Zasady programu dla deweloperów (obowiązuje od 1 października 2020 r)

Wspólnie twórzmy źródło aplikacji i gier, które cieszy się największym zaufaniem na świecie

Twoje innowacje to podstawa naszego wspólnego sukcesu, ale pamiętaj o wynikającej z niego odpowiedzialności. Zasady programu dla deweloperów wraz z Umową dystrybucyjną dla deweloperów są po to, byśmy razem dalej mogli oferować najbardziej innowacyjne i cieszące się największym zaufaniem aplikacje ponad miliardowi klientów Google Play. Zachęcamy do zapoznania się z naszymi zasadami poniżej.

Treści podlegające ograniczeniom

Użytkownicy na całym świecie codziennie korzystają z Google Play, by uzyskiwać dostęp do aplikacji i gier. Przed przesłaniem aplikacji należy się zastanowić, czy nadaje się ona do udostępnienia w Google Play i czy nie narusza lokalnych przepisów prawa.

Narażanie dzieci na niebezpieczeństwo

Aplikacje, które zawierają treści przedstawiające osoby nieletnie w kontekście seksualnym, będą natychmiast usuwane ze Sklepu.-Dotyczy to między innymi aplikacji promujących pedofilię lub nieodpowiednie interakcje z nieletnimi (np. obmacywanie lub pieszczoty).

Ponadto niedozwolone są aplikacje przeznaczone dla dzieci, ale zawierające tematykę tylko dla dorosłych, w tym aplikacje obrazujące nadmierną przemoc, krew i okrucieństwo oraz aplikacje przedstawiające szkodliwe bądź niebezpieczne działania lub zachęcające do takich działań. Zabraniamy również publikowania aplikacji, które promują negatywne postrzeganie ciała lub siebie, w tym aplikacji przedstawiających w celach rozrywkowych operacje plastyczne, odchudzanie lub inne zabiegi kosmetyczne mające na celu zmianę wyglądu.

Jeśli znajdziemy takie treści, zgłosimy je odpowiednim władzom i usuniemy konta Google osób uczestniczących w ich rozpowszechnianiu.

Nieodpowiednie treści

Aby mieć pewność, że platforma Google Play jest bezpiecznym i tolerancyjnym miejscem, stworzyliśmy standardy, które definiują i blokują materiały szkodliwe lub nieodpowiednie dla naszych użytkowników.

Treści o charakterze seksualnym i wulgaryzmy

Zabraniamy publikowania aplikacji zawierających lub promujących treści erotyczne i wulgaryzmy, w tym pornografię, oraz wszelkich treści i usług mających na celu wzbudzenie satysfakcji seksualnej. Treści zawierające nagość mogą być dozwolone, o ile mają charakter edukacyjny, dokumentalny, naukowy lub artystyczny i nie są użyte w sposób nieuzasadniony.

Oto kilka często spotykanych przykładów naruszenia zasad:

- przedstawianie nagości w kontekście erotycznym lub póz o charakterze jednoznacznie seksualnym, jeśli osoba jest w pełni naga, ma zamazane miejsca intymne lub jest tylko nieznacznie okryta ubraniem w sposób, który byłby nie do przyjęcia w miejscu publicznym;
- przedstawianie, również za pomocą animacji i ilustracji, aktów seksualnych lub póz o charakterze jednoznacznie seksualnym bądź przedstawianie części ciała w kontekście seksualnym;
- treści przedstawiające lub stanowiące gadżety bądź poradniki erotyczne oraz ukazujące nielegalne czynności seksualne i fetysze;
- treści lubieżne lub wulgarne – w tym między innymi wulgaryzmy, obelgi, przekleństwa oraz słowa kluczowe nawiązujące do treści dla dorosłych / treści erotycznych zamieszczone w informacjach o aplikacji lub w samej aplikacji;
- treści przedstawiające, opisujące lub promujące zoofilię;
- aplikacje promujące rozrywkę związaną z seksem, usługi towarzyskie lub inne usługi, które mogą zostać zinterpretowane jako świadczenie usług seksualnych za pieniądze;

- aplikacje, które poniżają lub uprzedmiotawiają innych.

Szerzenie nienawiści

Zabraniamy publikowania aplikacji promujących przemoc lub szerzących nienawiść do poszczególnych osób lub grup osób z powodu ich pochodzenia rasowego lub etnicznego, religii, niepełnosprawności, wieku, narodowości, statusu weterana, orientacji seksualnej, płci, tożsamości płciowej lub innego aspektu wiążącego się z systemową dyskryminacją lub marginalizacją.

W niektórych krajach zgodnie z lokalnymi przepisami i regulacjami możemy blokować aplikacje zawierające treści popularnonaukowe, dokumentalne, naukowe lub artystyczne dotyczące nazizmu.

Oto często spotykane przykłady naruszenia zasad:

- treści lub wypowiedzi mające na celu udowodnienie, że chroniona grupa osób jest nieludzka, gorsza lub zasługuje na nienawiść;
- aplikacje zawierające nienawistne wypowiedzi, obelgi, stereotypy lub teorie na temat chronionej grupy osób, przedstawiające te osoby jako wyróżniające się negatywnymi cechami (np. złymi intencjami, zepsuciem czy nikczemnością) albo w sposób bezpośredni lub pośredni mówiące o tym, że dana grupa osób stanowi zagrożenie;
- treści lub wypowiedzi nakłaniające do nienawiści bądź dyskryminacji grupy osób tylko dlatego, że należą one do grupy chronionej;
- treści promujące symbolikę kojarzoną z nienawiścią, np. flagi, symbole, insygnia lub inne przedmioty albo zachowania związane z grupami szerzącymi nienawiść.

