डेवलपर कार्यक्रम की नीतियां

(9 नवंबर, 2022 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 जो पैसे या दूसरे फ़ायदे के बदले यौन गतिविधि को बढ़ावा देता है. 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.

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

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

- यौन नग्नता या ऐसी अश्लील मुद्राएं दिखाना जिसमें व्यक्ति नग्न हो, धुंधला हो या उसने बहुत कम कपड़े पहने हों और/या किसी सार्वजनिक जगह के लिहाज़ से ऐसे कपड़े सही न हों.
- ऐनिमेशन, तस्वीरों या किसी और तरह से यौन गतिविधियों को दिखाना या अश्लील मुद्राएं या शरीर के अंगों को यौन रूप से दिखाना.
- ऐसा कॉन्टेंट जिसमें सेक्स को ज़्यादा मज़ेदार बनाने या कामुकता जगाने के बारे में बताया जाता है. साथ ही, जिसमें सेक्स गाइड, गैरकानूनी यौन थीम, और यौन गतिविधियां दिखाई जाती हों.
- इसमें ऐसा कॉन्टेंट शामिल है जो ऐप्लिकेशन या स्टोर पेज में 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 प्रचार करते हैं. इसके अलावा, ऐसी अन्य सेवाओं का प्रचार करते हैं जो हो सकता है कि पैसे देकर की जाने वाली यौन गतिविधियों की सुविधा उपलब्ध कराती हैं. इसमें, 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.

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.

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

- ऐसा 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.

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

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

आतंकवाद से जुड़ा कॉन्टेंट

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

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते हैं जिनमें आतंकवाद से जुड़ा कॉन्टेंट होता है, जैसे कि आतंकी गतिविधियों को बढ़ावा देने, हिंसा करने के लिए उकसाने या आतंकी हमलों का जश्न मनाने के लिए बना कॉन्टेंट. अगर आप शिक्षा, डॉक्यूमेंट्री, विज्ञान या कला को ध्यान में रखकर आतंकवाद से जुड़ा कॉन्टेंट पोस्ट कर रहे हैं, तो उस कॉन्टेंट से जुड़े ईडीएसए कॉन्टेंट को संदर्भ के तौर पर ज़रूर उपलब्ध कराएं.

खतरनाक संगठन और आंदोलन

हम ऐसे आंदोलनों और संगठनों को किसी भी काम 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 उन ऐप्लिकेशन को अनुमति नहीं देते जिनमें नागरिकों के ख़िलाफ़ हिंसा की योजना बनाने या उसकी तैयारी करने या हिंसा की तारीफ़ से जुड़ा कॉन्टेंट शामिल हो. अगर आपके ऐप्लिकेशन में इस तरह का कॉन्टेंट किसी ईडीएसए के मकसद से शामिल किया गया है, तो उस ईडीएसए कॉन्टेंट का संदर्भ ज़रूर उपलब्ध कराएं.

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.

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.

- 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.
- ऐसे ऐप्लिकेशन जो कोरोना वायरस बीमारी 2019 (COVID-19) से संबंधित ऐप्लिकेशन के लिए बने लेख में दर्ज ज़रूरी शर्तों का उल्लंघन करते हैं.

धमकाना और उत्पीड़न करना

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

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

- अंतरराष्ट्रीय या धार्मिक टकरावों से पीड़ित लोगों को धमकाना
- 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.

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

- इस्तेमाल करने वालों को ऐप्लिकेशन में मौजूद खरीदारी कार्ट की सुविधा की मदद से गांजा मंगवाने देना.
- 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 (इसमें ई-सिगरेट और वेप पेन भी शामिल हैं) बेचने की सुविधा देते हैं या जो तंबाकू या शराब के गैरकानूनी और गलत इस्तेमाल को बढ़ावा देते हैं.

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

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

वित्तीय सेवाएं

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

इस पॉलिसी के तहत, हम पैसों और क्रिप्टो करंसी को मैनेज करने या निवेश करने को वित्तीय उत्पाद और सेवा मानते हैं. इसमें इस्तेमाल करने वाले व्यक्ति की ज़रूरतों के हिसाब से सुझाव देना भी शामिल है.

अगर आपके ऐप्लिकेशन में वित्तीय उत्पाद या सेवाएं शामिल हैं या वह इन्हें प्रमोट करता है, तो जिस इलाके या देश के लोगों को किया जा रहा है वहां के, राज्य और स्थानीय नियमों का पालन करना होगा. उदाहरण के लिए, आपको स्थानीय कानून के मुताबिक ज़रूरी जानकारी सार्वजनिक करनी होगी.

बाइनरी विकल्प

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

क्रिप्टो करंसी

हम ऐसे ऐप्लिकेशन को मंज़ूरी नहीं देते जो डिवाइस पर क्रिप्टो करंसी बनाते हैं. हालांकि, हम उन ऐप्लिकेशन को मंज़ूरी देते हैं जो कहीं और से क्रिप्टो करंसी बनाए जाने को मैनेज करते हैं.

निजी क़र्ज़

हमारे हिसाब से निजी क़र्ज़ वह पैसे होते हैं जो एक व्यक्ति किसी दूसरे व्यक्ति, संगठन या इकाई से सिर्फ़ एक बार में लेता है. इस क़र्ज़ को संपत्ति खरीदने या शिक्षा के लिए नहीं लिया जाता. निजी क़र्ज़ लेने वालों को क़र्ज़ की क्वालिटी, सुविधाओं, शुल्क, रकम 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 कर सकें.

- उदाहरण के लिए: निजी क़र्ज़, पे-डे लोन, पीयर-टू-पीयर लोन, गाड़ी को गिरवी रखकर मिलने वाले क़र्ज़ (टाइटल पर क़र्ज़)
- उदाहरण में ये शामिल 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)

ऐसे ऐप्लिकेशन जो निजी क़र्ज़ देते हैं उन्हें 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 बनाते हैं, और ग्राहकों को तीसरे पक्ष के क़र्ज़ देने वालों से मिलाते हैं. इसमें, इनके अलावा और भी ऐप्लिकेशन 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. इसमें, क़र्ज़ पर ली गई रकम और लागू होने वाले सभी शुल्क शामिल होंगे
- ऐसी प्राइवेसी पॉलिसी जिसमें 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 को बढ़ावा देने वाले ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो क़र्ज़ की पूरी रकम लौटाने के लिए, 60 दिन या उससे भी कम समय देते हैं (इन्हें हम "कम अवधि वाले निजी क़र्ज़" कहते हैं).

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 के लिए, ट्रूथ इन लेंडिंग ऐक्ट (टिला) के तहत उनका ज़्यादा से ज़्यादा लिया जाने वाला एपीआर दिखाना ज़रूरी है.

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

भारत, इंडोनेशिया, और फ़िलिपींस में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के लिए अन्य ज़रूरी शर्तें

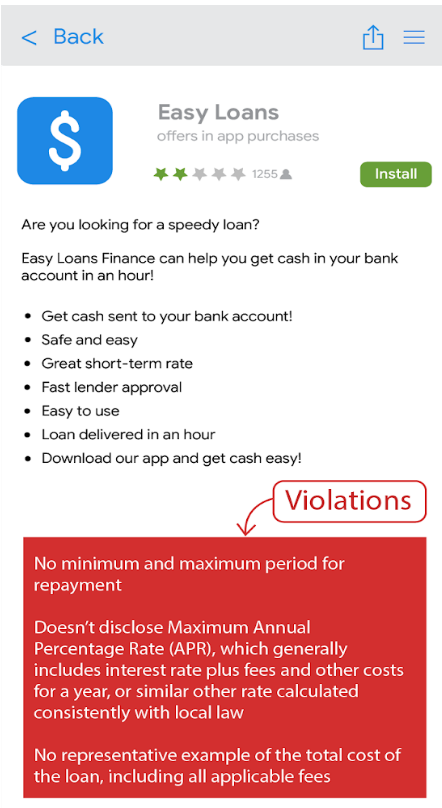
भारत, इंडोनेशिया, और फ़िलिपींस में निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के लिए, नीचे बताई गई अन्य ज़रूरी शर्तें पूरी करनी होंगी.

1. **भारत**
   - भारत के लिए, निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के एलान का फ़ॉर्म पूरा करें और उससे जुड़े ज़रूरी दस्तावेज़ उपलब्ध कराएं. उदाहरण के लिए:
     - 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 पैसे क़र्ज़ पर देने की गतिविधि में सीधे तौर पर शामिल नहीं हैं और आपकी ओर से सिर्फ़ एक ऐसा प्लैटफ़ॉर्म उपलब्ध कराया जाता है जिसका इस्तेमाल करके, रजिस्टर की गई गैर बैंकिंग वित्तीय कंपनियां (NBFC) या बैंक, उपयोगकर्ताओं को पैसे क़र्ज़ पर 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 NBFC और बैंक के नाम साफ़ तौर पर ज़ाहिर किए जाने चाहिए.
   - यह पक्का करें कि डेवलपर खाते का वही नाम हो जो आपने एलान में, रजिस्टर किए गए अपने कारोबार के नाम के तौर पर बताया हो.
2. **इंडोनेशिया**
   - इंडोनेशिया के लिए, निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के एलान का फ़ॉर्म पूरा करें और उससे जुड़े ज़रूरी दस्तावेज़ उपलब्ध कराएं. उदाहरण के लिए:
     - 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 सूचना प्रौद्योगिकी आधारित सेवाओं से जुड़ी गतिविधि में शामिल है, तो आपको अपने मान्य लाइसेंस की एक कॉपी सबमिट करनी होगी. हम उसकी जांच करेंगे.
   - यह पक्का करें कि डेवलपर खाते का वही नाम हो जो आपने एलान में, रजिस्टर किए गए अपने कारोबार के नाम के तौर पर बताया हो.

3. **फ़िलिपींस**

- फ़िलिपींस के लिए, निजी क़र्ज़ की सुविधा देने वाले ऐप्लिकेशन के एलान का फ़ॉर्म पूरा करें और उससे जुड़े दस्तावेज़ उपलब्ध कराएं.
  - फ़ाइनेंसिंग और पैसे क़र्ज़ पर देने वाली ऐसी सभी कंपनियों को फ़िलिपींस सिक्योरिटी ऐंड एक्सचेंज कमीशन (PSEC) से SEC रजिस्ट्रेशन नंबर और सर्टिफ़िकेट ऑफ अथॉरिटी (CA) नंबर लेना होगा जो ऑनलाइन प्लैटफ़ॉर्म (OLP) के ज़रिए क़र्ज़ देती हैं.
    - इसके अलावा, फ़ाइनेंसिंग/पैसे क़र्ज़ पर देने वाली कंपनी चलाने के लिए, आपको अपने ऐप्लिकेशन के ब्यौरे में कॉर्पोरेट नाम, कारोबार का नाम, PSEC रजिस्ट्रेशन नंबर, और सर्टिफ़िकेट ऑफ़ अथॉरिटी के बारे में जानकारी ज़ाहिर करनी होगी.
  - कुछ ऐप्लिकेशन, क़र्ज़ के लिए चंदे के तौर पर पैसे जुटाने से जुड़ी गतिविधियों में शामिल होते हैं. इन गतिविधियों में, पीयर-टू-पीयर लोन देने की सुविधा (P2P) या चंदे पर लागू होने वाले नियमों और कानूनों (चंदा इकट्ठा करने के नियम) के तहत बताई गई गतिविधियां शामिल हैं. इन ऐप्लिकेशन के लिए ज़रूरी है कि वे लेन-देन को प्रोसेस करने के लिए, उन प्लैटफ़ॉर्म की मदद लें जो PSEC के पास चंदे से जुड़ी गतिविधियों में मध्यस्थता करने वाले प्लैटफ़ॉर्म के तौर पर रजिस्टर हैं.

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



जुआ

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

ऐसा हो सकता है कि हम कभी-कभी असली पैसे दांव पर लगाकर खेले जाने वाले कुछ खास तरह के गेम के लिए, सीमित समय वाले पायलट कार्यक्रम चुनिंदा इलाकों में शुरू करें. ज़्यादा जानकारी के लिए, यह सहायता केंद्र पेज देखें.

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.

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.

- 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.

जो ऐप्लिकेशन यूजीसी या उसकी सुविधा उपलब्ध कराते हैं उनमें बेहतरीन, असरदार, और लगातार होने वाला यूजीसी मॉडरेशन लागू करना चाहिए. 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. इस यूजीसी मॉडरेशन में:

- ऐप्लिकेशन इस्तेमाल करने वाले लोगों का, यूजीसी बनाने या अपलोड करने से पहले ऐप्लिकेशन को इस्तेमाल करने की शर्तों और/या उपयोगकर्ता नीति को स्वीकार करना ज़रूरी हो;
- जो Google Play के डेवलपर कार्यक्रम की नीतियों के मुताबिक यह तय करता हो कि किस तरह का कॉन्टेंट और बर्ताव आपत्तिजनक है. साथ ही, ऐप्लिकेशन के इस्तेमाल की शर्तों और उपयोगकर्ता नीतियों के तहत उन पर पाबंदी लगाता हो;
- ऐसा यूजीसी मॉडरेशन लागू करता हो जो ऐप्लिकेशन पर होस्ट किए गए यूजीसी के मुताबिक सही और एक जैसा हो;
  - ऑगमेंटेड रिएलिटी (एआर) वाले ऐप्लिकेशन के मामले में, यूजीसी मॉडरेशन (जिसमें इन-ऐप्लिकेशन रिपोर्टिंग सिस्टम शामिल है) को, आपत्तिजनक एआर यूजीसी (उदाहरण के लिए, अश्लील यौन एआर इमेज) और संवेदनशील एआर एंकरिंग की जगह (उदाहरण के लिए, एआर एंकरिंग से उन जगहों के मालिकों को समस्या हो सकती है जिन पर पाबंदी लगी होती है, जैसे कि सेना का बेस या निजी संपत्ति) के लिए ज़िम्मेदार होना चाहिए.
- आपत्तिजनक यूजीसी और उपयोगकर्ताओं की शिकायत करने के लिए, इन-ऐप्लिकेशन सिस्टम की सुविधा देता हो. साथ ही, यूजीसी और/या उपयोगकर्ता के सही न होने पर, उसके ख़िलाफ़ कार्रवाई करता हो;
- यूजीसी और उपयोगकर्ताओं को ब्लॉक करने के लिए, इन-ऐप्लिकेशन सिस्टम की सुविधा देता हो;
- 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 ऐसे कॉन्टेंट की सुविधा दी जाती हो जो सेक्शुअल न हो और (2) जो खास तौर पर, न तो सेक्शुअल कॉन्टेंट का प्रचार करता हो या न ही उसका सुझाव देता हो, तो उसे "इंसिडेंटल" कॉन्टेंट माना जाता है. लागू होने वाले कानून के मुताबिक, सेक्शुअल कॉन्टेंट गैरकानूनी 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, अगर नीचे बताई गई इन सभी ज़रूरी शर्तों का पालन होता है:

- ऐसे कॉन्टेंट को डिफ़ॉल्ट रूप से, फ़िल्टर की मदद से छिपाया जाता है. इसे पूरी तरह से बंद करने के लिए, उपयोगकर्ताओं की कम से कम दो कार्रवाइयों की ज़रूरत होती है (उदाहरण के लिए, "सुरक्षित खोज" की सुविधा बंद न होने पर, डिफ़ॉल्ट रूप से, पेज पर अचानक दिखने वाले कॉन्टेंट को अस्पष्ट करने या उसे दिखने से रोकने वाले फ़िल्टर की मदद से).
- परिवार की नीति के मुताबिक, बच्चों को एज स्क्रीनिंग सिस्टम की मदद से, आपके ऐप्लिकेशन का इस्तेमाल करने पर पाबंदी हो. इसमें, न्यूट्रल एज स्क्रीन या लागू कानून के मुताबिक सही बताया गया सिस्टम शामिल है**.**
- आपका ऐप्लिकेशन, कॉन्टेंट रेटिंग की नीति के मुताबिक, यूजीसी की कॉन्टेंट रेटिंग से जुड़े सवालों 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.

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.

- 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.

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.

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.

- 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.

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.

- 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.

COVID-19 से जुड़ी पाबंदियां

सभी ऐप्लिकेशन को कोरोना वायरस बीमारी 2019 (COVID-19) से संबंधित ऐप्लिकेशन के लिए बने लेख में दर्ज ज़रूरी शर्तों का पालन करना होगा.

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.

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.

बौद्धिक संपत्ति

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

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

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

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

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

कॉपीराइट वाले कॉन्टेंट का बिना मंज़ूरी इस्तेमाल करना

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

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

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

- संगीत एल्बम, वीडियो गेम, और किताबों के लिए कवर आर्ट.
- फ़िल्मों, टेलीविजन या वीडियो गेम की मार्केटिंग इमेज.
- कॉमिक बुक, कार्टून, फ़िल्मों, संगीत वीडियो या टेलीविज़न के आर्टवर्क या इमेज.

