि इन कार्रवाइयों का आपके ऐप्लिकेशन या Google Play डेवलपर खाते पर क्या असर पड़ेगा.

जब तक नीति उल्लंघन ठीक करने के तरीके (एनफ़ोर्समेंट) से जुड़ी कोई जानकारी अलग से नहीं दी जाती, तब तक इन कार्रवाइयों का असर सभी देशों/इलाकों पर होगा. उदाहरण के लिए, अगर आपके ऐप्लिकेशन को निलंबित किया जाता है, तो वह किसी भी देश/इलाके में उपलब्ध नहीं होगा. जब तक कोई जानकारी अलग से नहीं दी जाती, तब तक मौजूदा कार्रवाइयां लागू रहेंगी. कार्रवाइयों के फ़ैसले को बदलने के लिए, उनके ख़िलाफ़ अपील करना और अपील को मंज़ूरी मिलना ज़रूरी है.

अस्वीकार किया जाना

- समीक्षा के लिए सबमिट किया गया नया ऐप्लिकेशन या ऐप्लिकेशन का अपडेट, Google Play पर उपलब्ध नहीं कराया जाएगा.
- 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: अस्वीकार किए गए ऐप्लिकेशन को तब तक फिर से सबमिट करने की कोशिश न करें, जब तक आप नीति के सभी उल्लंघनों को ठीक नहीं कर लेते.

हटाना

- ऐप्लिकेशन और उसके सभी पुराने वर्शन को Google Play से हटा दिया गया है. इसलिए, अब वे डाउनलोड किए जाने के लिए उपलब्ध नहीं हैं.
- ऐप्लिकेशन हटाए जाने के बाद, लोगों को ऐप्लिकेशन का स्टोर पेज नहीं दिखेगा. हटाए गए ऐप्लिकेशन के लिए, नीति का पालन करने वाला अपडेट सबमिट करने के बाद, ऐप्लिकेशन का स्टोर पेज फिर से दिखने लगेगा.
- हो सकता है कि 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 इस्तेमाल न कर पाएं.
- ऐप्लिकेशन हटाए जाने से, आपके Google Play डेवलपर खाते की स्थिति पर तुरंत कोई असर नहीं पड़ता. हालांकि, ऐप्लिकेशन को कई बार हटाए जाने पर, आपका डेवलपर खाता निलंबित किया जा सकता है.

ध्यान दें: हटाए गए ऐप्लिकेशन को फिर से पब्लिश करने की कोशिश तब तक न करें, जब तक आप नीति के सभी उल्लंघनों को ठीक न कर लें.

निलंबन

- ऐप्लिकेशन और उसके सभी पुराने वर्शन को Google Play से हटा दिया गया है. इसलिए, अब वे डाउनलोड किए जाने के लिए उपलब्ध नहीं हैं.
- अगर नीति का गंभीर या कई बार उल्लंघन किया जाता है, तो आपके ऐप्लिकेशन को निलंबित किया जा सकता है. इसके अलावा, ऐप्लिकेशन को बार-बार अस्वीकार किए जाने या हटाए जाने पर भी यह कार्रवाई की जा सकती है.
- ऐप्लिकेशन को निलंबित कर दिया गया है. इसलिए, लोगों को ऐप्लिकेशन का स्टोर पेज नहीं दिखेगा.
- निलंबित ऐप्लिकेशन के APK या ऐप्लिकेशन बंडल का इस्तेमाल नहीं किया जा सकता है.
- लोग, न तो कोई इन-ऐप्लिकेशन खरीदारी कर पाएंगे और न ही ऐप्लिकेशन में इन-ऐप बिलिंग की सुविधाओं का इस्तेमाल कर पाएंगे.
- ऐप्लिकेशन के निलंबन को शिकायत के तौर पर गिना जाता है. आपके Google Play डेवलपर खाते की अच्छी स्थिति पर इसका बुरा असर पड़ता है. कई बार निलंबन होने पर, किसी व्यक्ति के निजी खाते या उसके सभी Google Play डेवलपर खातों को बंद किया जा सकता है.

यह सीमित करना कि ऐप्लिकेशन किसे दिखेगा

- Google Play पर आपके ऐप्लिकेशन को खोजे जाने पर पाबंदी लगा दी गई है. हालांकि, Google Play पर आपका ऐप्लिकेशन उपलब्ध रहेगा. ऐप्लिकेशन के स्टोर पेज के लिंक से, उपयोगकर्ता उसे सीधे ऐक्सेस कर सकते हैं.
- ऐप्लिकेशन किसे दिखेगा, यह सीमित करने से आपके Google Play डेवलपर खाते की स्थिति पर असर नहीं पड़ता.
- ऐप्लिकेशन किसे दिखेगा, यह सीमित करने के बाद भी, उपयोगकर्ता ऐप्लिकेशन का मौजूदा स्टोर पेज, ऐप्लिकेशन इंस्टॉल करने वाले लोगों की संख्या, आंकड़े, और रेटिंग देख पाएंगे.