Przemoc

Zabraniamy publikowania aplikacji przedstawiających nieuzasadnioną przemoc lub inne niebezpieczne czynności oraz umożliwiających ich wykonanie. Generalnie dopuszczamy aplikacje przedstawiające fikcyjną przemoc w kontekście gry, np. w formie kreskówki, a także treści dotyczące polowań i wędkarstwa.

Oto kilka często spotykanych przykładów naruszenia zasad:

- drastyczne przedstawianie lub realistyczne opisy przemocy albo gróźb brutalnej przemocy względem ludzi bądź zwierząt;
- aplikacje promujące samookaleczanie się, samobójstwo, dręczenie, nękanie, zaburzenia odżywiania, zabawy w duszenie lub inne czynności, które mogą spowodować poważne obrażenia lub śmierć.

Treści związane z terroryzmem

Nie zezwalamy organizacjom terrorystycznym na publikowanie aplikacji w Google Play w żadnym celu, w tym do prowadzenia rekrutacji.

Zabronione jest publikowanie aplikacji związanych z terroryzmem, na przykład zawierających treści promujące akty terroru, podżegające do przemocy czy pochwalające ataki terrorystyczne. Jeśli treści związane z terroryzmem są publikowane w celach edukacyjnych, dokumentalnych, naukowych lub artystycznych, należy podać odpowiednie informacje, które pomogą użytkownikom zrozumieć ich kontekst.

Dramatyczne wydarzenia

Zabraniamy publikowania aplikacji niewykazujących odpowiedniej wrażliwości względem klęsk żywiołowych, okrucieństwa, konfliktów, śmierci lub innych tragicznych wydarzeń bądź aplikacji czerpiących z nich korzyści. Aplikacje zawierające treści związane z dramatycznymi wydarzeniami są zwykle dozwolone, jeśli są to materiały popularnonaukowe, dokumentalne, naukowe lub artystyczne albo mają one na celu ostrzeżenie użytkowników przed dramatycznym wydarzeniem lub poinformowanie ich o nim.

Oto często spotykane przykłady naruszenia zasad:

- brak wrażliwości w obliczu śmierci jakiejś osoby bądź grupy osób na skutek samobójstwa, przedawkowania, choroby itp.;
- zaprzeczanie, że tragiczne wydarzenie miało miejsce;
- możliwe czerpanie korzyści z tragicznego wydarzenia bez wyraźnej korzyści dla jego ofiar.

Dręczenie i nękanie

Zabraniamy publikowania aplikacji, które zawierają groźby, akty nękania lub dręczenia bądź umożliwiają wykonywanie takich działań.

Oto często spotykane przykłady naruszenia zasad:

- dręczenie ofiar konfliktów międzynarodowych i religijnych;
- treści, które mają służyć do wykorzystywania innych osób – wyłudzanie, szantaż itp.;
- udostępnianie treści w celu publicznego upokorzenia innej osoby;
- nękanie ofiar tragicznych wydarzeń bądź ich przyjaciół i rodzin.

Produkty niebezpieczne

Zabronione jest publikowanie aplikacji służących do sprzedawania materiałów wybuchowych, broni palnej, amunicji lub niektórych akcesoriów do broni palnej.

- Objęte zakazem są akcesoria, które umożliwiają symulowanie ognia ciągłego lub przerobienie broni pozwalające prowadzić ogień ciągły (np. kolby typu „bump", spusty typu „gatling", automatyczne zaczepy spustowe, zestawy części do przerabiania), oraz magazynki i taśmy nabojowe na ponad 30 nabojów.

Zabronione jest publikowanie aplikacji dostarczających instrukcje na temat wytwarzania materiałów wybuchowych, broni palnej, amunicji, akcesoriów do broni palnej, do których dostęp jest ograniczony, lub innych rodzajów broni. Obejmuje to instrukcje przerabiania broni palnej w celu uzyskania możliwości prowadzenia ognia ciągłego lub symulacji ognia ciągłego.

Marihuana

Zabraniamy publikowania aplikacji ułatwiających sprzedaż marihuany i produktów z marihuaną (niezależnie od ich legalności).

Oto kilka często spotykanych przykładów naruszenia zasad:

- umożliwianie użytkownikom zamawiania marihuany z użyciem funkcji koszyka w aplikacji;
- pomaganie użytkownikom w organizowaniu dostawy lub odbioru marihuany;
- ułatwianie sprzedaży produktów z THC (tetrahydrokannabinolem), w tym produktów takich jak oleje konopne zawierające THC.

Tytoń i alkohol

Zabraniamy publikowania aplikacji ułatwiających sprzedaż tytoniu (w tym e-papierosów i waporyzatorów do tytoniu) oraz zachęcających do nielegalnego lub niewłaściwego używania alkoholu bądź tytoniu.

Oto często spotykane przykłady naruszenia zasad:

- przedstawianie albo zachęcanie do spożywania alkoholu lub używania tytoniu przez osoby nieletnie albo do sprzedaży takich produktów nieletnim;
- sugerowanie, że używanie tytoniu może poprawić status społeczny, życie seksualne bądź zawodowe, intelekt lub kondycję fizyczną;
- przedstawianie nadmiernego spożywania alkoholu w sposób korzystny, m.in. przedstawianie w pozytywnym świetle spożywania dużych ilości alkoholu, upijania się i zawodów w piciu.