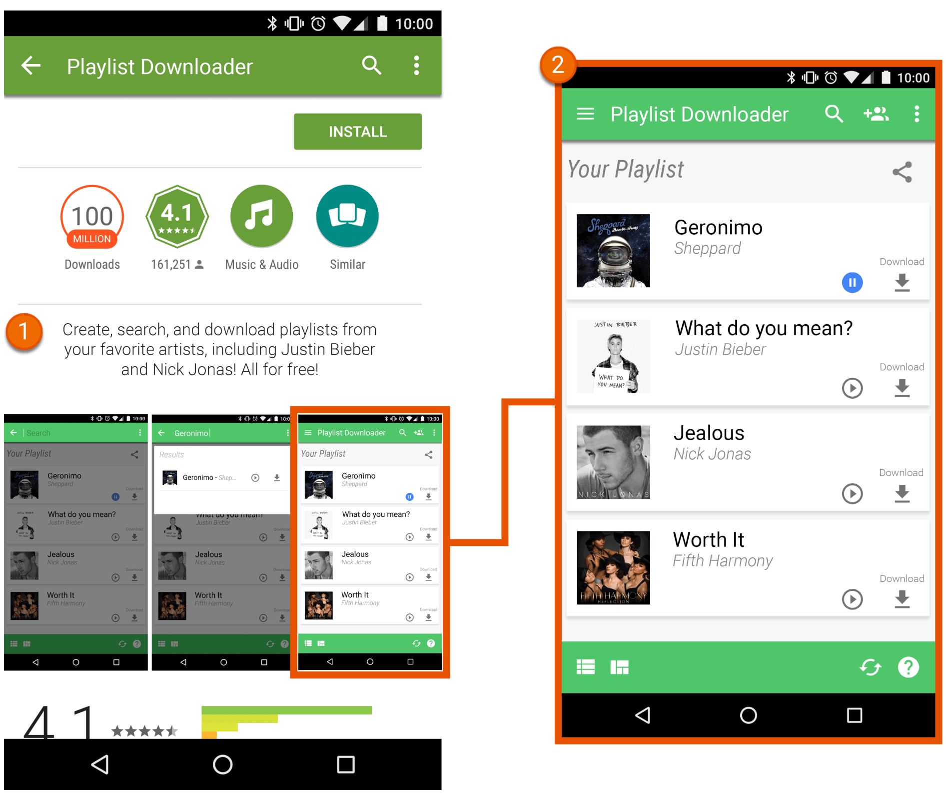
- कॉलेज और पेशेवर खेल टीम के लोगो.
- किसी लोकप्रिय हस्ती के सोशल मीडिया खाते से ली गई फ़ोटो.
- लोकप्रिय हस्तियों की पेशेवर फ़ोटो.
- कॉपीराइट के तहत आने वाला ऐसा रीप्रोडक्शन या “फ़ैन-आर्ट” जिसे मूल काम से अलग न किया जा सकता हो.
- वे ऐप्लिकेशन जिनमें ऐसे साउंडबोर्ड होते हैं जो कॉपीराइट वाले कॉन्टेंट की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

कॉपीराइट के उल्लंघन को बढ़ावा देना

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

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

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



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

ट्रेडमार्क का उल्लंघन करना

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

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

नकली

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

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

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के डेटा को किस तरह मैनेज किया जाता है, इस बारे में आपको साफ़ तौर पर बताना चाहिए. इसमें ऐप्लिकेशन इस्तेमाल करने वाले किसी व्यक्ति से इकट्ठा की गई या उसके बारे में जानकारी के अलावा, डिवाइस की जानकारी भी शामिल है. इसका मतलब है कि आपके ऐप्लिकेशन का ऐक्सेस, डेटा को इकट्ठा करने, इस्तेमाल करने, और उसे शेयर करने की जानकारी देना. साथ ही, डेटा का इस्तेमाल सिर्फ़ बताए गए उद्देश्यों के लिए करना. इसके अलावा, अगर आपका ऐप्लिकेशन उपयोगकर्ता का निजी या संवेदनशील डेटा मैनेज करता है, तो कृपया नीचे "उपयोगकर्ता की निजी और संवेदनशील जानकारी" सेक्शन में बताई गई अन्य ज़रूरी शर्तों को भी देखें. Google Play की ये ज़रूरी शर्तें, निजता और डेटा सुरक्षा के लागू कानूनों में बताई गई ज़रूरी शर्तों से अलग हैं. अगर आप अपने ऐप्लिकेशन में तीसरे पक्ष का कोड (उदाहरण के लिए, SDK टूल) शामिल करते हैं, तो यह पक्का करना होगा कि आपके ऐप्लिकेशन में इस्तेमाल किया गया तीसरे पक्ष का कोड, Google Play की डेवलपर कार्यक्रम की पॉलिसी (Google Play डेवलपर प्रोग्राम पॉलिसी) के मुताबिक हो.

उपयोगकर्ता का निजी और संवेदनशील डेटा

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति 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, Health Connect से मिला डेटा, डिवाइस पर मौजूद अन्य ऐप्लिकेशन की इन्वेंट्री, माइक्रोफ़ोन, कैमरा, और अन्य संवेदनशील डिवाइस या 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:

- उपयोगकर्ता के निजी और संवेदनशील डेटा को ऐक्सेस, इकट्ठा, इस्तेमाल, और शेयर सिर्फ़ ऐप्लिकेशन की सुविधाएं देने और उन्हें बेहतर बनाने के लिए किया जाना चाहिए. उदाहरण के लिए, ऐप्लिकेशन को उपयोगकर्ता की उम्मीद के हिसाब से वैसा ही काम करना चाहिए जैसा कि Google Play पर ऐप्लिकेशन के ब्यौरे और उससे जुड़े दस्तावेज़ों में बताया गया है. साथ ही, इसमें उपयोगकर्ता का निजी और संवेदनशील डेटा शेयर करने में SDK टूल या तीसरे पक्ष की सेवाओं का इस्तेमाल करना भी शामिल है. इस वजह से डेटा, तीसरे पक्ष को ट्रांसफ़र हो सकता है. ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने के लिए उपयोगकर्ता के निजी और संवेदनशील डेटा का इस्तेमाल करते हैं उन्हें हमारी विज्ञापन नीति का पालन करना होगा.
- उपयोगकर्ता के 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.

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

जिन मामलों में उपयोगकर्ताओं का निजी और संवेदनशील डेटा, आपके ऐप्लिकेशन में नीति का पालन करने वाली सुविधाओं या काम करने के तरीके में सुधार करने के लिए ज़रूरी न हो (जैसे कि ऐप्लिकेशन के बैकग्राउंड में डेटा इकट्ठा किया जाना), आपको नीचे बताई गई ज़रूरी शर्तों को पूरा करना होगा:

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

- ऐप्लिकेशन के अंदर होनी चाहिए, न कि सिर्फ़ ऐप्लिकेशन के ब्यौरे में या किसी वेबसाइट पर;
- ऐप्लिकेशन के सामान्य इस्तेमाल के दौरान 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.

ऐप्लिकेशन में दी जाने वाली जानकारी के साथ, ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति लेने का अनुरोध शामिल होना चाहिए और जानकारी से ठीक पहले इसे दिखाया जाना चाहिए. साथ ही, जहां ज़रूरत हो वहां एक रनटाइम अनुमति भी होनी चाहिए. उपयोगकर्ता की सहमति के बिना किसी भी निजी और संवेदनशील जानकारी को ऐक्सेस या इकट्ठा नहीं किया जा सकेगा. सहमति के लिए ऐप्लिकेशन का अनुरोध:

- सहमति संवाद को साफ़ और सीधे तौर पर पेश किया जाना चाहिए;
- ऐसी कार्रवाई का होना ज़रूरी है जिसे ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति स्वीकार कर सके. उदाहरण के लिए, स्वीकार करने के लिए टैप करें और चेक बॉक्स पर सही का निशान लगाएं;
- जहां जानकारी दी गई है वहां से कहीं और जाने (उदाहरण के लिए, टैप करके बाहर जाना या वापस जाने वाला बटन या होम बटन दबाना) को ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति की सहमति नहीं समझा जाना चाहिए; और
- उपयोगकर्ता की सहमति लेने के लिए, अपने-आप खारिज या खत्म होने वाले मैसेज का इस्तेमाल नहीं किया जाना चाहिए.

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

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

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.

- 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 होती है जो बताती है कि डेटा का इस्तेमाल किसलिए 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 प्राइवेसी पॉलिसी, 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 प्राइवेसी पॉलिसी, 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 पॉलिसी 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 इकट्ठा करता है और पूरी तरह से इसके इस्तेमाल की जानकारी नहीं देता है. साथ ही, ऊपर दी गई ज़रूरी शर्तों के मुताबिक सहमति लेता है.

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 के लिए ज़रूरी है कि Play Console में तय की गई जगह पर निजता नीति का लिंक पोस्ट करें. इसके अलावा, ऐप्लिकेशन के अंदर भी निजता नीति का लिंक या टेक्स्ट पोस्ट करें. 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 कैसे उपयोगकर्ता के डेटा को ऐक्सेस, इकट्ठा, शेयर, और इस्तेमाल करता है. निजता लेबल 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 (PDF नहीं) पर उपलब्ध हो जो काम करता हो, जिसे सभी ऐक्सेस कर सकें, और जिसकी जियोफ़ेंसिंग नहीं की गई है. साथ ही, उसमें बदलाव नहीं किया जा सके.

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 आंकड़ों का विश्लेषण करना 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. आप संवेदनशील जानकारी को ऐक्सेस करने वाले सिर्फ़ ऐसे एपीआई या अनुमतियों के लिए अनुरोध कर सकते हैं 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. आप ऐसे एपीआई या अनुमतियों का इस्तेमाल नहीं कर सकते 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 की गई निजी या संवेदनशील जानकारी कभी भी बेची नहीं जा सकती.

संवेदनशील जानकारी को ऐक्सेस करने वाले एपीआई या अनुमतियों के लिए, ज़रूरत के मुताबिक (ज़्यादा अनुमति मांगने की सुविधा की मदद से) डेटा ऐक्सेस करने का अनुरोध करें, ताकि उपयोगकर्ता यह समझ सकें कि आपके ऐप्लिकेशन को अनुमति क्यों चाहिए. डेटा का इस्तेमाल सिर्फ़ उन मकसद के लिए करें जिनके लिए उपयोगकर्ता ने सहमति दी है. अगर आप बाद में दूसरे मकसद के लिए डेटा का

इस्तेमाल करना चाहते हैं, तो आपको उपयोगकर्ताओं से पूछना होगा और यह पक्का करना होगा कि वे डेटा के दूसरे 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:

- पाबंदी वाली अनुमति की मदद से, ऐक्सेस किए जाने वाले उपयोगकर्ता या डिवाइस के संवेदनशील डेटा को तीसरे पक्ष को ट्रांसफ़र तब ही किया जा सकता है, जब यह उस ऐप्लिकेशन की मौजूदा सुविधाएं या सेवाएं देने या उन्हें बेहतर बनाने के लिए ज़रूरी हो जिससे डेटा इकट्ठा किया गया था. आप लागू कानून का पालन करने या मर्जर, मालिकाना हक या एसेट की बिक्री के लिए भी, उपयोगकर्ताओं को कानूनी रूप से ज़रूरी सूचना देकर डेटा ट्रांसफ़र कर सकते हैं. इसके अलावा, किसी भी तरह से उपयोगकर्ता के डेटा ट्रांसफ़र करने पर पाबंदी है.
- अगर उपयोगकर्ता पाबंदी वाली अनुमति देने से मना कर देते हैं, तो उनके फ़ैसलों का सम्मान करें. साथ ही, किसी गैर 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.
- अनुमतियों का इस्तेमाल करते समय, आधिकारिक तौर पर बताए गए Android डेवलपर के लिए ऐप्लिकेशन की अनुमतियां पाने के सबसे सही तरीकों या मौजूदा पॉलिसी का उल्लंघन करना साफ़ 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 गिनती के अपवादों की अनुमति दे सकते हैं. ऐसा हम उन बेहद खास मामलों में ही कर सकते हैं जहां ऐप्लिकेशन काफ़ी दमदार या बहुत ज़रूरी सुविधा देते हों और उसे मुहैया कराने का कोई दूसरा तरीका मौजूद नहीं हो. हम दिए गए अपवादों का आकलन, उपयोगकर्ताओं 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 चाहिए.

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

ऐप्लिकेशन सिर्फ़ अनुमति मिली हुई मुख्य फ़ंक्शन की सुविधा देने के लिए अनुमति (और अनुमति से पाए हुए किसी भी डेटा) का इस्तेमाल कर सकते हैं. मुख्य फ़ंक्शन की सुविधा को ऐप्लिकेशन के खास मकसद के तौर पर बताया गया है. इसमें मुख्य सुविधाओं का एक सेट शामिल हो सकता है, जिन्हें ऐप्लिकेशन की जानकारी में खास तौर से बताया जाना चाहिए और उनका प्रचार किया जाना चाहिए. मुख्य सुविधा (सुविधाओं) के बिना ऐप्लिकेशन "अधूरा" रहता है या किसी काम का नहीं रहता. इस डेटा का ट्रांसफ़र, शेयर करना या लाइसेंस लेकर किया गया इस्तेमाल, सिर्फ़ ऐप्लिकेशन के अंदर मुख्य सुविधाओं या सेवाओं को देने के लिए होना चाहिए. इसका इस्तेमाल किसी और मकसद (जैसे दूसरे ऐप्लिकेशन या सेवाओं, विज्ञापन या मार्केटिंग 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 देखने 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 देख 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 खास 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.

- **कम से कम जानकारी देखना**: 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.

सुलभता एपीआई

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

- उपयोगकर्ता की अनुमति के बिना, उपयोगकर्ता सेटिंग में बदलाव करने या उपयोगकर्ताओं के लिए किसी ऐप्लिकेशन या सेवा को बंद करने या अनइंस्टॉल करने की सुविधा को बंद करने 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, संगठन के 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.

सुलभता 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.

सुलभता 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 सुलभता 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 सुलभता 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, सुलभता 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 के 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
- उपयोगकर्ता ऐप्लिकेशन के पैकेज को इंस्टॉल कर सके, इसकी सुविधा.

इन कामों की अनुमति है:

- वेब ब्राउजिंग या वेब खोज; या
- ऐसी कम्यूनिकेशन सेवाएं जिनमें अटैचमेंट की सुविधा काम करे; या
- फ़ाइल शेयर, ट्रांसफ़र या मैनेज करने की सुविधा; या
- एंटरप्राइज़ से जुड़े डिवाइस को मैनेज करने की सुविधा.
- बैकअप लेने और डेटा वापस पाने की सुविधा
- एक डिवाइस से दूसरे डिवाइस पर या एक फ़ोन से दूसरे फ़ोन पर डेटा भेजने की सुविधा

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, एसेट फ़ाइल में अन्य APKs को खुद से 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 प्रक्रियाएं, Google Play की डिवाइस और नेटवर्क के गलत इस्तेमाल से जुड़ी नीति के मुताबिक होनी चाहिए. साथ ही, यह भी ज़रूरी है कि उपयोगकर्ता ही इन प्रक्रियाओं को शुरू और पूरा करे.

Health Connect by Android की अनुमतियां

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. साथ ही, इस पर नीचे दी गई दूसरी ज़रूरी शर्तें भी लागू होती हैं:

Health Connect को ऐक्सेस करने और इस्तेमाल करने का सही तरीका

Health Connect की मदद से डेटा ऐक्सेस करने के अनुरोध, आसान और साफ़ तौर पर समझ में आने वाले होने चाहिए. Health Connect का इस्तेमाल, लागू होने वाली नीतियों के साथ-साथ नियमों और शर्तों के मुताबिक ही किया जा सकता है. साथ ही, इसका इस्तेमाल इस 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 ही किया जा सकता है, जब आपका ऐप्लिकेशन या सेवा, इस्तेमाल के ऐसे मामलों में शामिल हो जिनके लिए अनुमति ली जा सकती है.

Health Connect की अनुमतियों को ऐक्सेस करने के लिए, इस्तेमाल के उन मामलों के बारे में नीचे बताया गया है जिनके लिए अनुमति ली जा सकती है:

- ऐसे ऐप्लिकेशन या सेवाएं जिनकी एक या एक से ज़्यादा सुविधाओं से उपयोगकर्ता की सेहत और फ़िटनेस को फ़ायदा पहुंचता हो. इसके लिए, एक यूज़र इंटरफ़ेस उपलब्ध कराया जाता है, जिसका इस्तेमाल करके उपयोगकर्ता सीधे तौर पर अपनी शारीरिक गतिविधि **नोट कर सकते हैं, उसकी रिपोर्ट तैयार कर सकते हैं, उस पर नज़र रख सकते हैं, और/या उसका विश्लेषण कर सकते हैं**. इसके अलावा, वे नींद, मानसिक स्वास्थ्य, पोषण, सेहत से जुड़ी जानकारी, शारीरिक ब्यौरों, और/या सेहत या फ़िटनेस से जुड़े अन्य ब्यौरों और जानकारी के लिए भी ऐसा कर सकते हैं.
- ऐसे ऐप्लिकेशन या सेवाएं जिनकी एक या एक से ज़्यादा सुविधाओं से उपयोगकर्ता की सेहत और फ़िटनेस को फ़ायदा पहुंचता हो. इसके लिए, एक यूज़र इंटरफ़ेस उपलब्ध कराया जाता है, जिसका इस्तेमाल करके, उपयोगकर्ता अपनी शारीरिक गतिविधि **सेव कर सकते हैं**. इसके अलावा, वे नींद, मानसिक स्वास्थ्य, पोषण, सेहत से जुड़ी जानकारी, शारीरिक ब्यौरों, और/या सेहत या फ़िटनेस से जुड़े अन्य ब्यौरों और जानकारी के लिए भी अपने फ़ोन और/या पहने जाने वाले डिवाइस पर ऐसा 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, डेटा को सेव रखने और उसे शेयर करने का एक ऐसा प्लैटफ़ॉर्म है जिसका इस्तेमाल अलग-अलग कामों के लिए किया जा सकता है. इसकी मदद से, उपयोगकर्ता अलग-अलग स्रोतों से, सेहत और फ़िटनेस से जुड़ा डेटा इकट्ठा करके उसे चुने गए तीसरे पक्षों के साथ शेयर कर सकते हैं. हो सकता है कि यह डेटा अलग-अलग स्रोतों से लिया गया हो. ये स्रोत, उपयोगकर्ता तय करते हैं. सभी डेवलपर को इस बात का आकलन कर लेना चाहिए कि Health Connect उस मकसद के लिए सही है या नहीं जिसके लिए वे इसे इस्तेमाल करना चाहते हैं. साथ ही, उन्हें Health Connect से मिले डेटा की क्वालिटी और उसके स्रोत की भी जांच कर लेनी चाहिए. भले ही वह किसी भी मकसद के लिए इस्तेमाल किया जा रहा हो. ऐसा करना तब और ज़रूरी हो जाता है, जब इस डेटा का इस्तेमाल खास तौर पर रिसर्च, सेहत या चिकित्सा के लिए किया जा रहा हो.

- जिन ऐप्लिकेशन में Health Connect से मिले डेटा का इस्तेमाल लोगों की सेहत से जुड़ी रिसर्च के लिए किया जाता है उन्हें इसमें हिस्सा लेने वाले लोगों की सहमति लेना ज़रूरी है. अगर हिस्सा लेने वाले नाबालिग हों, तो उनके माता-पिता या अभिभावक की अनुमति लेनी होगी. इस तरह की सहमति में ये चीज़ें ज़रूर होनी चाहिए: (a) रिसर्च की प्रकृति, मकसद, और उसकी अवधि; (b) रिसर्च के तरीके, खतरे, और हिस्सा लेने वाले लोगों को मिलने वाले फ़ायदे; (c) डेटा मैनेज करने और गोपनीयता की जानकारी (तीसरे पक्षों को शेयर किए जाने की जानकारी भी शामिल है); (d) हिस्सा लेने वाले लोगों के सवालों के जवाब देने के लिए संपर्क की जानकारी; और (e) अनुबंध से बाहर निकलने की प्रक्रिया. जिन ऐप्लिकेशन में Health Connect से मिले डेटा का इस्तेमाल लोगों की सेहत से जुड़ी रिसर्च के लिए किया जाता है उन्हें किसी स्वतंत्र बोर्ड की अनुमति लेनी होगी. इस बोर्ड के मकसद ये होने चाहिए: 1) हिस्सा लेने वाले लोगों की सुरक्षा करना, उनकी सेहत का ख्याल रखना, और उनके अधिकारों की रक्षा करने के साथ-साथ 2) लोगों पर की जाने वाली रिसर्च की जांच करना, उसमें बदलाव करना, और उसे अनुमति देना. अनुरोध किए जाने पर, आपको इस अनुमति का सबूत देना होगा.
- 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 ज़रूरतों का पालन किया जा रहा हो. लेबल में 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

Health Connect का सही इस्तेमाल करने का मतलब यह है कि इसकी मदद से ऐक्सेस किए गए डेटा का इस्तेमाल करते समय इन ज़रूरी शर्तों का भी पालन किया जाना चाहिए. ये ज़रूरी शर्तें, Health Connect की मदद से मिले रॉ डेटा के लिए लागू होती हैं. इसके अलावा, ये शर्तें रॉ डेटा से इकट्ठा किए गए डेटा, पहचान से जुड़ी जानकारी हटाकर बनाए गए डेटा या रॉ डेटा से बनाए गए डेटा के लिए भी लागू होती हैं.