वे चुनिंदा क्षेत्र जहां ऐप्लिकेशन उपलब्ध है

- कुछ क्षेत्रों में आपके ऐप्लिकेशन को उपयोगकर्ता, सिर्फ़ Google Play की मदद से डाउनलोड कर सकते हैं.

- अन्य क्षेत्रों के उपयोगकर्ताओं को Play Store पर ऐप्लिकेशन नहीं मिल पाएगा.
- वे उपयोगकर्ता जिन्होंने ऐप्लिकेशन को पहले ही इंस्टॉल कर लिया था वे अपने डिवाइस पर इसे अब भी इस्तेमाल कर सकते हैं, लेकिन उन्हें अपडेट नहीं मिलेंगे.
- चुनिंदा क्षेत्रों में आपके ऐप्लिकेशन को उपलब्ध कराने से आपके Google Play डेवलपर खाते की स्थिति पर कोई असर नहीं पड़ता.

खाते पर पाबंदी लगी होने की स्थिति

- अगर आपके डेवलपर खाते पर पाबंदी लगा दी जाती है, तो आपके कैटलॉग में शामिल सभी ऐप्लिकेशन Google Play से हटा दिए जाएंगे. साथ ही, आपके पास नए ऐप्लिकेशन पब्लिश करने या मौजूदा ऐप्लिकेशन को फिर से पब्लिश करने का विकल्प नहीं होगा. हालांकि, अब भी Play Console को ऐक्सेस किया जा सकेगा.
- सभी ऐप्लिकेशन हटाए जाने के बाद, लोगों को ऐप्लिकेशन का स्टोर पेज और आपकी डेवलपर प्रोफ़ाइल नहीं दिखेगी.
- आपके मौजूदा उपयोगकर्ता न तो कोई इन-ऐप्लिकेशन खरीदारी कर पाएंगे और न ही आपके ऐप्लिकेशन में इन-ऐप्लिकेशन बिलिंग की सुविधाओं का इस्तेमाल कर पाएंगे.
- हालांकि, Google Play को ज़्यादा जानकारी उपलब्ध कराने और खाते से जुड़ी अपनी जानकारी में बदलाव करने के लिए, अब भी Play Console का इस्तेमाल किया जा सकता है.
- नीति के सभी उल्लंघनों को ठीक करने के बाद, ऐप्लिकेशन फिर से पब्लिश किए जा सकेंगे.

खाता बंद किया जाना

- अगर आपका डेवलपर खाता बंद कर दिया जाता है, तो आपके कैटलॉग में शामिल सभी ऐप्लिकेशन Google Play से हटा दिए जाएंगे. साथ ही, आपके पास नए ऐप्लिकेशन पब्लिश करने का विकल्प भी नहीं होगा. इसका मतलब यह भी है कि बंद किए गए आपके खाते से जुड़े Google Play डेवलपर खातों को भी हमेशा के लिए निलंबित कर दिया जाएगा.
- खाते के कई बार निलंबित होने या नीति के गंभीर उल्लंघनों की वजह से, आपका Play Console खाता बंद किया जा सकता है.
- बंद किए गए खाते में मौजूद ऐप्लिकेशन हटाए जाने की वजह से, लोगों को आपके ऐप्लिकेशन का स्टोर पेज और आपकी डेवलपर प्रोफ़ाइल नहीं दिखेगी.
- आपके मौजूदा उपयोगकर्ता न तो कोई इन-ऐप्लिकेशन खरीदारी कर पाएंगे और न ही आपके ऐप्लिकेशन में इन-ऐप्लिकेशन बिलिंग की सुविधाओं का इस्तेमाल कर पाएंगे.

ध्यान दें: अगर पहले से आपका कोई खाता बंद किया गया है, तो कृपया नया Play Console खाता बनाने की कोशिश न करें. ऐसा करने पर, डेवलपर रजिस्ट्रेशन शुल्क रिफ़ंड किए बिना ही नए खाते को बंद कर दिया जाएगा.

डॉरमेंट खाते

डॉरमेंट खाते, वे डेवलपर खाते हैं जिन्हें बनाकर छोड़ दिया गया हो या जिनका इस्तेमाल नहीं किया जा रहा हो. डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट के मुताबिक, डॉरमेंट खाता होना अच्छी स्थिति नहीं है.