Usługi finansowe

Zabraniamy publikowania aplikacji, które oferują użytkownikom szkodliwe lub wprowadzające w błąd produkty i usługi finansowe.

Na potrzeby tych zasad za produkty i usługi finansowe uznaje się produkty i usługi związane z zarządzaniem pieniędzmi i kryptowalutami lub ich inwestowaniem (w tym spersonalizowane doradztwo).

Jeśli aplikacja zawiera lub promuje produkty i usługi finansowe, musi być zgodna ze wszystkimi przepisami obowiązującymi w krajach i regionach, w których ma być dostępna. Na przykład musi zawierać określone informacje wymagane przez lokalne przepisy.

Opcje binarne

Zabraniamy publikowania aplikacji, które umożliwiają użytkownikom handel opcjami binarnymi.

Kryptowaluty

Zabronione jest publikowanie aplikacji, które kopią kryptowaluty na urządzeniach. Dozwolone są aplikacje do zdalnego zarządzania kopaniem kryptowalut.

Kredyty konsumpcyjne

Kredyt konsumpcyjny to jednorazowe pożyczenie pieniędzy indywidualnemu konsumentowi przez osobę fizyczną, organizację bądź inny podmiot w celu innym niż sfinansowanie zakupu środka trwałego lub edukacji. Aby móc podjąć świadomą decyzję o zaciągnięciu kredytu konsumpcyjnego, konsumenci potrzebują informacji o jakości, warunkach, opłatach, harmonogramie spłaty, ryzyku i korzyściach związanych z produktami kredytowymi.

- Przykłady: kredyty konsumpcyjne, chwilówki, pożyczki społecznościowe, pożyczki pod zastaw.
- Produkty nieobjęte tą definicją: kredyty hipoteczne, kredyty samochodowe, kredyty studenckie, odnawialne linie kredytowe (np. karty kredytowe, osobiste linie kredytowe).

Aplikacje, które oferują kredyty konsumpcyjne, w tym aplikacje, które bezpośrednio oferują kredyty, służą do zdobywania potencjalnych klientów lub łączą klientów z zewnętrznymi pożyczkodawcami, muszą zawierać w metadanych te informacje:

- minimalny i maksymalny okres spłaty;
- maksymalna rzeczywista roczna stopa oprocentowania, która zwykle obejmuje odsetki, opłaty i inne roczne koszty, lub podobna stopa oprocentowania obliczona zgodnie z lokalnymi przepisami prawa;
- modelowy przykład całkowitego kosztu kredytu wraz ze wszystkimi obowiązującymi opłatami;
- polityka prywatności zawierająca szczegółowy opis sposobów odczytywania, zbierania, wykorzystywania oraz udostępniania danych osobowych i informacji poufnych użytkownika.

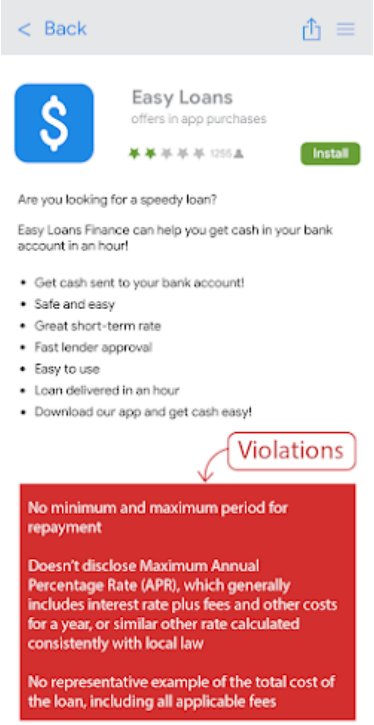
Nie zezwalamy na aplikacje, które promują kredyty konsumpcyjne wymagające spłaty w całości w ciągu maksymalnie 60 dni od daty udzielenia (nazywamy je „krótkoterminowymi kredytami konsumpcyjnymi”).

Kredyty konsumpcyjne z wysokim RRSO

W Stanach Zjednoczonych nie zezwalamy na aplikacje oferujące kredyty konsumpcyjne o rzeczywistej rocznej stopie oprocentowania (RRSO) wynoszącej 36% lub więcej. Aplikacje do kredytów konsumpcyjnych w USA muszą wyświetlać maksymalne RRSO obliczone zgodnie z ustawą TILA (Truth in Lending Act).

Te zasady dotyczą aplikacji bezpośrednio oferujących kredyty lub służących do zdobywania potencjalnych klientów oraz tych, które łączą klientów indywidualnych z zewnętrznymi pożyczkodawcami.

Oto przykład często spotykanego naruszenia zasad:



Hazard, gry i konkursy na prawdziwe pieniądze

Dopuszczamy aplikacje umożliwiające hazard na pieniądze, reklamy promujące hazard na pieniądze oraz gry typu fantasy sports, które spełniają określone wymagania.

Aplikacje hazardowe

Obecnie są dozwolone tylko we Francji, Irlandii i Wielkiej Brytanii.
We wszystkich innych lokalizacjach aplikacje zawierające treści lub usługi umożliwiające uprawianie hazardu online są zabronione.