- Health Connect से मिले डेटा का इस्तेमाल, सिर्फ़ उन मामलों या सुविधाओं को उपलब्ध कराने या उन्हें बेहतर बनाने के लिए करें जिनके लिए इस डेटा का इस्तेमाल करने की अनुमति है. ये सुविधाएं, उस ऐप्लिकेशन के यूज़र इंटरफ़ेस की मुख्य सुविधाएं होनी चाहिए जिसके लिए अनुमति पाने का अनुरोध किया जा रहा है.
- उपयोगकर्ता का डेटा, तीसरे पक्षों को सिर्फ़ तब ट्रांसफ़र करें, जब:
  - इसका इस्तेमाल, उन मामलों या सुविधाओं को उपलब्ध कराने या उन्हें बेहतर बनाने के लिए किया जाए जिनके लिए इस डेटा का इस्तेमाल करने की अनुमति है. ये सुविधाएं, उस ऐप्लिकेशन के यूज़र इंटरफ़ेस की होनी चाहिए जिसके लिए अनुमति पाने का अनुरोध किया जा रहा है. इस डेटा को ट्रांसफ़र करने के लिए, उपयोगकर्ता की सहमति लेना भी ज़रूरी है;
  - ऐसा करना सुरक्षा के लिहाज़ से ज़रूरी हो. उदाहरण के लिए, गलत इस्तेमाल की जांच करने के लिए;
  - ऐसा करना लागू होने वाले कानूनों और/या नियमों का पालन करने के लिए ज़रूरी हो; या
  - डेवलपर की एसेट मर्ज करनी हों, हासिल करनी हों या बेचनी हों. ऐसा करने से पहले, उपयोगकर्ता की सहमति लेना ज़रूरी है.
- लोगों को उपयोगकर्ता का डेटा देखने की अनुमति सिर्फ़ तब दें, जब:
  - उपयोगकर्ता से किसी खास डेटा को दिखाने की अनुमति मिल जाए;
  - ऐसा करना सुरक्षा के लिहाज़ से ज़रूरी हो. उदाहरण के लिए, गलत इस्तेमाल की जांच करने के लिए;
  - ऐसा करना, लागू कानूनों का पालन करने के लिए ज़रूरी हो; या
  - डेटा को इकट्ठा करके, उसका इस्तेमाल निजता और अधिकार क्षेत्र से जुड़ी, लागू होने वाली अन्य कानूनी ज़रूरतों के हिसाब से अंदरूनी कार्रवाइयों के लिए किया जाए. इसमें, रॉ डेटा से तैयार किया गया डेटा भी शामिल है.

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 (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 के डेटा को 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.

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

- Health Connect का इस्तेमाल ऐसे ऐप्लिकेशन, नेटवर्क या गतिविधियों को बनाने 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 काम न करने वाले डिवाइसों या प्लैटफ़ॉर्म के बीच डेटा सिंक करते हैं.
- Health Connect को ऐसे ऐप्लिकेशन, सेवाओं या सुविधाओं के साथ नहीं जोड़ा जा सकता जिनमें सिर्फ़ बच्चों को टारगेट किया जाता हो. Health Connect को उन सेवाओं में इस्तेमाल करने की अनुमति नहीं है जो खास तौर पर बच्चों के लिए बनाई गई हैं.

आपके ऐप्लिकेशन में या आपकी वेब-सेवा या ऐप्लिकेशन से जुड़ी वेबसाइट पर एक स्टेटमेंट ज़ाहिर किया जाना ज़रूरी है. इस स्टेटमेंट में यह बताया जाना चाहिए कि Health Connect से मिले डेटा का इस्तेमाल 'सीमित इस्तेमाल से जुड़े प्रतिबंधों' के मुताबिक किया जा रहा है. उदाहरण के लिए, होमपेज पर दिया गया, किसी खास पेज या निजता नीति का लिंक. इसमें, यह लिखा होना चाहिए: "Health Connect से मिली जानकारी का इस्तेमाल, Health Connect की अनुमतियों की नीति के साथ-साथ सीमित इस्तेमाल से जुड़ी ज़रूरी शर्तों के मुताबिक किया जाएगा."

कम से कम डेटा ऐक्सेस करें

सिर्फ़ उन अनुमतियों के ऐक्सेस का अनुरोध किया जा सकता है जो आपके ऐप्लिकेशन या सेवा को लागू करने के लिए ज़रूरी हैं.

इसका मतलब है कि:

- ऐसी जानकारी को ऐक्सेस करने का अनुरोध न करें जिसकी आपको ज़रूरत नहीं है. सिर्फ़ उन अनुमतियों के ऐक्सेस का अनुरोध करें जो आपके प्रॉडक्ट की सुविधाओं या सेवाओं को लागू करने के लिए ज़रूरी हैं. अगर आपके प्रॉडक्ट को खास अनुमतियों के ऐक्सेस की ज़रूरत नहीं है, तो आपको इन अनुमतियों के ऐक्सेस का अनुरोध नहीं करना चाहिए.

साफ़ तौर पर दी गई सही सूचना और कंट्रोल

Health Connect में, सेहत और फ़िटनेस से जुड़ा डेटा मैनेज किया जाता है. इसमें, निजी और संवेदनशील जानकारी भी शामिल होती है. इसलिए, सभी ऐप्लिकेशन और सेवाओं के लिए निजता नीति ज़रूरी है. इस नीति में इस बात की पूरी जानकारी देनी होगी कि आपके ऐप्लिकेशन या सेवा में, उपयोगकर्ता के डेटा को किस तरह इकट्ठा, इस्तेमाल, और शेयर किया जाता है. इसमें उन तीसरे पक्षों की जानकारी भी शामिल होनी चाहिए जिनके साथ डेटा शेयर किया जाता है. साथ ही, यह भी बताना चाहिए कि इसे किस तरह इस्तेमाल किया जाता है, सेव किया जाता है, और सुरक्षित रखा जाता है. इसके अलावा, आपको यह भी बताना होगा कि खाता बंद किए और/या मिटाए जाने के बाद, डेटा का क्या होता है.

लागू होने वाले कानून की ज़रूरी शर्तों के अलावा, आपको इन ज़रूरी शर्तों का पालन भी करना होगा:

- आपको डेटा को ऐक्सेस करने, इकट्ठा करने, इस्तेमाल करने, और शेयर करने के बारे में जानकारी देनी होगी. इस जानकारी में:
  - उस ऐप्लिकेशन या सेवा की पहचान साफ़ तौर पर ज़ाहिर करनी होगी जिसके लिए उपयोगकर्ता के डेटा का ऐक्सेस मांगा गया है;
  - इस बारे में साफ़ और सही तौर पर बताना होगा कि किस तरह का डेटा ऐक्सेस किया जाएगा, मांगा जाएगा, और/या इकट्ठा किया जाएगा;
  - यह बताना होगा कि डेटा को इस्तेमाल और/या शेयर कैसे किया जाएगा. अगर किसी एक काम के लिए डेटा मांगा गया है और उसका इस्तेमाल किसी दूसरी जगह भी किया जाएगा, तो इस्तेमाल के इन दोनों मामलों की सूचना उपयोगकर्ताओं को देनी होगी.
- आपको उपयोगकर्ताओं की मदद के लिए एक दस्तावेज़ उपलब्ध कराना होगा. इसमें यह जानकारी होनी चाहिए कि उपयोगकर्ता आपके ऐप्लिकेशन में अपना डेटा किस तरह मैनेज कर सकते हैं और उसे कैसे मिटा सकते है.

डेटा को सुरक्षित तरीके से मैनेज करना

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 जोड़ने 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.
- विज्ञापनों में इस तरह बदलाव करना जिससे ऐप्लिकेशन की कमाई पर असर पड़े.

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.

31 जुलाई, 2023 से लागू

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.

Device and Network Abuse

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.

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.

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

- ऐसे ऐप्लिकेशन जो विज्ञापन दिखाने पर अन्य ऐप्लिकेशन को ब्लॉक कर देते हैं या फिर उसमें रुकावट डालते हैं.
- गेम में धोखाधड़ी करने वाले ऐप्लिकेशन जो अन्य ऐप्लिकेशन के गेमप्ले पर असर डालते हैं.
- ऐसे ऐप्लिकेशन जो 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 व्हाइटलिस्ट करने की मंज़ूरी 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, वे ऐसा सिर्फ़ उन ऐप्लिकेशन में कर सकते हैं जिनका मुख्य मकसद ही प्रॉक्सी सेवा देना है.
- ऐप्लिकेशन या तीसरे पक्ष के कोड (उदाहरण के लिए, SDK टूल) जो Google Play के अलावा, किसी दूसरे स्रोत से इस्तेमाल किया जा सकने वाला कोड डाउनलोड करते हैं. इस तरह के कोड में dex फ़ाइलें और नेटिव कोड शामिल हैं.
- ऐसे ऐप्लिकेशन जो इस्तेमाल करने वाले व्यक्ति की अनुमति के बिना, दूसरे ऐप्लिकेशन को डिवाइस में इंस्टॉल करते हैं.
- ऐसे ऐप्लिकेशन जो नुकसान पहुंचाने वाले सॉफ़्टवेयर से लिंक कर देते हैं या लोगों तक उन्हें पहुंचाने या इंस्टॉल करने की सुविधा देते हैं.
- 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 स्रोतों (जैसे कि गलत इंटेंट वाले यूआरएल) से मिले, बिना पुष्टि वाले

यूआरएल लोड करता है.

धोखाधड़ी वाला व्यवहार

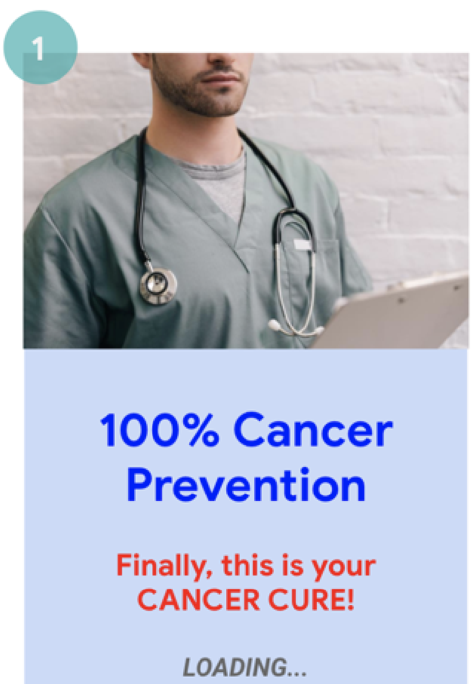
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो लोगों के साथ धोखाधड़ी करने की कोशिश करते हैं या बेईमानी करते हैं. इनमें वे ऐप्लिकेशन भी शामिल हैं जो ऐसी सुविधाएं देने का दावा करते हैं जिन्हें पूरा नहीं किया जा सकता. ऐप्लिकेशन को पूरे मेटाडेटा में अपनी सुविधाओं के बारे में सही जानकारी, ब्यौरा, और फ़ोटो/वीडियो 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.

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

- ऐसे ऐप्लिकेशन जो अपनी सुविधाओं को गलत तरीके से पेश करते हैं या सही जानकारी नहीं देते हैं:
  - ऐसा ऐप्लिकेशन जिसके ब्यौरे और स्क्रीनशॉट में रेसिंग गेम होने का दावा किया जाता है, जबकि असल में वह टाइल स्लाइड करने की पहेली वाला गेम हो, जिसके टाइल पर एक कार की तस्वीर बनी हो.
  - ऐसा ऐप्लिकेशन जो एंटी-वायरस ऐप्लिकेशन होने का दावा करता है, 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 बातें शामिल हैं.
- साफ़ तौर पर धोखाधड़ी करने वाला या गलत कॉन्टेंट वाले ऐप्लिकेशन. जिनका इस्तेमाल मतदान की प्रक्रिया में दखल देने के लिए हो सकता है.
- ऐसे ऐप्लिकेशन जो सरकार की किसी इकाई से जुड़े होने का झूठा दावा करते हैं या ऐसी सरकारी सेवाएं देने का दावा करते हैं जिनकी उन्हें अनुमति नहीं है.
- ऐसे ऐप्लिकेशन जो 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 स्वास्थ्य 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.

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

- ऐसे ऐप्लिकेशन जो 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

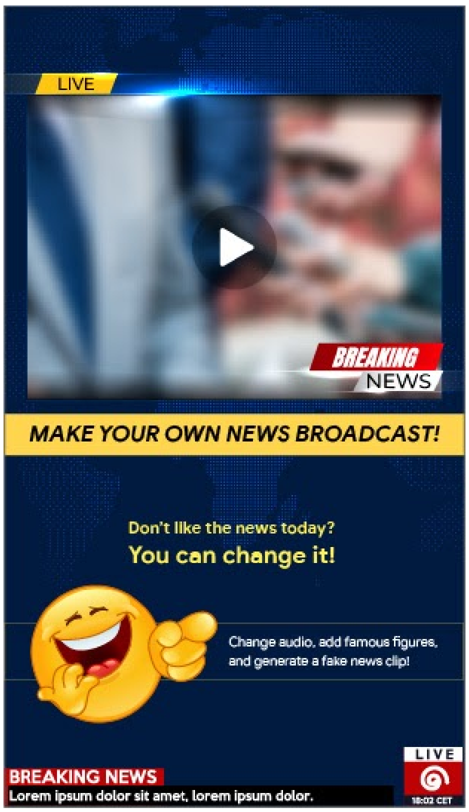
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते हैं जो गुमराह करने वाली जानकारी का प्रचार करते हैं या इसे बनाने में मदद करते हैं. ये ऐप्लिकेशन तस्वीरों वीडियो और/या टेक्स्ट से गुमराह करने वाले दावे करते हैं या जानकारी का प्रचार करते हैं. हम ऐसे ऐप्लिकेशन को

अनुमति नहीं देते हैं जो हमेशा गुमराह करने वाली जानकारी का प्रचार करते हैं या ऐसी तस्वीरों, वीडियो और/या टेक्स्ट का प्रचार करते हैं जो धोखाधड़ी को बढ़ावा देते है. इनकी वजह से संवेदनशील कार्यक्रम, राजनीतिक, सामाजिक या दूसरे सार्वजनिक मामलों को नुकसान पहुंच सकता है.

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

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

- 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.

Misrepresentation

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. इन ज़रूरी शर्तों 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 खास एपीआई लेवल को टारगेट नहीं करते वे उन नए उपयोगकर्ताओं के लिए उपलब्ध नहीं होंगे जिनके डिवाइस Android ओएस के नए वर्शन पर काम करते हैं. जो उपयोगकर्ता पहले ही Google Play से ऐप्लिकेशन इंस्टॉल कर चुके हैं वे Android ओएस के ऐसे किसी भी वर्शन पर ऐप्लिकेशन को खोजने के साथ-साथ उसे फिर से इंस्टॉल और इस्तेमाल भी कर पाएंगे 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 की पूरी जानकारी के लिए, कृपया सहायता केंद्र के लेख पर जाएं.

Malware

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 स्टोर' 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.

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.

15 फरवरी, 2023 से लागू

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.

सेवा में रुकावट (DoS)

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

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

गलत तरीके से डाउनलोड करने वाले मैलवेयर

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

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

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

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

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

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

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

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

फ़िशिंग

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

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

खास अधिकारों का गलत इस्तेमाल

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

उदाहरणों में ये शामिल हैं:

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

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

रैंसमवेयर

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

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

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

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

रूट किया जा रहा है

ऐसा कोड जो डिवाइस को रूट करता है.

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

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

स्पैम

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

स्पायवेयर

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

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

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

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

ट्रोजन

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

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

असामान्य ऐप्लिकेशन पर नोट

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

बैकडोर वाले मैलवेयर पर नोट

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

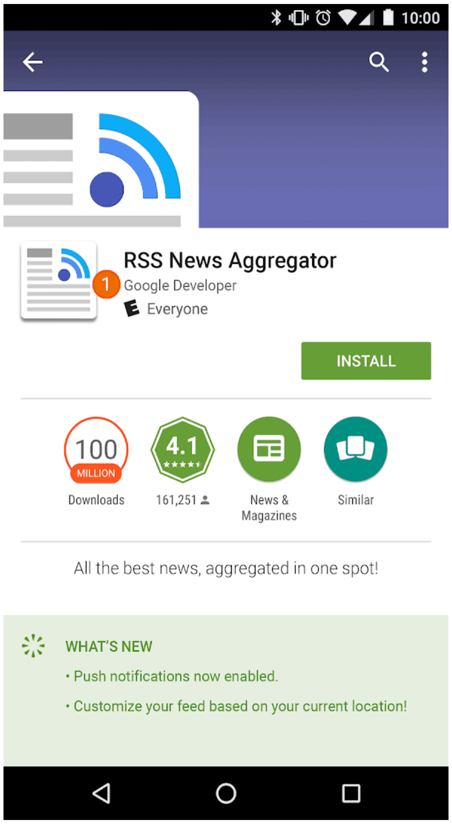
हालांकि, अगर कोई ऐप्लिकेशन आर्बिट्रेरी कोड को कार्रवाई करने की अनुमति देता है और हमें लगता है कि इस कोड की वजह से डिवाइस को नुकसान पहुंचाने वाली गतिविधि को बढ़ावा नहीं मिला है, तो उस ऐप्लिकेशन को बैकडोर मैलवेयर के तौर पर देखने के बजाय, जोखिम की संभावना वाले ऐप्लिकेशन के तौर पर देखा जाएगा. साथ ही, डेवलपर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

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.

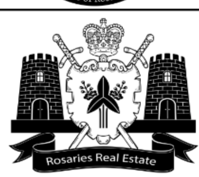
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- ऐसे डेवलपर जो किसी अन्य 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.

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.

Mobile Unwanted Software

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 की सुरक्षा करना

ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति के निजी और संवेदनशील डेटा को ऐक्सेस, इस्तेमाल, इकट्ठा, और शेयर करने के बारे में साफ़ और पारदर्शी 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 रखनी चाहिए.

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

उल्लंघनों के उदाहरण:

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

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

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

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

- ऐसा ऐप्लिकेशन जो 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.