Google Play डेवलपर खाते, उन डेवलपर के लिए हैं जो अपने खाते का इस्तेमाल करते रहते हैं. वे अपने खाते से ऐप्लिकेशन पब्लिश करने के साथ-साथ मैनेज भी करते रहते हैं. किसी भी तरह के गलत इस्तेमाल को रोकने के लिए, हम ऐसे खातों को बंद कर देते हैं जो डॉरमेंट हैं या जिनका इस्तेमाल नहीं किया जा रहा है. ऐसे खाते भी बंद कर दिए जाते हैं जिनसे नियमित तौर पर किसी ऐप्लिकेशन को पब्लिश और अपडेट नहीं किया जाता, आंकड़े ऐक्सेस नहीं किए जाते या स्टोर पेजों को मैनेज नहीं किया जाता.

डॉरमेंट खाता बंद किए जाने पर, आपका खाता और उससे जुड़ा डेटा मिटा दिया जाएगा. आपका रजिस्ट्रेशन शुल्क रिफ़ंड नहीं किया जाएगा. उसे दंड के तौर पर ज़ब्त कर लिया जाएगा. डॉरमेंट खाते को बंद करने से पहले, हम उस खाते में आपकी ओर से दी गई संपर्क जानकारी का इस्तेमाल करके, आपको खाता बंद किए जाने की सूचना देंगे.

डॉरमेंट खाते को बंद किए जाने का मतलब यह नहीं है कि उपयोगकर्ता नया खाता नहीं बना पाएगा. उपयोगकर्ता जब चाहें खाता बनाकर, Google Play पर ऐप्लिकेशन पब्लिश कर सकते हैं. हालांकि, आपके पास बंद किए गए खाते को फिर से चालू करने की अनुमति नहीं होगी. उस खाते से जुड़ा डेटा या पुराने ऐप्लिकेशन, नए खाते पर उपलब्ध नहीं होंगे.

नीति के उल्लंघनों का प्रबंधन और उनकी शिकायत करना

नीति के उल्लंघन की वजह से की गई कार्रवाई के ख़िलाफ़ अपील करना

हम आपके ऐप्लिकेशन दोबारा तब पब्लिश करेंगे, जब कोई गड़बड़ी हुई हो और हमें पता चले कि आपका ऐप्लिकेशन, Google Play कार्यक्रम की नीतियों और डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट का उल्लंघन न करता हो. अगर आपने नीतियों को ध्यान से पढ़ लिया है और

आपको लगता है कि हमारे फ़ैसले में गड़बड़ी हुई है, तो इसके ख़िलाफ़ अपील करने के लिए कृपया, नीति उल्लंघन ठीक करने के तरीके बताने वाली ईमेल सूचना में दिए गए निर्देशों का पालन करें या यहां क्लिक करें.

दूसरे संसाधन

अगर आपको नीति के उल्लंघन की वजह से की गई कार्रवाई या ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति की दी गई रेटिंग/टिप्पणी के बारे में ज़्यादा जानकारी चाहिए, तो आप नीचे दिए गए कुछ संसाधनों को देख सकते हैं या Google Play के सहायता केंद्र पर जाकर, हमसे संपर्क कर सकते हैं. हालांकि, हम आपको कानूनी सलाह नहीं दे सकते हैं. अगर आपको कानूनी सलाह चाहिए, तो कृपया अपने कानूनी सलाहकार से संपर्क करें.

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

Play Console से जुड़ी ज़रूरी शर्तें

ऐप्लिकेशन के हमारे पूरे ईकोसिस्टम की सुरक्षा के लिए, Google Play पर मौजूद सभी डेवलपर को Play Console की ज़रूरी शर्तें पूरी करनी होंगी. इनमें ऐसे डेवलपर भी शामिल हैं जिनकी प्रोफ़ाइल Play Console डेवलपर खाते से लिंक है. लोगों को डेवलपर के ऐप्लिकेशन डाउनलोड करने में झिझक न हो, इसके लिए Google Play पर वह जानकारी दिखेगी जिसकी पुष्टि हो चुकी है. Google Play पर दिखने वाली जानकारी के बारे में ज़्यादा जानें.

Google Play पर दो तरह के डेवलपर खाते बनाए जा सकते हैं: निजी खाता और संगठन का खाता. खाते का आसानी से इस्तेमाल करने के लिए, सही डेवलपर खाता चुनना और पुष्टि से जुड़ी ज़रूरी प्रोसेस पूरी करना सबसे ज़रूरी है. डेवलपर खाते का टाइप चुनने के बारे में ज़्यादा जानें.