Treści i usługi ułatwiające uprawianie hazardu online są dozwolone, o ile spełniają te wymagania:

- Deweloper musi ukończyć proces zgłoszenia aplikacji, by móc udostępnić ją w Google Play.
- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w kraju, w którym jest udostępniana.
- Deweloper musi mieć ważną licencję na prowadzenie działalności związanej z hazardem w każdym kraju, w którym udostępnia aplikację.
- Aplikacja musi uniemożliwiać użytkownikom niepełnoletnim uprawianie hazardu w aplikacji.
- Aplikacja musi uniemożliwiać uprawianie hazardu za jej pomocą w krajach, w których nie obowiązuje licencja dewelopera na prowadzenie działalności hazardowej.
- Aplikacja NIE może być oferowana jako płatna w Google Play ani używać Rozliczeń w aplikacji przez Google Play.
- Aplikacja musi być dostępna do pobrania i zainstalowania bezpłatnie ze Sklepu.
- Aplikacja musi mieć ocenę AO (tylko dla dorosłych) lub odpowiednik IARC.
- Aplikacja i jej opis w sklepie muszą w czytelny sposób przedstawiać informacje o odpowiedzialnym hazardzie.

Inne aplikacje oferujące gry, konkursy i zawody na pieniądze

Nie zezwalamy na publikowanie treści ani usług umożliwiających lub ułatwiających zawieranie zakładów, obstawianie stawek lub uczestniczenie w grach bądź konkursach wymagających prawdziwych pieniędzy (dotyczy to także kupna produktów w aplikacji za pieniądze) w celu uzyskania nagrody pieniężnej. Chodzi tu między innymi o kasyna online, zakłady sportowe, loterie niespełniające powyższych wymagań dotyczących aplikacji hazardowych oraz gry oferujące nagrody pieniężne lub materialne.

Oto przykłady naruszenia zasad:

- gry, które akceptują pieniądze w zamian za możliwość wygrania nagrody materialnej lub pieniężnej;
- gry z punktami „lojalnościowymi" (np. za zaangażowanie lub aktywność), które (1) są naliczane lub powielane, gdy użytkownik kupi coś za pieniądze; (2) mogą być wymieniane na przedmioty lub nagrody o wartości pieniężnej;
- aplikacje, które przyjmują lub kontrolują zakłady hazardowe, waluty w aplikacji wymagane do udziału w grze lub konkursie, wygrane albo zaliczki, za pomocą których użytkownik ma uzyskać lub przyspieszyć uzyskanie nagrody materialnej lub pieniężnej;
- aplikacje zawierające „wezwanie do działania" i służące do zawierania zakładów, obstawiania stawek lub udziału w grach, konkursach lub zawodach na pieniądze, np. aplikacje z elementami nawigacyjnymi (pozycjami menu, kartami, przyciskami itp.), które zapraszają użytkowników do zarejestrowania się lub wzięcia udziału w grze i wygrania nagrody pieniężnej.

Reklamy hazardu oraz gier, konkursów i zawodów na prawdziwe pieniądze w aplikacjach udostępnianych w Google Play

Zezwalamy na aplikacje reklamujące hazard oraz gry i zawody na pieniądze, jeśli spełniają one te wymagania:

- Aplikacja i reklama (od reklamodawcy) muszą być zgodne ze wszystkimi przepisami i standardami branżowymi obowiązującymi w miejscu wyświetlania reklamy.
- Reklama musi spełniać lokalne wymagania dotyczące licencji w odniesieniu do wszystkich promowanych produktów i usług związanych z hazardem.
- Aplikacja nie może wyświetlać reklam związanych z hazardem osobom, które nie ukończyły 18 lat.
- Aplikacja nie może brać udziału w programie Dla całej rodziny.
- Aplikacja nie może być kierowana do osób w wieku poniżej 18 lat.
- Jeśli reklamujesz aplikację hazardową (zgodnie z definicją powyżej), strona docelowa reklamy, strona z informacjami o reklamowanej aplikacji lub sama aplikacja musi zawierać wyraźne informacje o odpowiedzialnym hazardzie.
- Aplikacja nie może zawierać treści symulujących hazard (jak na przykład społecznościowe aplikacje hazardowe lub aplikacje z wirtualnymi automatami do gier).
- Aplikacja nie może oferować funkcji pomocnych w grach hazardowych, grach na prawdziwe pieniądze, loteriach i zawodach (np. funkcji pomagających w zawieraniu zakładów, realizowaniu wypłat, śledzeniu wyników sportowych, szacowaniu prawdopodobieństwa różnych wyników czy zarządzaniu środkami przeznaczonymi na hazard).
- Nie możesz mieć prawa własności do usług związanych z grami hazardowymi, grami na prawdziwe pieniądze, loteriami lub zawodami reklamowanymi w aplikacji.

- Zawartość aplikacji nie może promować usług związanych z grami hazardowymi, grami na prawdziwe pieniądze, loteriami czy zawodami ani też kierować użytkowników do takich usług.

Reklamy hazardu na pieniądze, gier na pieniądze, loterii i zawodów mogą być wyświetlane tylko w aplikacjach hazardowych (zgodnie z definicją powyżej) i aplikacjach, które spełniają wszystkie wymagania dotyczące reklam hazardu.

Oto kilka przykładów naruszenia zasad:

- aplikacja przeznaczona dla osób niepełnoletnich wyświetlająca reklamę usług hazardowych;
- gra symulująca kasyno, która promuje prawdziwe kasyna lub kieruje użytkowników do prawdziwych kasyn;
- specjalna aplikacja do śledzenia prawdopodobieństwa wystąpienia różnych wyników sportowych, zawierająca zintegrowane reklamy hazardu prowadzące do witryny oferującej zakłady sportowe;
- aplikacja z wiadomościami, która wyświetla reklamy usług hazardowych należących do dewelopera aplikacji lub przez niego zarządzanych;
- aplikacje, które zawierają reklamy hazardu naruszające nasze zasady dotyczące reklam wprowadzających w błąd, np. reklamy wyświetlane użytkownikom jako przyciski, ikony lub inne interaktywne elementy w aplikacji.