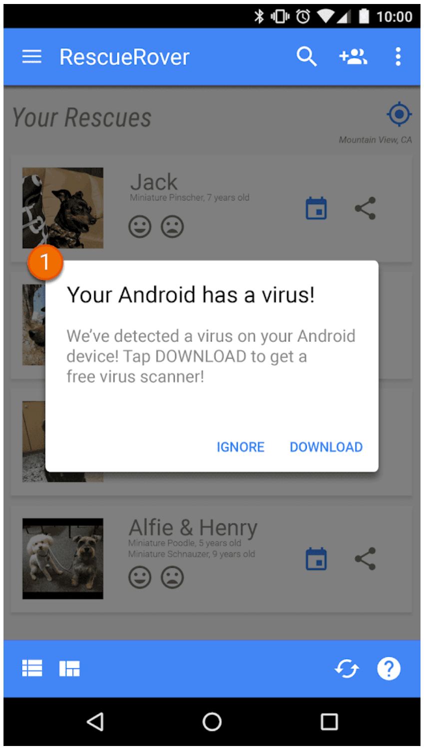
सिस्टम के काम करने के तरीके का बिना अनुमति इस्तेमाल करना या उसकी नकल करना

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.

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

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



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

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

Social Engineering

We do not allow apps that pretend to be another app with the intention of deceiving users into performing actions that the user intended for the original trusted app.

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

Google Play, डेवलपर और उपयोगकर्ताओं 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. ऐसे डेवलपर जो Google Play से ऐप्लिकेशन डाउनलोड करने पर शुल्क लेते हैं, उन्हें इन लेन-देन के लिए पैसे चुकाने के तरीके के तौर पर, Google Play के बिलिंग सिस्टम का इस्तेमाल करना होगा.
2. Play पर मौजूद उन ऐप्लिकेशन को, लेन-देन के लिए Google Play के बिलिंग सिस्टम का इस्तेमाल करना होगा जिनमें इन-ऐप्लिकेशन सुविधाओं या सेवाओं को ऐक्सेस करने के लिए पैसे चुकाने पड़ते हैं. इनमें, किसी भी ऐप्लिकेशन की मुख्य सुविधाएं और

उनके काम करने का तरीका, डिजिटल कॉन्टेंट या डिजिटल सामान शामिल हैं. इनके कलेक्शन को "इन-ऐप्लिकेशन खरीदारी" कहते हैं. ऐसा तब किया जाता है, जब सेक्शन 3 या सेक्शन 8 लागू न हो.

> ऐप्लिकेशन की ऐसी सुविधाओं या सेवाओं के उदाहरण जिनके लिए Google Play के बिलिंग सिस्टम का इस्तेमाल करने की ज़रूरत पड़ती है, उनमें इन-ऐप्लिकेशन खरीदारी के अलावा, ये चीज़ें भी 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 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 बिल, जैसे कि केबल और दूरसंचार सेवाओं के लिए चुकाए गए पैसे;
   b. पैसे चुकाने में, पीयर-टू-पीयर पेमेंट, ऑनलाइन नीलामी, और बिना टैक्स वाले दान शामिल हैं;
   c. ऐसे कॉन्टेंट या सेवाओं के लिए पैसे चुकाना जो ऑनलाइन जुए से जुड़ी सुविधाएं देते हैं, जैसा कि असली पैसों के इनाम वाला जुआ, गेम, और प्रतियोगिताएं नीति के जुए से जुड़े ऐप्लिकेशन वाले सेक्शन में बताया गया है;
   d. किसी ऐसी प्रॉडक्ट कैटगरी के लिए पैसे नहीं चुकाए जा सकते जो Google के पेमेंट सेंटर से जुड़ी कॉन्टेंट की नीति के तहत गलत मानी जाती है.

> 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 Google Pay डेवलपर पेज पर जाएं.

4. सेक्शन 3 और सेक्शन 8 में बताई गई शर्तों के अलावा, ऐप्लिकेशन अपने उपयोगकर्ताओं को Google Play के बिलिंग सिस्टम के बजाय पैसे चुकाने के किसी अन्य तरीके पर नहीं ले जा सकते. इस पाबंदी में, नीचे दिए गए तरीकों से उपयोगकर्ताओं को पैसे चुकाने के अन्य तरीकों पर ले जाना भी शामिल है (इनमें और तरीके भी शामिल हो सकते हैं):
   - Google Play में ऐप्लिकेशन की लिस्टिंग;
   - खरीदे जा सकने वाले कॉन्टेंट का ऐप्लिकेशन में प्रमोशन;
   - इन-ऐप्लिकेशन वेबव्यू, बटन, लिंक, मैसेज सेवा, विज्ञापन या दूसरे कॉल-टू-ऐक्शन; और
   - इन-ऐप्लिकेशन यूज़र इंटरफ़ेस फ़्लो के साथ खाता बनाने या साइन-अप वाले फ़्लो भी शामिल हैं. ये फ्लो, लोगों को Google Play के बिलिंग सिस्टम के अलावा, ऐप्लिकेशन से लोगों को पैसे चुकाने के किसी दूसरे तरीके पर ले जाते हैं.
5. इन-ऐप्लिकेशन वर्चुअल करंसी का इस्तेमाल, सिर्फ़ ऐसे ऐप्लिकेशन या गेम के शीर्षक 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, कोई भी इन-ऐप्लिकेशन सुविधाओं या खरीदारी के लिए ऑफ़र की जा रही सदस्यताओं के बारे में भी साफ़ और सही जानकारी देनी चाहिए. इन-ऐप्लिकेशन कीमत को, उपयोगकर्ता के Play Billing इंटरफ़ेस में दिख रही कीमत से मेल खाना 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 अन्य 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, किसी खरीदारी के दौरान लोगों को किसी भी क्रम में लगने वाले वर्चुअल आइटम खरीदने के मौके देते हैं. इसमें “लूट बॉक्स” के अलावा और भी चीज़ें शामिल हो सकती हैं. इन ऐप्लिकेशन को खरीदारी से पहले ही साफ़ तौर पर बताना होगा कि उन आइटम को हासिल करने की संभावना कितनी है. साथ ही, यह भी बताना होगा कि लोग उन आइटम को पाने के कितने करीब हैं.
8. जब तक सेक्शन 3 में बताई गई शर्तें लागू नहीं होती, तब तक Play पर उपलब्ध, मोबाइल फ़ोन और टैबलेट के लिए मौजूद ऐप्लिकेशन के ऐसे डेवलपर जो दक्षिण कोरिया में इन-ऐप्लिकेशन खरीदारी के ऐक्सेस के लिए उपयोगकर्ताओं से पेमेंट लेते या स्वीकार करते हैं वे इन लेन-देन के लिए उपयोगकर्ताओं को Google Play के बिलिंग सिस्टम के अलावा, इन-ऐप्लिकेशन बिलिंग

सिस्टम की सुविधा दे सकते हैं. इसके लिए, उपयोगकर्ताओं को एक से ज़्यादा इन-ऐप बिलिंग सिस्टम के लिए एलान वाला फ़ॉर्म भरना होगा और उसमें शामिल अन्य शर्तों और कार्यक्रम की ज़रूरतों के लिए सहमति देनी होगी.

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

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

हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जिनमें गुमराह या परेशान करने वाले विज्ञापन शामिल होते हैं. विज्ञापन सिर्फ़ उस ऐप्लिकेशन में दिखाए जाने चाहिए जिसमें वे उपलब्ध कराए जा रहे हैं. आपके ऐप्लिकेशन में दिखाए जाने वाले विज्ञापन और उनसे जुड़े ऑफ़र को हम आपके ऐप्लिकेशन का हिस्सा मानते हैं. आपके ऐप्लिकेशन में दिखाए जाने वाले विज्ञापन, हमारी सभी पॉलिसी के मुताबिक होने चाहिए. जुए के विज्ञापनों से जुड़ी पॉलिसी के लिए, कृपया यहां क्लिक करें.

विज्ञापनों के लिए जगह की जानकारी के डेटा का इस्तेमाल

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

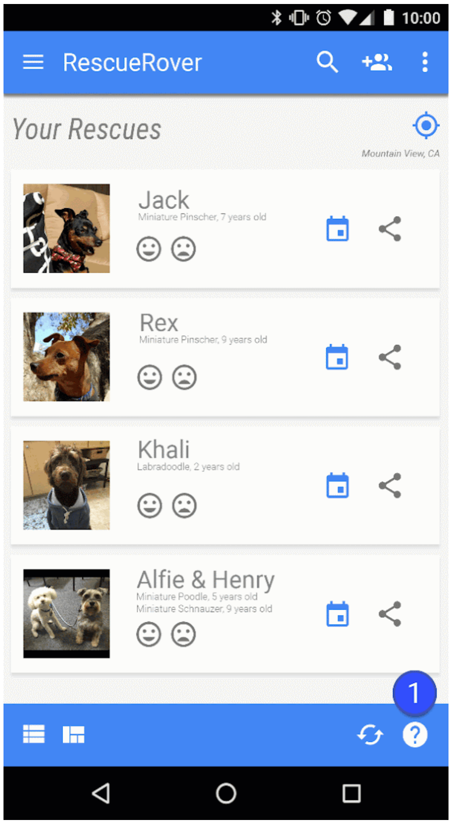
- ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को ठीक से पता होना चाहिए कि विज्ञापन दिखाने के लिए, अनुमति मांगकर डिवाइस की जगह की जानकारी का डेटा क्यों लिया जाता है या उसका इस्तेमाल किस तरह किया जाता है. साथ ही, यह जानकारी ऐप्लिकेशन की ज़रूरी प्राइवेसी पॉलिसी में दस्तावेज़ के रूप में दर्ज होनी चाहिए. इसके अलावा, किसी ऐसे काम के विज्ञापन नेटवर्क की प्राइवेसी पॉलिसी का उदाहरण दिया जाना चाहिए जिसमें जगह की जानकारी के डेटा के इस्तेमाल के बारे में बताया गया हो.
- जगह की जानकारी के ऐक्सेस की ज़रूरतों के मुताबिक, जगह की जानकारी की अनुमति ऐप्लिकेशन में मौजूदा सुविधाओं और सेवाओं को लागू करने के लिए मांगी जा सकती है, लेकिन सिर्फ़ विज्ञापनों के लिए नहीं.

धोखाधड़ी करने वाले विज्ञापन

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

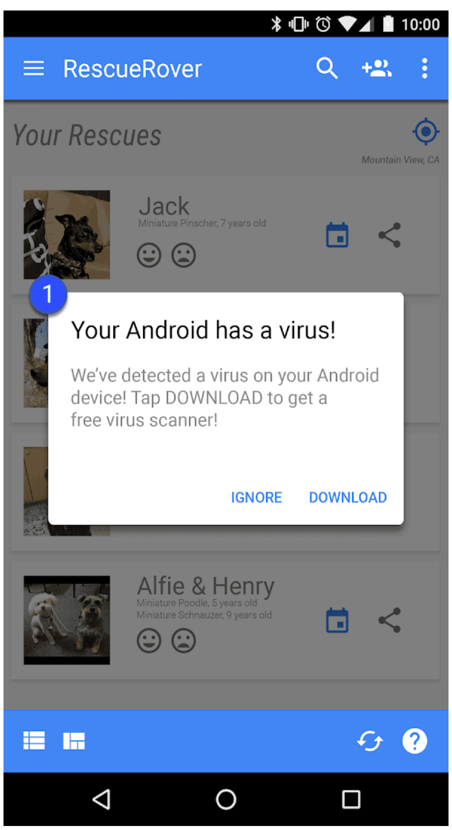
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

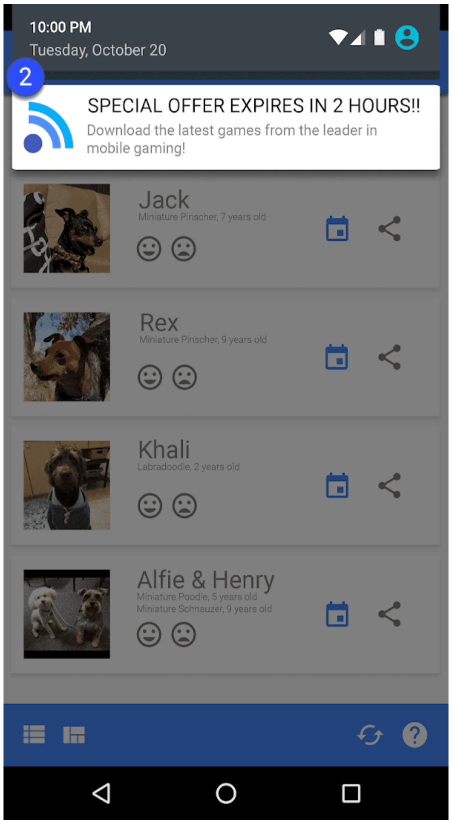
- ऐसे विज्ञापन जो किसी ऐप्लिकेशन के यूज़र इंटरफ़ेस (यूआई) की नकल करते हैं:



① इस ऐप्लिकेशन में दिया गया प्रश्नवाचक चिह्न का आइकॉन एक ऐसा विज्ञापन है जो ऐप्लिकेशन इस्तेमाल करने वाले व्यक्ति को किसी बाहरी लैंडिंग पेज पर ले जाता है.

- ऐसे विज्ञापन जो सिस्टम सूचना की नकल करते हैं:





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

लॉकस्क्रीन पर कमाई कराने की सुविधा

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

परेशान करने वाले विज्ञापन

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

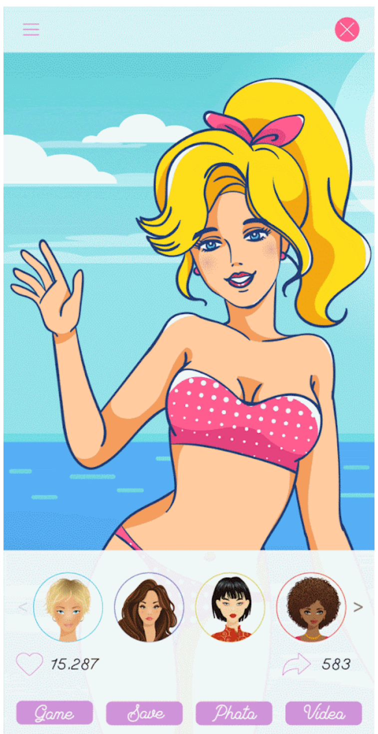
आपका ऐप्लिकेशन, विज्ञापन के मकसद से उपयोगकर्ता को तब तक किसी विज्ञापन पर क्लिक करने या अपनी निजी जानकारी देने के लिए मजबूर नहीं कर सकता, जब तक वह ऐप्लिकेशन को पूरी तरह से इस्तेमाल नहीं करता है. साथ ही, पेज पर अचानक दिखने वाले विज्ञापन सिर्फ़ उसी ऐप्लिकेशन में दिखाए जा सकते हैं जिसमें वे मौजूद हैं. अगर आपका ऐप्लिकेशन पेज पर अचानक दिखने वाले विज्ञापन या ऐसे दूसरे विज्ञापन दिखाता है जो सामान्य इस्तेमाल में रुकावट डालते हैं, तो उन्हें ऐसा होना चाहिए कि बिना किसी पेनल्टी के आसानी से खारिज किया जा सके.

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

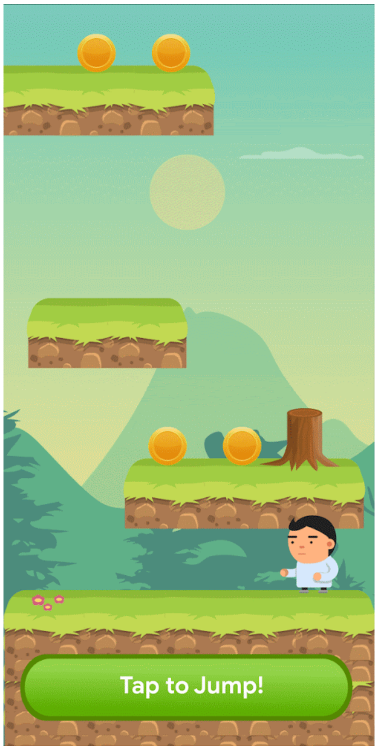
- ऐसे विज्ञापन जो पूरी स्क्रीन घेरते हैं या ऐप्लिकेशन इस्तेमाल करने में रुकावट डालते हैं और जिन्हें बंद करने का सही तरीका मालूम नहीं होता है:

① इस विज्ञापन को बंद करने का कोई बटन नहीं है.

- ऐसे विज्ञापन जो इस्तेमाल करने वाले व्यक्ति को इसे बंद करने के लिए गलत बटन पर क्लिक करने के लिए मजबूर करते हैं या ऐसी जगहों पर अचानक विज्ञापन दिखाते हैं जहां उपयोगकर्ता आम तौर पर दूसरी सुविधा के लिए टैप करता हो.