जो डेवलपर यहां दी गई सेवाएं उपलब्ध करा रहे हैं उन्हें Play Console खाता बनाते समय, संगठन के तौर पर रजिस्टर करना होगा:

- फ़ाइनेंशियल प्रॉडक्ट और सेवाएं, बैंक, लोन, स्टॉक ट्रेडिंग, निवेश से जुड़े फ़ंड, क्रिप्टो करंसी के सॉफ़्टवेयर वॉलेट, और क्रिप्टो करंसी एक्सचेंज की सेवाएं. इनमें इनके अलावा और भी सेवाएं शामिल हैं. वित्तीय सेवाओं से जुड़ी नीति के बारे में ज़्यादा जानें.
- सेहत से जुड़े ऐप्लिकेशन. जैसे, मेडिकल ऐप्लिकेशन और लोगों की सेहत से जुड़ी रिसर्च करने वाले ऐप्लिकेशन. सेहत से जुड़े ऐप्लिकेशन की कैटगरी के बारे में ज़्यादा जानें.
- VpnService क्लास का इस्तेमाल करने की अनुमति पा चुके ऐप्लिकेशन. वीपीएन सेवा की नीति के बारे में ज़्यादा जानें.
- सरकारी ऐप्लिकेशन. जैसे, सरकारी एजेंसी के बनाए गए या उनकी ओर से बनवाए गए ऐप्लिकेशन.

खाते का टाइप चुनने के बाद, ये काम ज़रूर करें:

- अपने डेवलपर खाते की सटीक जानकारी दें. इसमें यह जानकारी भी दें:
  - कानूनी नाम और पता
  - अगर आपने संगठन के तौर पर रजिस्टर किया है, तो डीयूएनएस नंबर
  - संपर्क करने के लिए ईमेल पता और फ़ोन नंबर
  - Google Play पर दिखने वाला डेवलपर का ईमेल पता और फ़ोन नंबर (जहां उपलब्ध कराना ज़रूरी हो)
  - पेमेंट के तरीके (जहां उपलब्ध कराना ज़रूरी हो)
  - आपके डेवलपर खाते से लिंक की गई Google पेमेंट्स प्रोफ़ाइल
- एक संगठन के तौर पर रजिस्टर करने पर, आपको यह पक्का करना चाहिए कि डेवलपर खाते की जानकारी अप-टू-डेट हो. साथ ही, यहां दी गई जानकारी और Dun & Bradstreet प्रोफ़ाइल पर सेव की गई जानकारी एक जैसी हो

अपने ऐप्लिकेशन को सबमिट करने से पहले, ये काम ज़रूर करें:

- ऐप्लिकेशन की सभी जानकारी और मेटाडेटा सही-सही उपलब्ध कराएं
- अपने ऐप्लिकेशन की निजता नीति अपलोड करें और डेटा की सुरक्षा वाले सेक्शन में ज़रूरी जानकारी भरें
- एक ऐसा डेमो खाता उपलब्ध कराएं जो चालू हो. साथ ही, लॉगिन की जानकारी और Google Play को आपके ऐप्लिकेशन की समीक्षा करने के लिए ज़रूरी अन्य सभी चीज़ें (खास तौर पर, लॉगिन क्रेडेंशियल, क्यूआर कोड वगैरह) उपलब्ध कराएं

हमेशा की तरह, आपको यह पक्का करना चाहिए कि आपका ऐप्लिकेशन, उपयोगकर्ता को भरोसेमंद, दिलचस्प, और रिस्पॉन्सिव अनुभव देता हो. दोबारा जांच लें कि आपके ऐप्लिकेशन में मौजूद सभी चीज़ें Google Play Developer Program की नीतियों के मुताबिक हैं या नहीं. इनमें, विज्ञापन नेटवर्क कंपनियां, आंकड़ों से जुड़ी सेवाएं, और तीसरे पक्ष के एसडीके टूल शामिल हैं. अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो यह पक्का करें कि आपका ऐप्लिकेशन हमारी परिवार से जुड़ी नीति का भी पालन करता हो.

याद रखें कि डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट और Developer Program की सभी नीतियों को देखना आपकी ज़िम्मेदारी है, ताकि आप यह पक्का कर सकें कि आपका ऐप्लिकेशन पूरी तरह इनका पालन करता है.

Developer Distribution Agreement

और मदद चाहिए?

आगे दिए गए कदमों को आज़माएं:

हमसे संपर्क करें

हमें ज़्यादा जानकारी दें और हम आपकी पूरी मदद करेंगे