Aplikacje typu fantasy sports

Dozwolone są wyłącznie aplikacje typu fantasy sports (zgodnie z definicją określoną przez obowiązujące przepisy lokalne), które spełniają te wymagania:

- Aplikacja jest 1) rozpowszechniana tylko w Stanach Zjednoczonych lub 2) zgodna z powyższymi wymaganiami dotyczącymi aplikacji hazardowych.
- Deweloper musi przesłać aplikację typu fantasy sports do weryfikacji. Dopiero po zatwierdzeniu będzie ją można udostępnić w Google Play.
- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w krajach, w których jest udostępniana.
- Aplikacja musi uniemożliwiać użytkownikom niepełnoletnim robienie zakładów lub przeprowadzanie transakcji pieniężnych w aplikacji.
- Aplikacja NIE może być oferowana jako płatna w Google Play ani używać Rozliczeń w aplikacji przez Google Play.
- Aplikacja musi być dostępna do pobrania i zainstalowania bezpłatnie ze Sklepu.
- Aplikacja musi mieć ocenę AO (tylko dla dorosłych) lub odpowiednik IARC.
- Aplikacja i jej opis w sklepie muszą w czytelny sposób przedstawiać informacje o odpowiedzialnym hazardzie.

W przypadku rozpowszechniania aplikacji w USA obowiązują te dodatkowe wymagania:

- Aplikacja musi być zgodna ze wszystkimi przepisami i standardami branżowymi obowiązującymi w USA lub na terytorium USA, w którym jest udostępniana.
- Deweloper musi mieć ważną licencję w każdym stanie i na każdym terytorium USA, które wymagają licencji na rozpowszechnianie aplikacji typu fantasy sports.
- Aplikacja musi uniemożliwiać używanie jej w stanach i na terytoriach USA, na terenie których deweloper nie ma licencji wymaganej do rozpowszechniania aplikacji typu fantasy sports.
- Aplikacja musi uniemożliwiać używanie jej w stanach i na terytoriach USA, na terenie których aplikacje typu fantasy sports są nielegalne.

Działania niezgodne z prawem

Zabraniamy publikowania aplikacji umożliwiających lub promujących podejmowanie działań niezgodnych z prawem.

Oto kilka często spotykanych przykładów naruszenia zasad:

- umożliwianie sprzedaży lub zakupu narkotyków albo leków na receptę bez recepty;
- przedstawianie albo zachęcanie do używania lub sprzedaży narkotyków, alkoholu bądź tytoniu przez osoby nieletnie;
- instrukcje uprawy nielegalnych roślin lub produkowania narkotyków.

Treści użytkowników

Treści użytkowników to treści umieszczane przez użytkowników w aplikacji, które są widoczne lub dostępne dla co najmniej niektórych spośród użytkowników aplikacji.

Aplikacje zawierające treści użytkowników muszą:

- wymagać, by użytkownicy zaakceptowali warunki korzystania z aplikacji lub zasady dotyczące użytkowników, zanim będą mogli utworzyć lub przesłać swoje treści;
- definiować kontrowersyjne treści i zachowania (w sposób zgodny z Zasadami programu dla deweloperów w Google Play) oraz informować o tym, że są one zabronione, w warunkach korzystania z aplikacji lub zasadach dotyczących użytkowników;
- prowadzić skuteczną i stałą moderację treści użytkowników stosownie do typu treści umieszczanych przez nich w aplikacji;
  - w przypadku aplikacji umożliwiających transmisję na żywo – usuwać kontrowersyjne treści użytkowników najszybciej jak to możliwe;
  - w przypadku aplikacji opartych na rzeczywistości rozszerzonej (AR) – moderować treści użytkowników (co obejmuje też system zgłaszania treści w aplikacji) z uwzględnieniem zarówno kontrowersyjnych treści użytkowników (np. obrazów AR o charakterze jednoznacznie seksualnym), jak i kotwiczenia elementów AR w newralgicznych miejscach (np. na obszarze o ograniczonym dostępie, takim jak baza wojskowa lub prywatna posiadłość, gdzie zakotwiczenie elementu AR może przysporzyć właścicielowi problemów);
- mieć łatwy w użyciu system do zgłaszania kontrowersyjnych treści użytkowników i podejmowania w związku z nimi odpowiednich działań;
- usuwać lub blokować użytkowników, którzy naruszają warunki korzystania z aplikacji lub zasady dotyczące użytkowników;
- mieć zabezpieczenia uniemożliwiające zarabianie na promowaniu nieodpowiedzialnego wydawania środków.

Aplikacje, których głównym celem jest prezentowanie kontrowersyjnych treści użytkowników, będą usuwane z Google Play. Aplikacje, które z biegiem czasu zaczną być używane głównie do zamieszczania kontrowersyjnych treści użytkowników lub zyskają reputację miejsca, w którym takie treści są dostępne, również będą usuwane z Google Play.