- ऐसा विज्ञापन जो खुद को बंद करने के लिए गलत बटन दिखाता हो



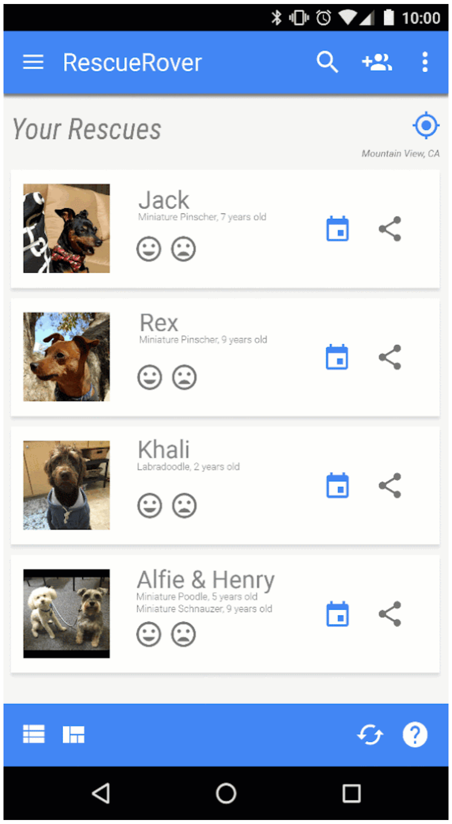
ऐसा विज्ञापन जो उस जगह पर अचानक दिखता है जहां ऐप्लिकेशन इस्तेमाल करने वाला व्यक्ति, ऐप्लिकेशन की सुविधाओं के लिए आम तौर पर टैप करता है

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

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

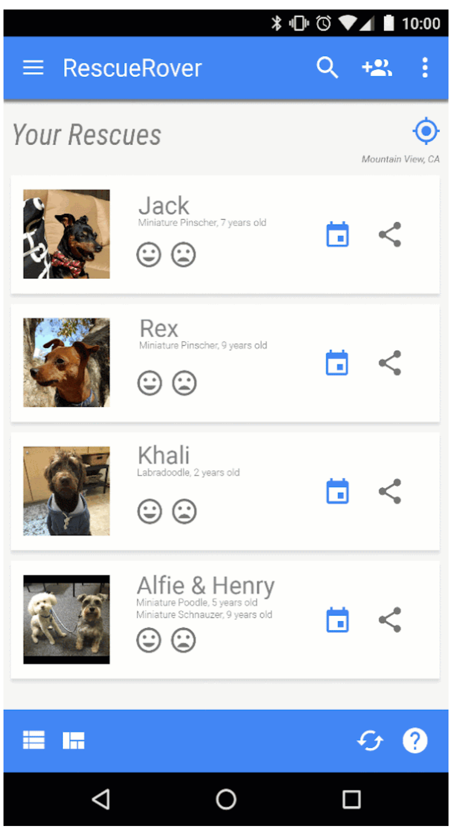
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

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



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

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

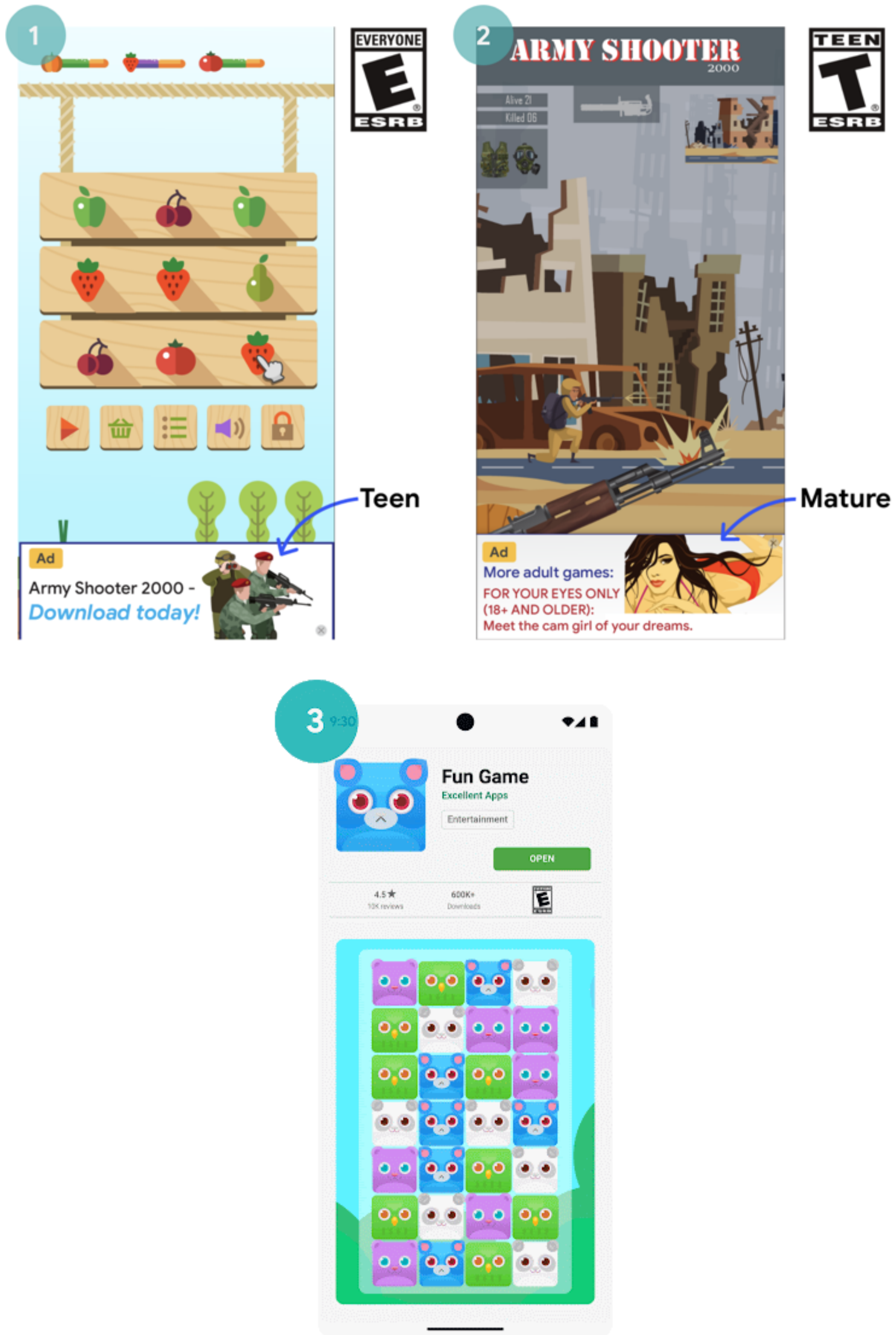


ब्यौरा: उपयोगकर्ता, ऐप्लिकेशन से बाहर निकलने और होम स्क्रीन पर जाने की कोशिश करता है, लेकिन इस तरह के विज्ञापन की वजह से ऐसा करने में रुकावट आ जाती है.

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 अन्य पॉलिसी के मुताबिक हो.

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



① यह विज्ञापन (किशोर के लिए), ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए उचित नहीं है (हर किसी के लिए)
② यह विज्ञापन (वयस्क के लिए), ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए उचित नहीं है (किशोर के लिए)
③ विज्ञापन का ऑफ़र (वयस्क वाला ऐप्लिकेशन डाउनलोड करने का प्रचार करने वाला), उस गेम ऐप्लिकेशन की कॉन्टेंट रेटिंग के लिए उचित नहीं है जिसमें विज्ञापन दिखाया जाना है (हर किसी के लिए)

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 आंकड़ों 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 ने जो चुना है उसके मुताबिक**.
  - 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.

Better Ads Experiences

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, गेम की कोई सुविधा या कॉन्टेंट का इस्तेमाल करने के बदले उपयोगकर्ता को ऑफ़र करता है. यह नीति ऐसे विज्ञापन और

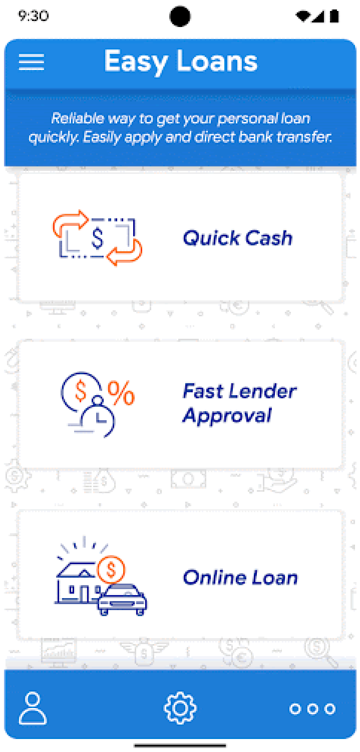
कमाई करने से जुड़े कॉन्टेंट पर भी लागू नहीं होती जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट नहीं डालता. उदाहरण के लिए, विज्ञापन से जुड़ा वीडियो कॉन्टेंट, ऐसे बैनर विज्ञापन जो पूरी स्क्रीन पर नहीं आते.

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.

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

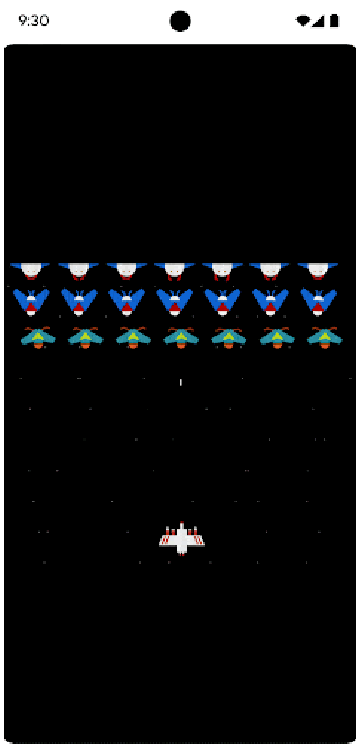
- ऐसे अनचाहे विज्ञापनों की अनुमति नहीं है जो गेम खेलने के दौरान या कॉन्टेंट वाले हिस्से के शुरू होने पर दिखते हैं. उदाहरण के लिए, किसी बटन पर उपयोगकर्ता के क्लिक करने के बाद और बटन पर क्लिक करने से होने वाली कार्रवाई से ठीक पहले. ये विज्ञापन उपयोगकर्ताओं के लिए अनचाहे होते हैं, क्योंकि उपयोगकर्ताओं को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

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.

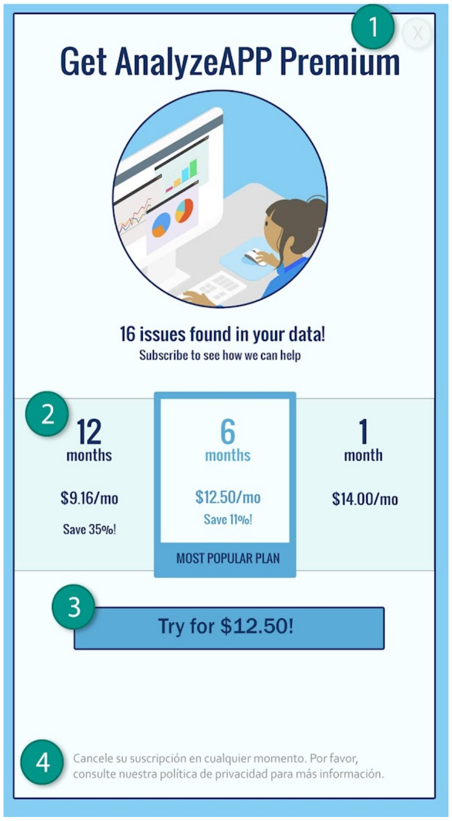
सदस्यताओं के साथ ऑफ़र किए जाने वाले फ़ायदे, सदस्यता चालू रहने के दौरान उपयोगकर्ताओं को लगातार या तय अवधि पर बार-बार देने होंगे. ऐसे फ़ायदे ऑफ़र नहीं किए जाने चाहिए जिनका इस्तेमाल उपयोगकर्ता सिर्फ़ एक बार कर सकते हों. उदाहरण के लिए, ऐसे SKUs जिनके साथ ऐप्लिकेशन के अंदर एकमुश्त क्रेडिट/मुद्रा मिलती हो 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.

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.

- 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:



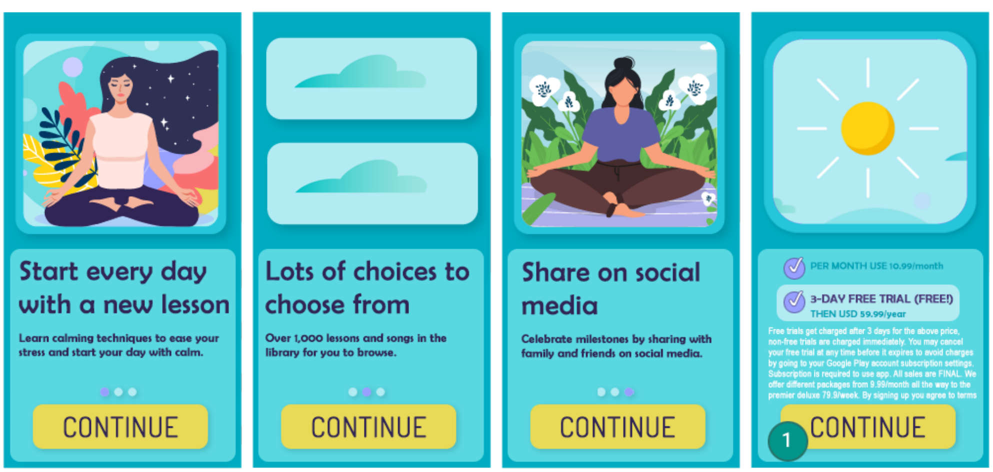
① जब 'खारिज करें' बटन साफ़ तौर पर न दिखे, जिससे लोग यह न समझ पाएं कि वे सदस्यता का ऑफ़र स्वीकार किए बिना भी ऐप्लिकेशन की सुविधाएं ऐक्सेस कर सकते हैं.

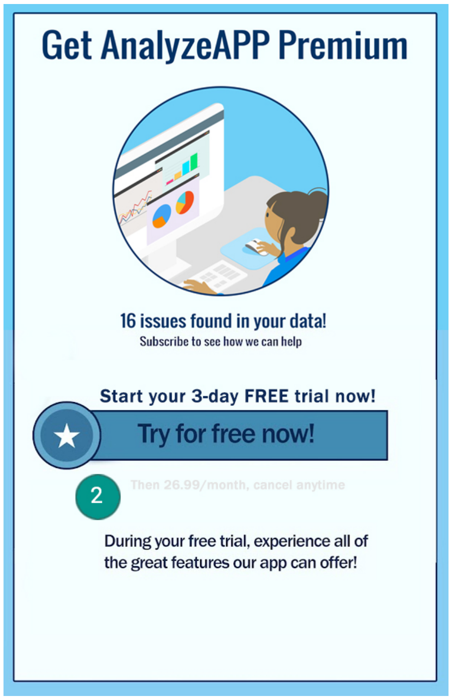
② जब सदस्यता के ऑफ़र में सिर्फ़ महीने का शुल्क दिखे, जिससे लोग यह न समझ पाएं कि सदस्यता लेते समय उनसे छह महीने का शुल्क लिया जाएगा.

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.

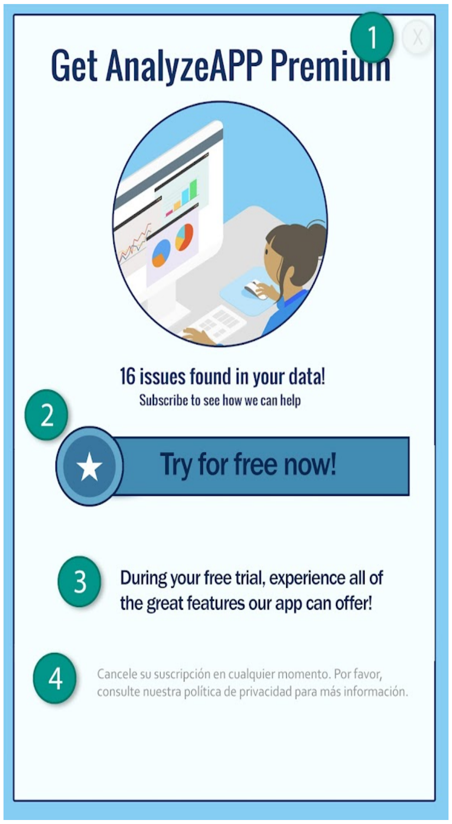
② पढ़कर यह पता लगाना मुश्किल होता है कि मुफ़्त में आज़माने की अवधि खत्म होने पर उपयोगकर्ताओं से कितनी रकम ली जाएगी. इससे, उपयोगकर्ताओं को ऐसा लग सकता है कि प्लान मुफ़्त है

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.

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

- ऐसे 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 Google Play की नीतियों के हिसाब से खुद प्रमाणित किए गए विज्ञापन SDK टूल इस्तेमाल करने होंगे. साथ ही इन्हें, विज्ञापन SDK टूल को खुद से प्रमाणित करने की नीचे दी गई ज़रूरी शर्तों के मुताबिक होना चाहिए.

अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे और वयस्क दोनों ही उपयोगकर्ता शामिल हैं, तो आपको यह पक्का करना होगा कि बच्चों को विज्ञापन दिखाने के लिए, खास तौर पर खुद से प्रमाणित किए गए इन विज्ञापन SDK टूल में से किसी का इस्तेमाल किया जाए. उदाहरण के लिए, न्यूट्रल एज स्क्रीन का तरीका इस्तेमाल करके. परिवार के लिए बनाए गए कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़ खुद से प्रमाणित किए गए विज्ञापन SDK टूल इस्तेमाल करें.

ध्यान रहे, 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. 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, Google न तो इसकी कोई ज़िम्मेदारी लेता है और न ही कोई गारंटी देता है.

परिवार के लिए बनाए गए कार्यक्रम में विज्ञापन दिखाने के लिए SDK टूल 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.

परिवार के लिए बनाए गए कार्यक्रम के लिए इस्तेमाल होने वाले, खुद से प्रमाणित किए गए विज्ञापन SDK टूल से जुड़ी ज़रूरी शर्तें

- तय करें कि किस तरह के विज्ञापन और व्यवहार आपत्तिजनक हैं. साथ ही, विज्ञापन SDK टूल की शर्तों या नीतियों के मुताबिक उन पर 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, पसंद बताने के लिए नीचे दिया गया फ़ॉर्म भरते समय देता 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 को लागू कानूनों और नियमों, जैसे कि यूएस चिल्ड्रेन्स ऑनलाइन प्राइवसी ऐंड प्रोटेक्शन ऐक्ट (कोपा) और ईयू (यूरोपीय संघ) जनरल डेटा प्रोटेक्शन रेगुलेशन (जीडीपीआर) के मुताबिक होना 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 फ़ॉर्मेट चुनने की अनुमति दें जो Google Play की परिवारों के लिए विज्ञापन और कमाई करने की नीति के मुताबिक हों और शिक्षकों की अनुमति वाले ऐप्लिकेशन के कार्यक्रम 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.
- 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: परिवार के लिए बनाए गए कार्यक्रम के लिए इस्तेमाल होने वाले खुद से प्रमाणित किए गए विज्ञापन 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.

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

- परिवार के लिए बनाए गए कार्यक्रम के लिए खुद से प्रमाणित किए गए विज्ञापन SDK टूल ही इस्तेमाल करें 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, परिवार के लिए बनाए गए कार्यक्रम के लिए इस्तेमाल होने वाले ऐसे विज्ञापन SDK टूल की सूची यहां देख सकते हैं जिन्हें खुद से प्रमाणित करना होता 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 उदाहरण नीचे दिए गए हैं:

- वेबसाइट, ऐप्लिकेशन या अन्य प्रॉपर्टी पर, धोखाधड़ी करने वाले विज्ञापनों का इस्तेमाल करना. इनमें ऐसी सूचनाएं भी शामिल हैं जो सिस्टम से मिलने वाली सूचनाओं और चेतावनियों जैसी ही होती हैं.
- अश्लील विज्ञापनों का इस्तेमाल करके, लोगों को Google Play पर अपने ऐप्लिकेशन के स्टोर पेज पर भेजना, ताकि वे ऐप्लिकेशन को डाउनलोड करें.
- प्रमोशन या इंस्टॉल कराने के ऐसे तरीके जो उपयोगकर्ताओं को Google Play पर ले जाते हैं या उपयोगकर्ताओं को कार्रवाई की सूचना दिए बिना ही ऐप्लिकेशन डाउनलोड कर देते हैं.
- एसएमएस सेवाओं का इस्तेमाल करके अनचाहा प्रचार करना.

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

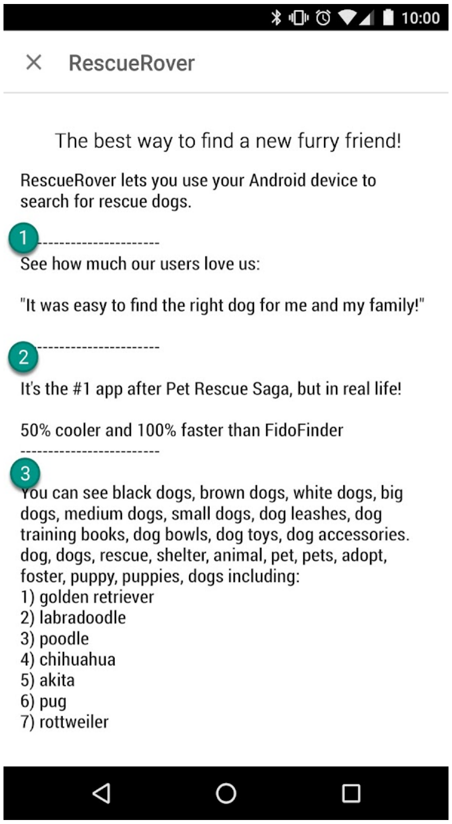
Metadata

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, शीर्षक, 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 टेस्टीमोनियल 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.

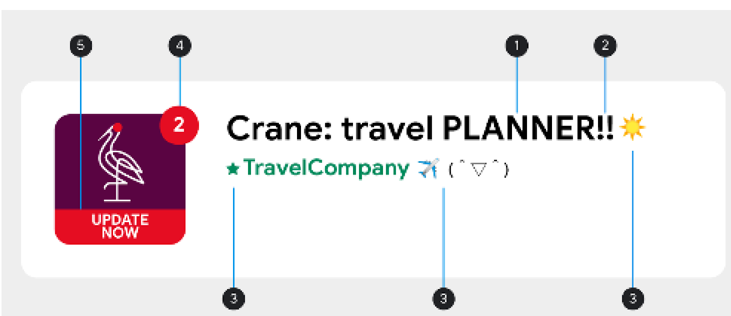
आपके ऐप्लिकेशन को खोजने और उसके बारे में जानने के लिए खास तौर पर, ऐप्लिकेशन का शीर्षक, आइकॉन, और डेवलपर के नाम उपयोगी होते हैं. इसलिए, इन मेटाडेटा में इमोजी और इमोटिकॉन का इस्तेमाल न करें. इसके अलावा, विशेष वर्णों का भी बार-बार इस्तेमाल न करें. सिर्फ़ बड़े अक्षर लिखने से बचें. ऐसा तब ही करें, जब आपके 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 शीर्षक 30 या उससे कम वर्णों का होना चाहिए.

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.

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



① बिना पहचान के या पहचान छिपाकर दिए गए उपयोगकर्ता टेस्टीमोनियल
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 विशेष वर्ण के क्रम, जो ऐप्लिकेशन के लिए किसी काम के नहीं
③ इमोजी, इमोटिकॉन (जैपनीज़ इमोटिकॉन शामिल), और विशेष वर्णों का इस्तेमाल
④ गुमराह करने वाला सिंबल
⑤ गुमराह करने वाला टेक्स्ट

आपके स्टोर पेज में मौजूद गलत टेक्स्ट, इमेज या वीडियो के कुछ उदाहरण यहां 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 शामिल हो. भले ही, उसे चित्र के तौर पर दिखाया गया हो या असल रूप में.
- ऐप्लिकेशन के स्टोर पेज पर ऐसी भाषा का इस्तेमाल करना जो किसी धर्म का अपमान करती 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 शीर्षक और विवरण, ऐप्लिकेशन के फ़ंक्शन के बारे में सही जानकारी देता हो.
- दोहराए जाने वाले या बेवजह के कीवर्ड या संदर्भों का इस्तेमाल करने से बचें.
- अपने ऐप्लिकेशन की जानकारी कम और आसान शब्दों में दें. कम शब्दों में जानकारी का मकसद, खास तौर पर छोटे डिसप्ले वाले डिवाइस पर बेहतरीन उपयोगकर्ता अनुभव देना है. हद से ज़्यादा लंबे, विवरण, गलत फ़ॉर्मैट या दोहराई जाने वाली जानकारी से, इस नीति का उल्लंघन हो सकता है.
- ध्यान रखें कि आपका स्टोर पेज, आम दर्शक के हिसाब से होना चाहिए. अपने स्टोर पेज में गलत टेक्स्ट, इमेज या वीडियो के इस्तेमाल से बचें. साथ ही, ऊपर बताए गए दिशा-निर्देशों का पालन करें.

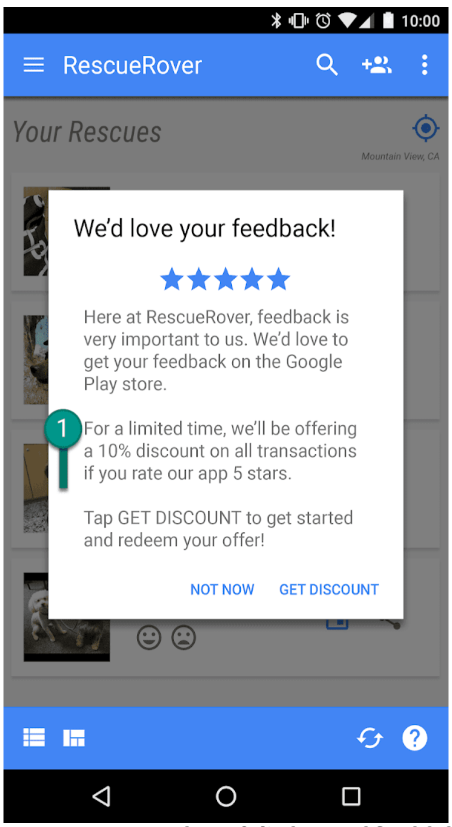
User Ratings, Reviews, and Installs

डेवलपर को Google Play में किसी भी ऐप्लिकेशन के प्लेसमेंट में बदलाव करने की कोशिश नहीं करनी चाहिए. इसमें धोखाधड़ी या कोई फ़ायदा देकर कराए गए इंस्टॉल, समीक्षाएं, और रेटिंग जैसे अवैध तरीकों से, प्रॉडक्ट रेटिंग, समीक्षाएं या इंस्टॉलेशन की संख्याओं को बढ़ाने जैसी अन्य बातें भी शामिल हैं. ऐप्लिकेशन की कीमत या प्रमोशन से जुड़ी अन्य जानकारी देने के लिए, ऐप्लिकेशन के शीर्षक, आइकॉन या डेवलपर के नाम में किसी इमेज या टेक्स्ट का इस्तेमाल किया गया है, तो उसे भी फ़ायदा देकर हासिल किए गए इंस्टॉल, समीक्षाओं, और रेटिंग में शामिल माना जाएगा.

डेवलपर को ऐप्लिकेशन के शीर्षक, आइकॉन या डेवलपर के नाम में ऐसा कोई भी टेक्स्ट या इमेज नहीं जोड़ना चाहिए जिससे स्टोर पेज की परफ़ॉर्मेंस या रैंकिंग दिखती हो या फिर मौजूदा Google Play कार्यक्रम (Google Play प्रोग्राम) से जुड़े सुझाव दिखते हों.

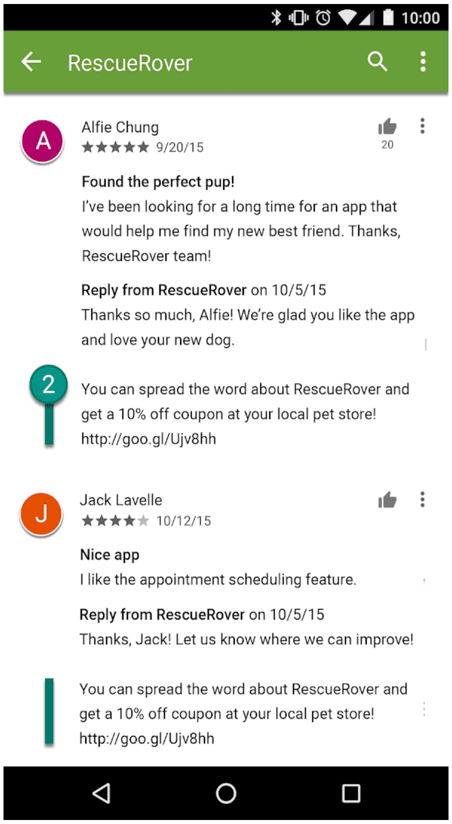
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- इंसेंटिव ऑफ़र करके, उपयोगकर्ताओ से अपने ऐप्लिकेशन को रेटिंग देने के लिए कहना:



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

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



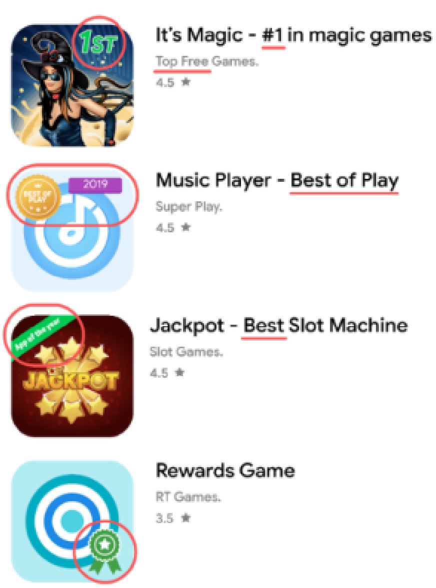
② यह समीक्षा इस्तेमाल करने वालों को एक कूपन का ऑफ़र देकर RescueRover ऐप्लिकेशन का प्रचार करने के लिए बढ़ावा देती है.

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

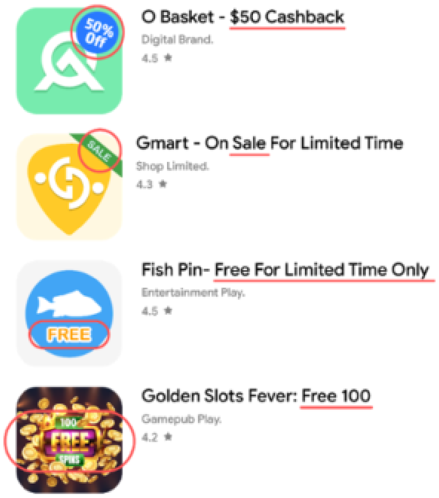
- अपने जवाब में उपयोगकर्ता की टिप्पणियों में उठाई गईं समस्याओं को हल करने पर ध्यान दें, न कि ज़्यादा रेटिंग की मांग करें.
- सहायता पता या अक्सर पूछे जाने वाले सवालों के पेज जैसे मददगार संसाधनों को शामिल करें.

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.

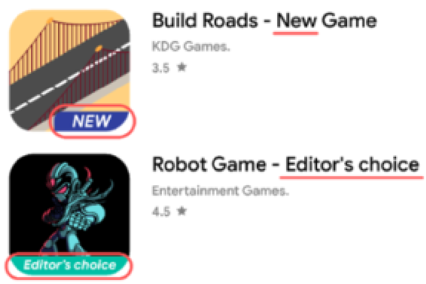
- ऐसी इमेज या टेक्स्ट जिससे स्टोर पेज की परफ़ॉर्मेंस या रैंकिंग के बारे में पता चलता हो. जैसे, 'साल का सबसे अच्छा ऐप्लिकेशन,' '#1,' 'साल 20XX में Google Play का सबसे अच्छा ऐप्लिकेशन,' 'लोकप्रिय,' अवॉर्ड आइकॉन वगैरह.



- 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 के कार्यक्रमों (Google Play प्रोग्राम) के बारे में पता चलता हो. उदाहरण के लिए, 'संपादक की पसंद,' 'नया' वगैरह.



Content Ratings

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

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

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

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

रेटिंग से जुड़ी अपील

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

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 .

Spam and Minimum Functionality

At a minimum, apps should provide users with a basic degree of functionality and a respectful user experience. Apps that crash, exhibit other behavior that is not consistent with a functional user experience, or that serve only to spam users or Google Play are not apps that expand the catalog in a meaningful way.

Spam

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.

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.

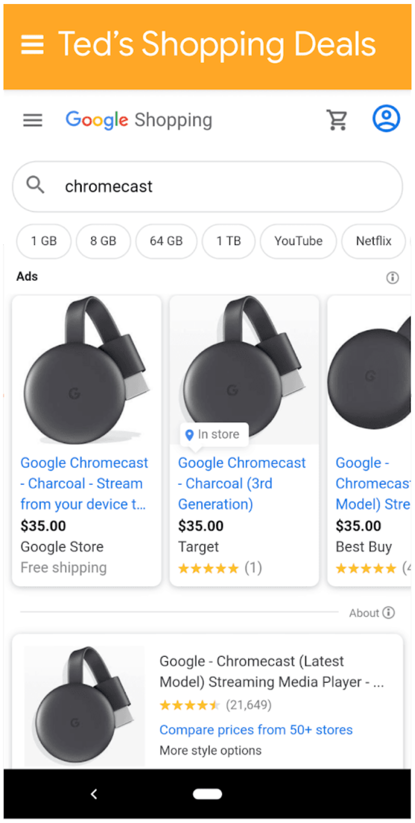
- जब उपयोगकर्ता 'शेयर करें' बटन दबाता है, तो ऐप्लिकेशन उसकी तरफ़ से मैसेज भेजता है. उपयोगकर्ता को यह सुविधा नहीं दी जाती कि मैसेज भेजे जाने से पहले वह कॉन्टेंट और पाने वाले लोगों के नाम की पुष्टि कर सके:

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.

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

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



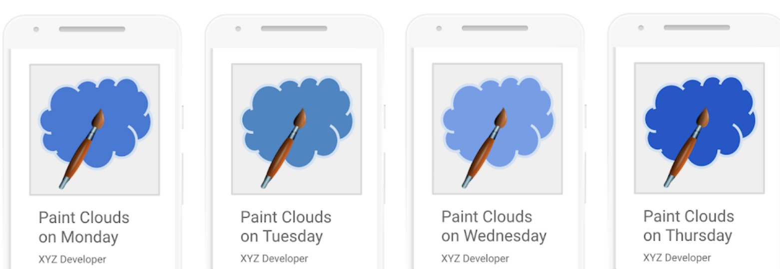
① इस ऐप्लिकेशन को "Ted's shopping Deals" कहा जाता है और यह सामान्य तौर पर Google Shopping का वेबव्यू दिखाता है.

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.

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

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

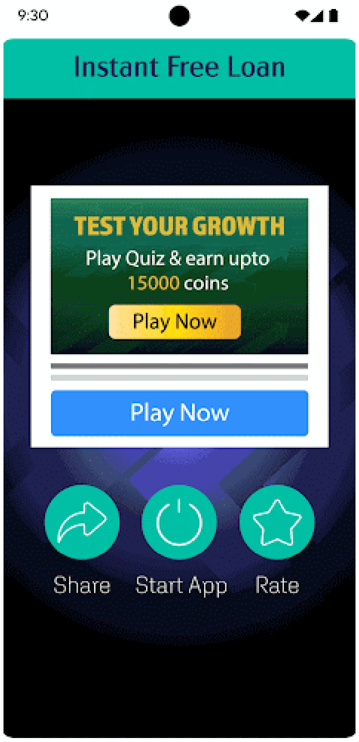


विज्ञापन के लिए बनाए गए ऐप्लिकेशन

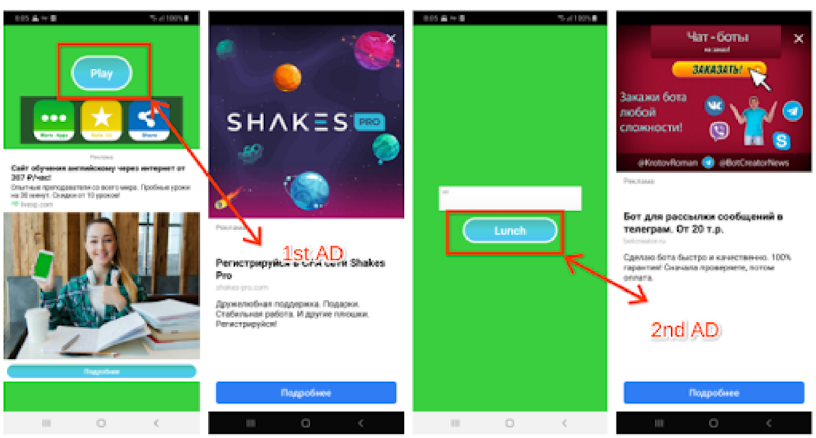
हम ऐसे ऐप्लिकेशन को अनुमति नहीं देते जो उपयोगकर्ताओं का ध्यान खींचने के लिए बार-बार उन्हें अचानक दिखने वाले (इंटरस्टीशियल) विज्ञापन दिखाते हैं. इससे, उपयोगकर्ता को ऐप्लिकेशन से इंटरैक्ट करने और ऐप्लिकेशन के अंदर कोई टास्क पूरा करने में रुकावट होती है.

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

• ऐसे ऐप्लिकेशन 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.



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.



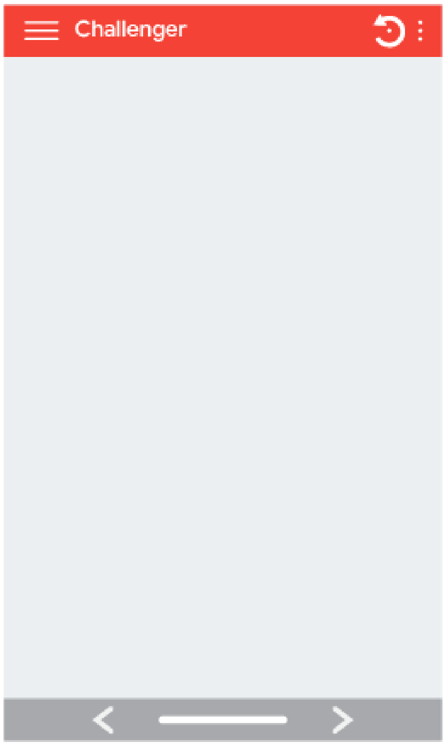
पहले पेज पर, उपयोगकर्ता को **Play** पर क्लिक करने के लिए ले जाया जाता है, क्योंकि ऐप्लिकेशन का इस्तेमाल करने के लिए सिर्फ़ यह बटन उपलब्ध होता है. जब उपयोगकर्ता उस पर क्लिक करता है, तो अचानक दिखने वाला (इंटरस्टीशियल) विज्ञापन नज़र आता है. विज्ञापन बंद होने के बाद, उपयोगकर्ता **Launch** पर क्लिक करता है,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

कम से कम सुविधाएं

पक्का करें कि आपका ऐप्लिकेशन भरोसेमंद, दिलचस्प, और बेहतर उपयोगकर्ता अनुभव देता है.