Oto kilka często spotykanych przykładów naruszenia zasad:

- promowanie treści użytkowników o charakterze jednoznacznie seksualnym, m.in. przez implementowanie lub akceptowanie płatnych funkcji, które zachęcają głównie do udostępniania kontrowersyjnych treści;
- aplikacje z treściami użytkowników, w których brakuje wystarczających środków ochrony przed groźbami, nękaniem lub dręczeniem, zwłaszcza w odniesieniu do osób nieletnich;
- posty, komentarze lub zdjęcia w aplikacji, których głównym przeznaczeniem jest nękanie lub wyodrębnienie konkretnej osoby w celu znęcania się nad nią, zaatakowania jej lub ośmieszenia;
- aplikacje, które notorycznie nie reagują na skargi użytkowników dotyczące kontrowersyjnych treści.

Niezatwierdzone substancje

Google Play nie dopuszcza aplikacji, które promują lub sprzedają niezatwierdzone substancje, niezależnie od deklaracji na temat ich legalności. Przykłady:

- wszystkie pozycje z tego niepełnego wykazu zabronionych leków i suplementów;
- produkty zawierające efedrynę;
- produkty zawierające gonadotropinę kosmówkową (hCG) w powiązaniu z utratą/kontrolą wagi lub w połączeniu z promocją sterydów anabolicznych;
- preparaty ziołowe i suplementy diety zawierające substancję czynną lub niebezpieczne składniki;
- nieprawdziwe lub wprowadzające w błąd oświadczenia zdrowotne, w tym oświadczenia, które sugerują, że produkt jest równie skuteczny jak leki na receptę lub substancje kontrolowane;
- produkty zatwierdzone nieoficjalne instytucje, reklamowane tak, by sugerować bezpieczeństwo i skuteczność w leczeniu oraz profilaktyce określonych chorób i dolegliwości;
- produkty, które były albo są przedmiotem dochodzeń lub ostrzeżeń ze strony urzędów czy instytucji państwowych;
- produkty, których nazwy są łudząco podobne do nazw niezatwierdzonych leków, suplementów lub substancji kontrolowanych.

Więcej informacji o niezatwierdzonych lub wprowadzających w błąd lekach i suplementach, które monitorujemy, znajdziesz tutaj: www.legitscript.com.

Własność intelektualna

Gdy deweloperzy kopiują czyjąś pracę lub wykorzystują ją bez zgody twórcy, może to zaszkodzić właścicielowi tej pracy. Nie należy stosować metod, które polegają na nieuczciwym wykorzystaniu czyjejś pracy.

Własność intelektualna

Zabraniamy publikowania takich aplikacji i tworzenia takich kont dewelopera, które naruszają prawa własności intelektualnej innych podmiotów (w tym znaki towarowe, prawa autorskie, patenty, tajemnice handlowe i pozostałe prawa własności). Niedozwolone są również aplikacje zachęcające lub nakłaniające do naruszania praw własności intelektualnej.

Google reaguje na zrozumiałe zawiadomienia o domniemanym naruszeniu praw autorskich. Aby uzyskać więcej informacji lub złożyć zawiadomienie o naruszeniu ustawy DMCA, zapoznaj się z naszymi procedurami dotyczącymi praw autorskich.

Aby przesłać skargę dotyczącą sprzedaży lub promocji podróbek produktów w aplikacji, prześlij powiadomienie o podróbkach.

Jeśli uważasz, że należący do Ciebie znak towarowy został bezprawnie wykorzystany w aplikacji w Google Play, w celu rozwiązania problemu najpierw skontaktuj się bezpośrednio z jej deweloperem. Jeśli nie możecie osiągnąć porozumienia, prześlij skargę dotyczącą znaku towarowego za pomocą tego formularza.

Jeśli masz pisemne potwierdzenie, że osoba trzecia wyraziła zgodę na wykorzystanie jej własności intelektualnej w Twojej aplikacji lub na stronie z informacjami o aplikacji (dotyczy to np. nazw i logo marek czy zasobów graficznych), przed przesłaniem aplikacji skontaktuj się z zespołem Google Play, by uniknąć jej odrzucenia z powodu naruszenia praw własności intelektualnej.

Nieautoryzowane używanie treści chronionych prawem autorskim

Zabraniamy publikowania aplikacji naruszających prawa autorskie. Modyfikowanie treści chronionych prawem autorskim nadal może skutkować naruszeniem. Aby deweloperzy mogli korzystać z takich treści, możemy poprosić, by udowodnili swoje uprawnienia.

Zachowaj ostrożność, korzystając z treści chronionych prawem autorskim przy prezentowaniu funkcji aplikacji. Zasadniczo najlepszym podejściem jest przygotowanie własnych, oryginalnych materiałów.

Oto niektóre przykłady treści chronionych prawem autorskim, które często są używane bez zezwolenia lub niezgodnie z prawem:

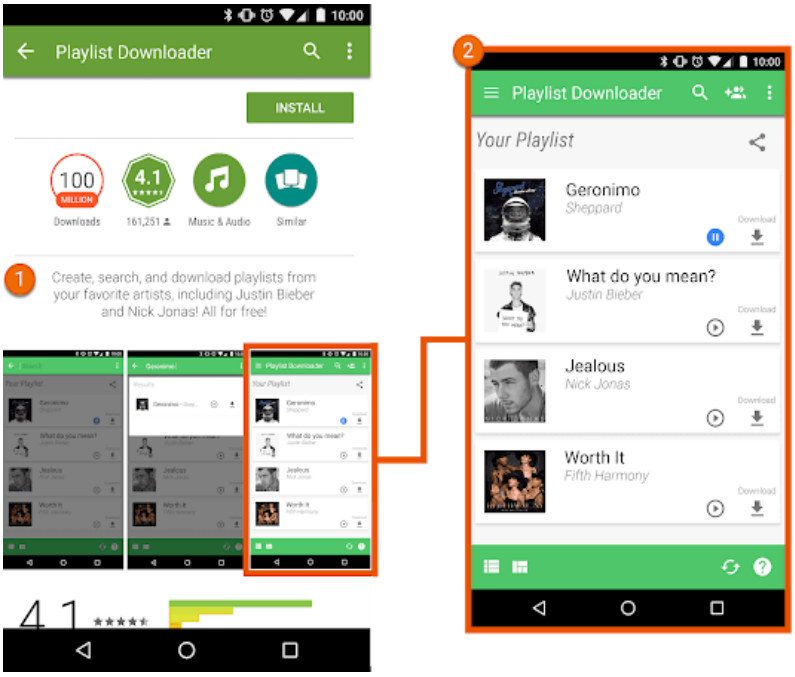
- Okładki albumów muzycznych, gier wideo i książek
- Obrazy marketingowe z filmów, telewizji lub gier wideo
- Plakaty lub obrazy związane z komiksami, kreskówkami, filmami, teledyskami lub telewizją
- Logo uczelni i zawodowych drużyn sportowych
- Zdjęcia skopiowane z konta osoby publicznej w serwisie społecznościowym
- Profesjonalne zdjęcia osób publicznych
- Reprodukcje prac graficznych niemożliwe do odróżnienia od oryginalnych utwórów chronionych prawami autorskimi
- Aplikacje z elementami odtwarzającymi klipy dźwiękowe z treści objętych prawami autorskimi
- Bezpłatne kopie lub tłumaczenia książek, które nie należą do domeny publicznej

Zachęcanie do naruszenia praw autorskich

Zabronione jest publikowanie aplikacji nakłaniających lub zachęcających do naruszania praw autorskich. Przed opublikowaniem aplikacji należy zastanowić się, w jaki sposób może ona zachęcać do naruszania praw autorskich, i w razie potrzeby skonsultować się z prawnikiem.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje do odtwarzania strumieniowego, które umożliwiają użytkownikom pobranie lokalnej kopii treści chronionych prawami autorskimi bez zezwolenia;
- aplikacje zachęcające użytkowników do pobierania i strumieniowego odtwarzania utworów chronionych prawami autorskimi, w tym muzyki i filmów, co stanowi naruszenie odpowiednich praw autorskich:



① Opis w informacjach o tej aplikacji zachęca użytkowników do pobrania bez zezwolenia treści chronionych prawami autorskimi.
② Zrzuty ekranu w informacjach o tej aplikacji zachęcają użytkowników do pobrania bez zezwolenia treści chronionych prawami autorskimi.

Naruszenie praw do znaków towarowych

Zabronione jest publikowanie aplikacji naruszających prawa do znaków towarowych. Znak towarowy to słowo, symbol lub ich połączenie, które określa źródło towaru lub usługi. Właściciel znaku towarowego ma prawo do jego wyłącznego używania razem z określonymi towarami lub usługami.

Naruszenie znaku towarowego to niewłaściwe lub nieautoryzowane użycie identycznego lub podobnego znaku, które może powodować niejasności co do pochodzenia produktu. Jeśli aplikacja korzysta z cudzych znaków towarowych w sposób, który może wprowadzać w błąd, możemy ją zawiesić.

Podróbki

Zabronione jest publikowanie aplikacji, za pomocą których prowadzona jest sprzedaż podróbek produktów lub w których taka sprzedaż jest promowana. Podróbki produktów mają znak towarowy lub logo, które jest identyczne lub niemal identyczne ze znakiem towarowym innego produktu. Naśladują też cechy danej marki, co ma przekonać nabywców, że są to oryginalne wyroby.

Prywatność, oszustwa i używanie urządzeń niezgodnie z przeznaczeniem

Dokładamy wszelkich starań, by chronić prywatność użytkowników i oferować im bezpieczne usługi. Surowo zabraniamy publikowania aplikacji wprowadzających w błąd, złośliwych lub wykorzystujących w nieodpowiedni sposób sieć, urządzenia czy dane osobowe.

Dane użytkownika

Aplikacje muszą w przejrzysty sposób informować o tym, jak są przetwarzane dane użytkownika (np. informacje zbierane od użytkownika, w tym te z jego urządzenia). Oznacza to obowiązek informowania o uzyskiwaniu przez aplikację dostępu do danych, ich zbieraniu, używaniu i udostępnianiu. Konieczne jest ograniczenie korzystania z danych tylko do celów zgodnych z ujawnionymi. Jeśli aplikacja obsługuje dane osobowe lub poufne użytkownika, obowiązują dodatkowe wymagania, które zostały wymienione w sekcji „Dane osobowe i poufne” poniżej. Te wymagania Google Play obowiązują jako uzupełnienie przepisów prawa dotyczących ochrony prywatności i danych.