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

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



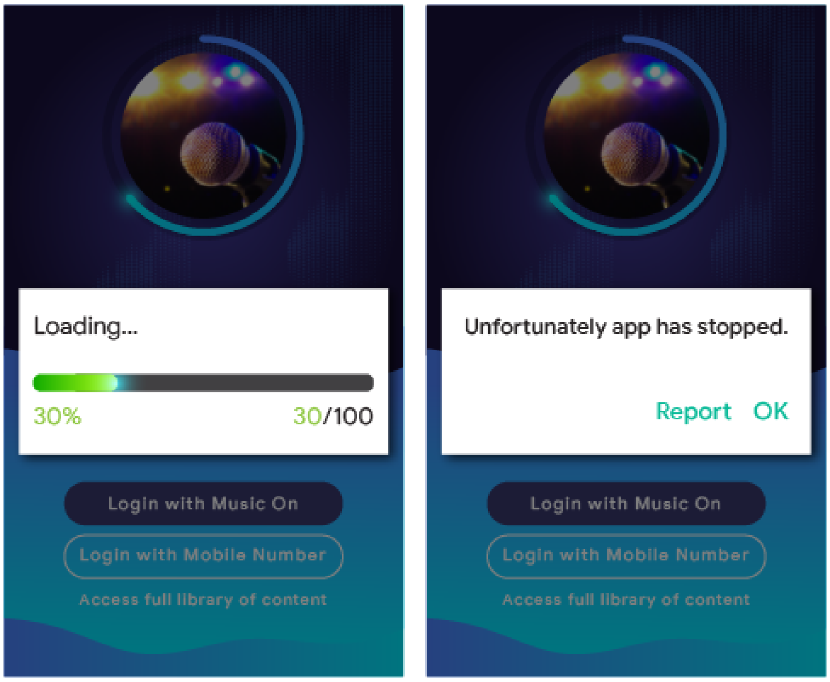
अधूरी सुविधाएं

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

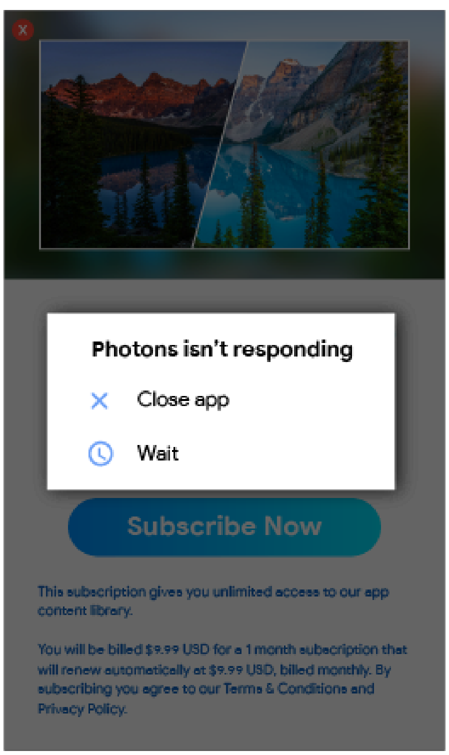
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- ऐसे ऐप्लिकेशन जो **इंस्टॉल नहीं होते**

- ऐसे ऐप्लिकेशन जो इंस्टॉल तो होते हैं, लेकिन **लोड नहीं होते**



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



Other Programs

In addition to compliance with the content policies set out elsewhere in this Policy Center, apps that are designed for other Android experiences and distributed via Google Play may also be subject to

program-specific policy requirements. Be sure to review the list below to determine if any of these policies apply to your app.

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

तकनीकी जानकारी

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

ऐप्लिकेशन इंस्टॉल करने की सुविधा का ऑफ़र देना

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

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

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

डिवाइस में बदलाव करने की स्थिति

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

ऐप्लिकेशन कैसा दिखेगा

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

डिवाइस पहचानकर्ता

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

डिवाइस पहचानकर्ता भी शामिल हो सकते हैं:

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

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

नेटवर्क ट्रैफ़िक

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

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.

नीचे दिए गए इमोजी के उदाहरणों का इस्तेमाल करके, यह पता लगाएं कि आपके ऐप्लिकेशन पर यूनिकोड का नया वर्शन काम करता है या नहीं:

उदाहरण	यूनिकोड वर्शन
🫠 🫱🏼‍🫲🏾 🫰🏽	14.0
😶‍🌫️ 🧔🏻‍♀️ 💑🏾	13.1
🥲 🥷🏿 🐻‍❄️	13.0
🧑‍🦰 🧑‍🦯 🧑‍🤝‍🧑	12.1
🦩 🦻🏿 👭	12.0

परिवार

Google Play offers a rich platform for developers to showcase their high-quality, age appropriate content for the whole family. Before submitting an app to the Designed for Families program or submitting an app that targets children to the Google Play Store, you are responsible for ensuring your app is appropriate for children and compliant with all relevant laws.

Learn about the families process and review the interactive checklist at Academy for App Success.

Designing Apps for Children and Families

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

अलग-अलग जगह-भाषा और परिस्थितियों में "बच्चे" शब्द का मतलब अलग हो सकता है. आप अपने कानूनी सलाहकार से पूछ सकते हैं कि आपके ऐप्लिकेशन पर किस तरह की कानूनी जवाबदेही और/या उम्र से 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.

परिवार के लिए बनाए गए कार्यक्रम में, खास तौर पर बच्चों के लिए बनाए गए ऐप्लिकेशन का शामिल होना ज़रूरी है. अगर आपका ऐप्लिकेशन बच्चों और बड़ों, दोनों तरह के दर्शकों को टारगेट करता है, तब भी आप परिवार के लिए बनाए गए कार्यक्रम में शामिल हो सकते हैं. जो ऐप्लिकेशन परिवार के लिए बनाए गए कार्यक्रम में ऑप्ट-इन करते हैं उन सभी को शिक्षकों से मंज़ूरी मिले ऐप्लिकेशन वाले कार्यक्रम में शामिल होने के लिए रेट किया जा सकता है. हालांकि, हम गारंटी नहीं दे सकते कि आपका ऐप्लिकेशन, शिक्षकों से मंज़ूरी मिले ऐप्लिकेशन वाले कार्यक्रम में शामिल होगा. अगर आप परिवार के लिए बनाए गए कार्यक्रम में शामिल नहीं होते हैं, तब भी आपके लिए नीचे दी गई Google Play की परिवार नीति का पालन करना ज़रूरी है. साथ ही, Google Play के डेवलपर कार्यक्रम की नीतियों और डेवलपर वितरण अनुबंध का पालन करना भी ज़रूरी है.

Play Console से जुड़ी ज़रूरी शर्तें

टारगेट ऑडियंस और कॉन्टेंट

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

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

आपको अपने ऐप्लिकेशन की टारगेट ऑडियंस के लिए एक से ज़्यादा उम्र समूह तभी चुनने चाहिए, जब आपने ऐप्लिकेशन को उन चुने हुए उम्र समूह (समूहों) के लोगों को ध्यान में रखकर बनाया हो. साथ ही, आप पक्के तौर पर यह जानते हो कि आपका ऐप्लिकेशन उनके लिए पूरी तरह सही है. उदाहरण के लिए, अगर आपका ऐप्लिकेशन बच्चों, छोटे बच्चों, और प्रीस्कूल में पढ़ने वाले बच्चों के लिए है, तो उम्र समूह टारगेट करते समय "पांच साल और उससे कम" उम्र का समूह ही चुनना चाहिए. अगर आपका ऐप्लिकेशन 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 जिसे बच्चे ऐक्सेस कर सकते हैं उसे उनकी उम्र के हिसाब से सही होना चाहिए. अगर आपके ऐप्लिकेशन में ऐसा कॉन्टेंट है जिसे पूरी दुनिया में हर जगह सही नहीं माना जाता, लेकिन वह कॉन्टेंट किसी

खास इलाके के बच्चों के लिए सही माना जाता है, तो ऐप्लिकेशन को उसी इलाके (सीमित इलाके) में उपलब्ध कराया जा सकता है. हालांकि, वह अन्य 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 अफ़िलिएट मार्केटिंग से आने वाले ट्रैफ़िक को किसी वेबसाइट पर भेजना नहीं होना चाहिए. भले ही, वेबसाइट का मालिकाना हक किसी के भी पास हो.
   - हम लगातार नए तरीके खोज रहे हैं, ताकि बच्चों के लिए ऐप्लिकेशन बनाने वाले डेवलपर को काम करने में आसानी हो और उन्हें अच्छा अनुभव मिले. अगर आपको शिक्षा से जुड़े ऐप्लिकेशन बनाने के हमारे भरोसेमंद वेब ऐप्लिकेशन के पायलट प्रोजेक्ट से जुड़ना है, तो कृपया अपनी दिलचस्पी के बारे में यहां बताएं.
3. **Google Play Console में सवालों के जवाब:** आपको Google Play Console में अपने ऐप्लिकेशन से जुड़े सवालों के सही जवाब देने चाहिए. ऐप्लिकेशन में कोई भी बदलाव होने पर, जवाबों को अपडेट कर देना चाहिए. इसमें, कॉन्टेंट रेटिंग से जुड़े सवालों के जवाबों में ऐप्लिकेशन के उन हिस्सों की साफ़ जानकारी देना शामिल है जिनसे इंटरैक्ट किया जा सकता है. इसके अलावा, इसमें और भी जानकारी शामिल हो सकती है. उदाहरण के लिए:
   - आपके ऐप्लिकेशन के उपयोगकर्ताओं का आपस में बातचीत करना या जानकारी शेयर करना;
   - आपके ऐप्लिकेशन का, उपयोगकर्ताओं की जानकारी को तीसरे पक्षों के साथ शेयर करना; और
   - आपके ऐप्लिकेशन का, उपयोगकर्ता की मौजूदा जगह की जानकारी को अन्य उपयोगकर्ताओं के साथ शेयर करना.
4. **विज्ञापन:** अगर आपका ऐप्लिकेशन बच्चों को या ऐसे लोगों को विज्ञापन दिखाता है जिनकी उम्र के बारे में पता नहीं है, तो आप:
   - उन लोगों को विज्ञापन दिखाने के लिए, सिर्फ़ Google Play से प्रमाणित, विज्ञापन दिखाने के लिए इस्तेमाल किए जाने वाले SDK टूल इस्तेमाल करें;
   - यह पक्का करें 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 करें कि बच्चों को विज्ञापन दिखाने से जुड़े, सभी लागू कानूनों और इंडस्ट्री स्टैंडर्ड का पालन हो.
5. **डेटा इस्तेमाल करने के तरीके:** आपको अपने ऐप्लिकेशन में, बच्चों से मिली किसी भी तरह की निजी और संवेदनशील जानकारी इकट्ठा करने के बारे में 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 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. इनके अलावा, इसमें और भी जानकारी शामिल हो सकती है. आपको यह 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, MAC, SSID, IMEI, और/या IMSI को शेयर 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 के ज़रिए, जगह की जानकारी का अनुरोध नहीं किया जाना चाहिए. साथ ही, जगह की सटीक जानकारी को इकट्ठा, इस्तेमाल, और शेयर नहीं 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.
6. **एपीआई और SDK टूल:** आपको यह पक्का करना चाहिए कि आपका ऐप्लिकेशन हर एपीआई और SDK टूल को सही तरीके से लागू करता हो.
   - सिर्फ़ बच्चों को टारगेट करने वाले ऐप्लिकेशन में ऐसे एपीआई या SDK टूल नहीं होने चाहिए जिन्हें खास तौर पर बच्चों से जुड़ी सेवाओं में इस्तेमाल करने की मंज़ूरी न मिली हो. इसमें, Google साइन-इन (या किसी Google खाते से जुड़ा डेटा ऐक्सेस करने वाली कोई भी अन्य Google API सेवा), Google Play गेम सेवाएं, और पुष्टि करने और अनुमति देने के लिए OAuth टेक्नोलॉजी का इस्तेमाल करने वाली कोई भी दूसरी एपीआई सेवा शामिल है.

- जो ऐप्लिकेशन बच्चों और बड़ों, दोनों को टारगेट करते हैं उनमें 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 किया जाना चाहिए या ऐसे इस्तेमाल किया जाना चाहिए कि बच्चों से डेटा इकट्ठा न हो. जो ऐप्लिकेशन बच्चों और बड़ों, दोनों को टारगेट करते हैं उनमें ऐसे एपीआई या SDK टूल से लोगों को साइन इन या कॉन्टेंट ऐक्सेस करने के लिए नहीं कहना चाहिए जिन्हें बच्चों के लिए बनी सेवाओं में इस्तेमाल की मंज़ूरी नहीं मिली है.

7. **ऑगमेंटेड रिएलिटी (एआर):** अगर आपके ऐप्लिकेशन में ऑगमेंटेड रिएलिटी (एआर) का इस्तेमाल किया गया है, तो आपको एआर सेक्शन लॉन्च होते ही एक सुरक्षा चेतावनी शामिल करनी होगी. चेतावनी में नीचे दी गई जानकारी शामिल होनी चाहिए:
   - माता-पिता 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 होने वाली चीज़ों के बारे में सजग रहना.
   - आपके ऐप्लिकेशन को ऐसे डिवाइस के इस्तेमाल की ज़रूरत नहीं होनी चाहिए जो बच्चों के इस्तेमाल के लिए सही नहीं है. उदाहरण के लिए, Daydream और Oculus.
8. **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 और 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 का लेन-देन करने की सुविधा उपलब्ध कराने से पहले, आपको वयस्क होने से जुड़ी जानकारी वाली 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 से जुड़ी जानकारी वाली कार्रवाई को ज़रूरी शर्तों में शामिल करना होगा.
   - वयस्क होने से जुड़ी जानकारी वाली 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 की पुष्टि से जुड़ा पिन, पासवर्ड, जन्मतिथि, 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 में शामिल हैं: chat roulette जैसे ऐप्लिकेशन, डेटिंग ऐप्लिकेशन, बच्चों पर फ़ोकस करने वाले ओपन चैट रूम वगैरह.
9. **कानून का पालन:** आपको यह पक्का करना होगा कि आपका ऐप्लिकेशन अमेरिका में लागू बच्चों की ऑनलाइन निजता और संरक्षण नियम (कोपा), ईयू (यूरोपीय संघ) में लागू सामान्य डेटा से जुड़े सुरक्षा कानून (जीडीपीआर), और किसी भी अन्य लागू कानून या नियम के मुताबिक हो. साथ ही, ऐसे सभी एपीआई या SDK टूल भी इन नियमों के मुताबिक हों जिन्हें आपके ऐप्लिकेशन में इस्तेमाल किया गया है या जिनसे आपका ऐप्लिकेशन जानकारी जुटाता है.

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

- ऐसे ऐप्लिकेशन जो अपने स्टोर पेज में प्रचार 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 चौंकाने वाला ऐसा कॉन्टेंट शामिल है जो बच्चों के लिए सही नहीं है.
- डेटिंग सेवाएं देने वाले या ऐसे ऐप्लिकेशन जो यौन या शादीशुदा ज़िंदगी से जुड़ी सलाह देते हैं.
- ऐसे ऐप्लिकेशन जिनमें उन वेबसाइटों के लिंक होते हैं जो Google Play की डेवलपर कार्यक्रम की नीतियों का उल्लंघन करने वाले कॉन्टेंट को पेश करती हैं.
- ऐसे ऐप्लिकेशन जो बड़ों के लिए बनाए गए विज्ञापन बच्चों को दिखाते हैं, जैसे कि वे विज्ञापन जिनमें जुआ खेलने से जुड़ा, हिंसक, और सेक्शुअल कॉन्टेंट होता है. जो व्यावसायिक कॉन्टेंट, इन-ऐप्लिकेशन खरीदारी, और विज्ञापन बच्चों के लिए होते हैं उनसे जुड़ी Google Play की नीतियों के बारे में ज़्यादा जानकारी के लिए, परिवार के लिए बनाए गए विज्ञापन और कमाई करने की नीतियां देखें.

परिवार के लिए बनाया गया कार्यक्रम

खास तौर पर, बच्चों के लिए बनाए गए ऐप्लिकेशन को, परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेना चाहिए. अगर आपका ऐप्लिकेशन हर किसी के लिए बनाया गया है, जिनमें बच्चे और परिवार भी शामिल हैं, तो आप भी इस कार्यक्रम में हिस्सा लेने के लिए आवेदन कर सकते हैं.

कार्यक्रम में शामिल होने की मंज़ूरी पाने के लिए ज़रूरी है कि आपका ऐप्लिकेशन, परिवार नीति और परिवार के लिए बनाए गए कार्यक्रम की सभी ज़रूरी शर्तें पूरी करे. इनके अलावा, इसे Google Play के डेवलपर कार्यक्रम की नीतियों और डेवलपर वितरण अनुबंध की ज़रूरी शर्तें भी पूरी करनी होंगी.

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

कार्यक्रम की ज़रूरी शर्तें

परिवार के लिए बनाए गए कार्यक्रम में हिस्सा लेने वाले सभी ऐप्लिकेशन का और उनमें शामिल विज्ञापन का कॉन्टेंट ऐसा होना चाहिए जो बच्चों (ऐप्लिकेशन को ईएसआरबी से 'सभी' या 'सभी 10+' या इसके बराबर रेटिंग मिली होनी चाहिए) के लिए सही और उनके काम का हो. साथ ही, ऐप्लिकेशन में सिर्फ़ Google Play से प्रमाणित किए गए विज्ञापन SDK टूल का इस्तेमाल किया जाना चाहिए. परिवार के लिए बनाए गए कार्यक्रम में स्वीकार किए गए ऐप्लिकेशन को, कार्यक्रम की सभी ज़रूरी शर्तों का पालन करना होगा. Google Play, परिवार के लिए बनाए गए कार्यक्रम के लिए गलत पाए जाने वाले किसी भी ऐप्लिकेशन को खारिज कर सकता है, हटा सकता है या निलंबित कर सकता है.

Here are some examples of common apps that are ineligible for the program:

- ऐसे ऐप्लिकेशन जिन्हें 'ईएसआरबी सभी' रेटिंग दी गई है, लेकिन उनमें जुए के कॉन्टेंट के विज्ञापन शामिल हैं
- अभिभावकों या देखभाल करने वालों के लिए बने ऐप्लिकेशन (उदाहरण के लिए, स्तनपान कराने की गतिविधि ट्रैक करने वाला ऐप्लिकेशन, डेवलपर गाइड)
- माता-पिता के लिए गाइड या ऐसे डिवाइस मैनेजमेंट ऐप्लिकेशन जिनका इस्तेमाल सिर्फ़ माता-पिता या देखभाल करने वाले लोग ही कर सकते हैं

श्रेणियां

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

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

दिमाग लगाने वाले गेम: ऐसे गेम जिन्हें खेलने के लिए बहुत सोचना पड़ता है. इनमें पहेलियां, मिलान करने वाले गेम, सवाल-जवाब, और ऐसे दूसरे गेम शामिल हैं जो याद करने की क्षमता, समझदारी या तर्क को चुनौती देते हैं.

रचनात्मकता: ऐसे ऐप्लिकेशन और गेम जो रचनात्मकता को बढ़ावा देते हैं. इनमें ड्रॉइंग, पेंटिंग, और कोडिंग ऐप्लिकेशन के अलावा, ऐसे दूसरे ऐप्लिकेशन और गेम शामिल हैं जिनमें आप चीज़ें बना और तैयार कर सकते हैं.

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

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

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

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.

फ़ॉर्मैट से जुड़ी ज़रूरी शर्तें

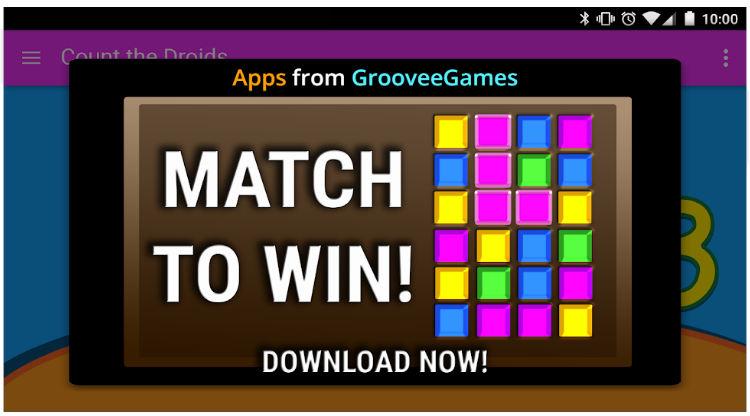
कमाई करने और विज्ञापन के लिए आपके ऐप्लिकेशन में ऐसे कॉन्टेंट का इस्तेमाल नहीं किया जाना चाहिए जिससे धोखाधड़ी की संभावना बने या उस कॉन्टेंट को ऐसे डिज़ाइन न किया गया हो जिससे कि बच्चे अनजाने में उसे क्लिक करें. नीचे दी गई चीज़ों पर पाबंदी है:

- ऐसे विज्ञापन या कमाई करने से जुड़ा कॉन्टेंट जिससे लोगों को परेशानी हो. इसमें, ऐसे विज्ञापन या कमाई करने से जुड़ा कॉन्टेंट भी शामिल है जो स्क्रीन को ढक लेता है या सामान्य इस्तेमाल में रुकावट डालता है और जिसे हटाने के लिए साफ़ तौर पर कोई तरीका उपलब्ध नहीं कराया जाता (जैसे कि विज्ञापन वॉल)
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट डालता है और जिसे पांच सेकंड के बाद भी हटाया नहीं जा सकता.
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जो ऐप्लिकेशन के सामान्य इस्तेमाल या गेम खेलने में रुकावट नहीं डालता, लेकिन यह पांच सेकंड के बाद भी दिखता रहता है (जैसे कि विज्ञापन से जुड़ा वीडियो कॉन्टेंट).
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जो ऐप्लिकेशन लॉन्च होते ही दिखता है
- पेज पर एक से ज़्यादा विज्ञापन प्लेसमेंट (उदाहरण के लिए, ऐसे बैनर विज्ञापन जो एक प्लेसमेंट में एक से ज़्यादा ऑफ़र दिखाते हैं या एक से ज़्यादा बैनर या वीडियो विज्ञापन दिखाते हैं. इसकी अनुमति नहीं है).
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जिसे आपके ऐप्लिकेशन के कॉन्टेंट से साफ़ तौर पर अलग नहीं किया जा सकता
- विज्ञापन के दर्शकों की संख्या बढ़ाने या इन-ऐप्लिकेशन खरीदारी को बढ़ाने के लिए, ऐसे तरीकों का इस्तेमाल जो चौंकाने वाले हों या गलत तरह से इमोशनल करने वाले हों
- इन-ऐप्लिकेशन खरीदारी करने के लिए, गेम के वर्चुअल सिक्कों और असली पैसों के बीच फ़र्क़ न दिखाना

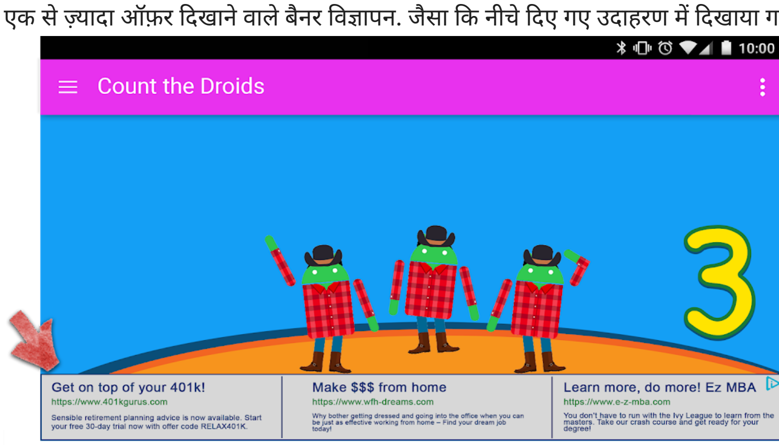
यह पक्का करने के लिए कि Google Play एक सुरक्षित और सम्मानजनक प्लैटफ़ॉर्म बना रहे, हमने ऐसे कॉन्टेंट को परिभाषित और प्रतिबंधित करने के मानक बनाए हैं जो हमारे उपयोगकर्ताओं के लिए हानिकारक या गलत हो.

- ऐसे विज्ञापन 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:

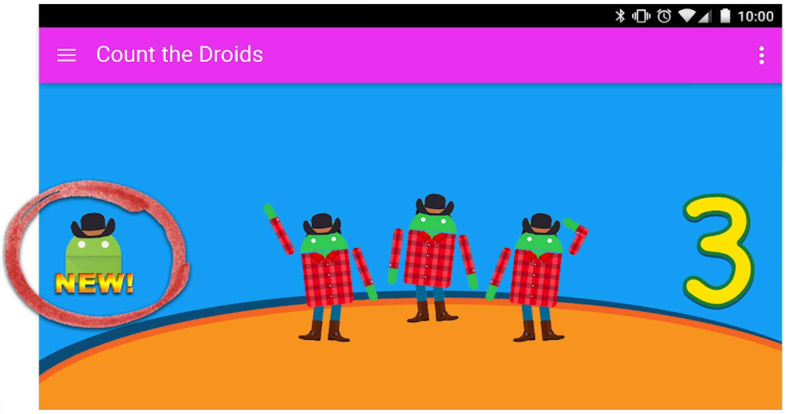
- ऐसे विज्ञापन और कमाई करने से जुड़ा कॉन्टेंट जो उपयोगकर्ता को विज्ञापन हटाने का तरीका साफ़ तौर पर बताए बिना, डिवाइस की पूरी स्क्रीन या उसके ज़्यादातर हिस्से पर दिखने लगता है, जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



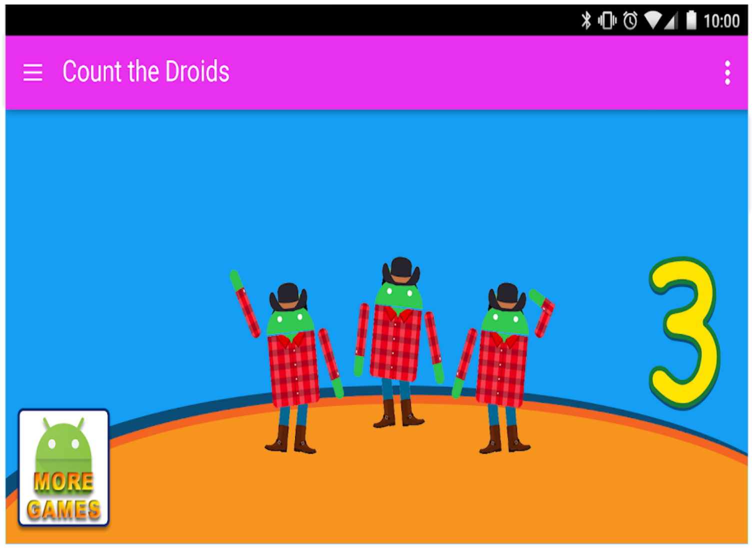
- एक से ज़्यादा ऑफ़र दिखाने वाले बैनर विज्ञापन. जैसा कि नीचे दिए गए उदाहरण में दिखाया गया है:



- 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, म्यूज़िक 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 SDK टूल

अगर आपके ऐप्लिकेशन में विज्ञापन दिखाए जाते हैं और आपकी टारगेट ऑडियंस में सिर्फ़ बच्चे शामिल हैं, तो आपको सिर्फ़ परिवार के लिए बनाए गए कार्यक्रम के लिए इस्तेमाल होने वाले खुद से प्रमाणित विज्ञापन SDK टूल 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 विज्ञापन दिखाने के लिए, खास तौर पर खुद से

प्रमाणित किए गए किसी विज्ञापन SDK टूल का इस्तेमाल किया जाए. परिवार के लिए बनाए गए कार्यक्रम में मौजूद ऐप्लिकेशन के लिए ज़रूरी है कि वे सिर्फ़, खुद से प्रमाणित किए हुए विज्ञापन SDK टूल का इस्तेमाल करें.

इन ज़रूरी शर्तों के बारे में ज़्यादा जानकारी और खुद से प्रमाणित किए जाने वाले विज्ञापन SDK टूल की मौजूदा सूची देखने के लिए, कृपया परिवार के लिए बनाए गए कार्यक्रम के लिए इस्तेमाल होने वाले खुद से प्रमाणित किए गए विज्ञापन SDK टूल के नीति वाले पेज पर 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.

इन-ऐप्लिकेशन खरीदारी

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

Enforcement

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

पॉलिसी का कवरेज

आपके ऐप्लिकेशन में जो भी कॉन्टेंट दिखाया जाता है या जिससे वह जुड़ा हुआ है उस पर Google Play की नीतियां लागू होती हैं. इसमें, ऐप्लिकेशन इस्तेमाल करने वाले लोगों को दिखाए जाने वाले विज्ञापन शामिल हैं. साथ ही, किसी भी तरह का यूज़र जनरेटेड कॉन्टेंट जिसे ऐप्लिकेशन होस्ट करता है या जिससे यह जुड़ा हुआ है उस पर भी ये नीतियां लागू होती हैं. इसके अलावा, 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 और चेतावनी मिलने पर आप ऐप्लिकेशन को अनइंस्टॉल कर सकते हैं.

नीति उल्लंघन ठीक करने के तरीके को लागू करने की प्रक्रिया

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

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

इन नीतियों या डेवलपर वितरण अनुबंध (DDA) के बार-बार होने वाले या गंभीर उल्लंघनों (जैसे कि मैलवेयर, धोखाधड़ी, और उपयोगकर्ता या डिवाइस को नुकसान पहुंचाने वाले ऐप्लिकेशन) की वजह से किसी व्यक्ति के या उससे जुड़े Google Play डेवलपर खातों को बंद कर दिया जाएगा.

नीति के उल्लंघन की वजह से की जाने वाली कार्रवाईयां

नीति उल्लंघन ठीक करने की अलग-अलग कार्रवाइयां, आपके ऐप्लिकेशन पर अलग-अलग असर डाल सकती हैं. नीचे दिए गए सेक्शन में उन कार्रवाइयों की जानकारी दी गई है जो Google Play कर सकता है. साथ ही, यह जानकारी भी दी गई है कि इन कार्रवाइयों का आपके ऐप्लिकेशन या Google Play डेवलपर खाते पर क्या असर पड़ेगा. यह जानकारी इस वीडियो में भी दी गई 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 पहले के किसी भी वर्शन को Google Play से हटा दिया जाता है. इसके बाद, वे डाउनलोड करने के लिए मौजूद नहीं होंगे.
- ऐप्लिकेशन को हटा दिया गया है. इसलिए, लोग ऐप्लिकेशन के स्टोर पेज, मौजूदा उपयोगकर्ता इंस्टॉल, आंकड़े और रेटिंग नहीं देख पाएंगे. हटाए गए ऐप्लिकेशन में नीति का पालन करने वाला अपडेट करने पर जानकारी वापस आ जाएगी.
- जब तक Google Play नीति का पालन करने वाले वर्शन को मंज़ूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले सकते.
- ऐप्लिकेशन को कई बार हटाने से उस पर रोक लगा सकते हैं, लेकिन इसका असर आपके Google Play डेवलपर खाते की स्थिति पर तुरंत नहीं पड़ता.

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

निलंबन

- ऐप्लिकेशन और उसके पहले के किसी भी वर्शन को Google Play से हटा दिया जाता है. इसके बाद, वे डाउनलोड करने के लिए मौजूद नहीं होंगे.
- नीति के बहुत खराब या एक से ज़्यादा बार उल्लंघन होने के साथ ही, कई बार खारिज होने या हटाने से ऐप्लिकेशन निलंबित हो सकता है.
- ऐप्लिकेशन निलंबित होने के बाद, लोग ऐप्लिकेशन का स्टोर पेज, ऐप्लिकेशन इंस्टॉल करने वाले लोगों की मौजूदा संख्या, आंकड़े, और रेटिंग नहीं देख पाएंगे. नीति का पालन करने वाला अपडेट सबमिट करने के बाद, यह जानकारी Google Play पर वापस उपलब्ध करा दी जाएगी.
- ऐप्लिकेशन निलंबित होने के बाद, आप उसके APK या ऐप्लिकेशन बंडल का इस्तेमाल नहीं कर सकते.
- जब तक Google Play नीति का पालन करने वाले वर्शन को मंज़ूरी नहीं देता, तब तक लोग इन-ऐप्लिकेशन खरीदारी या इन-ऐप्लिकेशन बिलिंग की सुविधा का फ़ायदा नहीं ले पाएंगे.
- निलंबन को आपके Google Play डेवलपर खाते की अच्छी स्थिति के ख़िलाफ़ हमला माना जाता है. एक से ज़्यादा बार निलंबित होने पर आपका Google Play डेवलपर खाता और उससे जुड़े खाते बंद किए जा सकते हैं.

ध्यान दें: निलंबित किए गए ऐप्लिकेशन को तब तक फिर से प्रकाशित करने की कोशिश न करें, जब तक Google Play की टीम आपसे ऐसा करने के लिए न कहे.

यह सीमित करना कि ऐप्लिकेशन किसे दिखेगा

- Google Play पर आपके ऐप्लिकेशन को खोजे जाने पर पाबंदी लगा दी जाती है. आपका ऐप्लिकेशन Google Play पर उपलब्ध रहेगा और ऐप्लिकेशन के 'Play स्टोर" में दिए सीधे लिंक के साथ लोग इसे ऐक्सेस कर सकते है.
- ऐप्लिकेशन 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, लोग 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.

खाता बंद किया जाना

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

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

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. इसके अलावा, वे अपने खाते से ऐप्लिकेशन प्रकाशित करने के साथ ही, बीच-बीच में ऐप्लिकेशन मैनेज भी करते रहते हैं. किसी भी तरह के गलत इस्तेमाल को रोकने के लिए, हम ऐसे खातों को बंद कर देते हैं जो चालू नहीं हैं या जिनका इस्तेमाल नहीं किया जा रहा. हालांकि, जिन खातों से किसी ऐप्लिकेशन को प्रकाशित किया जाता है और नियमित तौर पर अपडेट किया जाता है, आंकड़े ऐक्सेस किए जाते हैं या स्टोर पेज को मैनेज किया जाता है उन्हें बंद नहीं किया जाएगा.

अगर डॉरमेंट खाता बंद किया जाता है, तो 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 आप आने वाले में नया खाता नहीं बना पाएंगे. आप जब चाहें खाता बनाकर, Google Play पर ऐप्लिकेशन प्रकाशित कर सकते हैं. हालांकि, आप बंद किए गए खाते को फिर से चालू नहीं कर पाएंगे और उस खाते से जुड़ा डेटा या पुराने ऐप्लिकेशन, नए खाते पर उपलब्ध नहीं होंगे.

पॉलिसी संबंधी उल्लंघनों का प्रबंधन और रिपोर्टिंग

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

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

Google Play अपने उपयोगकर्ताओं को ऐप्लिकेशन के इस्तेमाल का सुरक्षित और शानदार अनुभव देना चाहता है. साथ ही, Google Play अपने सभी डेवलपर को भी एक अच्छा अवसर उपलब्ध कराना चाहता है, ताकि वे सफल हो सकें. हम यह पक्का करने की कोशिश करते हैं कि उपयोगकर्ता को, आपका ऐप्लिकेशन ज़्यादा आसानी से उपलब्ध हो.

आम तौर पर होने वाले उल्लंघनों की वजह से, ऐप्लिकेशन की समीक्षा की प्रोसेस धीमी हो सकती है या समीक्षा के अनुरोध को अस्वीकार भी किया जा सकता है. इससे बचने के लिए, Play Console का इस्तेमाल करके जानकारी सबमिट करते समय, आप नीचे बताए गए काम ज़रूर करें.

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

- ऐप्लिकेशन से जुड़ी सभी जानकारी और मेटाडेटा सही-सही उपलब्ध कराएं
- पक्का करें कि आपकी संपर्क जानकारी अप-टू-डेट हो
- ऐप्लिकेशन की प्राइवेसी पॉलिसी अपलोड करें और **डेटा की सुरक्षा** वाले सेक्शन में ज़रूरी जानकारी भरें
- एक ऐसा डेमो खाता उपलब्ध कराएं जो चालू हो. इसके अलावा, लॉगिन से जुड़ी जानकारी और अपने ऐप्लिकेशन की समीक्षा के लिए ज़रूरी अन्य सभी चीज़ें (उदाहरण के लिए, 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 की डेवलपर कार्यक्रम (डेवलपर प्रोग्राम) की पॉलिसी के मुताबिक हैं या नहीं. इनमें, विज्ञापन नेटवर्क कंपनियां, आंकड़ों से जुड़ी सेवाएं, और तीसरे पक्ष के उपलब्ध कराए गए SDK टूल शामिल हैं. अगर आपके ऐप्लिकेशन की टारगेट ऑडियंस में बच्चे भी शामिल हैं, तो यह पक्का करें कि आपका ऐप्लिकेशन हमारी फ़ैमिली पॉलिसी का भी पालन करता हो.

याद रखें कि डेवलपर डिस्ट्रिब्यूशन एग्रीमेंट और डेवलपर कार्यक्रम (डेवलपर प्रोग्राम) की सभी पॉलिसी को देखना आपकी ज़िम्मेदारी है, ताकि यह पक्का हो सके कि आपका ऐप्लिकेशन पूरी तरह इसका 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