Dane osobowe i poufne

Dane osobowe i poufne użytkownika obejmują między innymi: dane umożliwiające identyfikację, informacje finansowe i dane karty, informacje służące do uwierzytelniania, wpisy z książki telefonicznej, dane o lokalizacji urządzenia, SMS-y, kontakty i dane związane z połączeniami, dane rejestrowane za pomocą mikrofonu i aparatu, a także inne poufne informacje z urządzenia oraz dane o korzystaniu z niego. Jeśli aplikacja używa poufnych danych użytkownika:

- Dostęp do danych osobowych lub poufnych oraz ich zbieranie, używanie i udostępnianie należy ograniczyć do celów bezpośrednio związanych z korzystaniem z funkcji aplikacji i ich usprawnianiem (np. funkcji zgodnych z przeznaczeniem aplikacji, które są wymienione w jej opisie w Sklepie Play). Aplikacje, w których użycie tych danych jest poszerzone o wyświetlanie reklam, muszą być zgodne z naszymi Zasadami dotyczącymi reklam.
- Należy dodać informacje o polityce prywatności w przeznaczonym do tego polu w Konsoli Play oraz w samej aplikacji. Polityka prywatności w połączeniu z innymi objaśnieniami w aplikacji musi wyraźnie informować o tym, w jaki sposób aplikacja uzyskuje dostęp do danych użytkownika oraz jak je zbiera, wykorzystuje i udostępnia. Polityka prywatności musi też określać rodzaje danych osobowych i poufnych, do których aplikacja ma dostęp oraz które zbiera, wykorzystuje i udostępnia. Musi również wskazywać rodzaje podmiotów, którym udostępniane są takie dane.
- Ze wszystkimi danymi osobowymi lub poufnymi użytkownika postępuj w bezpieczny sposób, używając nowoczesnych metod szyfrowania (np. protokołu HTTPS).
- Jeśli to możliwe, przed uzyskaniem dostępu do danych objętych uprawnieniami Androida należy skorzystać z prośby o udzielenie uprawnienia na czas działania.
- Danych osobowych i poufnych nie wolno sprzedawać.

Wymagania dotyczące zgody oraz informacji dobrze widocznych dla użytkownika

W przypadkach, w których użytkownicy mogą z uzasadnionych przyczyn nie spodziewać się, że ich dane osobowe lub poufne będą potrzebne do obsługi lub usprawniania zgodnych z zasadami funkcji aplikacji (np. dane są zbierane w tle), musisz spełnić te wymagania:

W aplikacji musi znajdować się wyjaśnienie dotyczące dostępu do danych oraz ich zbierania, używania oraz udostępniania. Informacje w aplikacji:

- muszą znajdować się w samej aplikacji, a nie tylko w jej opisie czy na stronie internetowej;
- muszą być wyświetlane podczas normalnego używania aplikacji, nie wymagając otwarcia menu czy ustawień;
- muszą zawierać opis danych, do których aplikacja ma dostęp lub które zbiera;
- muszą wyjaśniać, jak dane będą używane lub udostępniane;
- **nie mogą** znajdować się tylko w polityce prywatności lub warunkach usługi;
- **nie mogą** być częścią innych informacji, które nie dotyczą zbierania danych osobowych lub poufnych.

Informacje w aplikacji muszą wyświetlać się bezpośrednio przed prośbą o zgodę użytkownika i – tam, gdzie ma to zastosowanie – przed powiązaną prośbą o udzielenie odpowiedniego uprawnienia na czas działania. Zabraniamy uzyskiwania dostępu do danych osobowych lub poufnych oraz ich zbierania przed uzyskaniem zgody użytkownika. Prośba aplikacji o zgodę musi spełniać te wymagania:

- Okno z prośbą o zgodę na przetwarzanie danych osobowych musi być prezentowane w jasny i jednoznaczny sposób.
- Wyrażenie zgody musi wymagać działania użytkownika (np. kliknięcia przycisku lub zaznaczenia pola wyboru).
- **Nie wolno** traktować jako zgody opuszczenia przez użytkownika ekranu z tymi informacjami (również przez kliknięcie w innym miejscu aplikacji albo naciśnięcie przycisku Wstecz lub przycisku ekranu głównego).
- Do uzyskania zgody **nie wolno** stosować komunikatów automatycznie zamykanych lub wygasających.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacja, która ma dostęp do listy aplikacji zainstalowanych przez użytkownika i nie traktuje jej jako danych osobowych lub poufnych zgodnie z polityką prywatności, zasadami postępowania z danymi oraz wymaganiami w zakresie zgody i informacji dobrze widocznych dla użytkownika;
- aplikacja, która ma dostęp do danych z listy kontaktów lub książki telefonicznej i nie traktuje ich jako danych osobowych lub poufnych zgodnie z polityką prywatności, zasadami postępowania z danymi oraz wymaganiami w zakresie zgody i informacji dobrze widocznych dla użytkownika;
- aplikacja, która rejestruje zawartość ekranu na urządzeniu użytkownika i nie traktuje tych danych jako osobowych ani poufnych zgodnie z tymi zasadami;
- aplikacja, która zbiera dane o lokalizacji urządzenia i nie informuje wyczerpująco o sposobie ich użycia ani nie prosi o zgodę na ich użycie, jak nakazują powyższe wymagania;
- aplikacja, która korzysta w tle z uprawnień z ograniczeniami, w tym z uprawnień do śledzenia, prowadzenia badań i marketingu, i nie informuje wyczerpująco o sposobie użycia tych danych ani nie prosi o zgodę na ich użycie, jak nakazują powyższe wymagania.

Określone ograniczenia związane z dostępem do poufnych danych

Tabela poniżej zawiera obowiązujące dodatkowo wymagania związane z określonymi czynnościami.

Aktywność	Wymaganie
Aplikacja obsługuje informacje finansowe, dane związane z płatnościami lub urzędowe numery identyfikacyjne	Aplikacja nie może nigdy publicznie ujawniać żadnych danych osobowych ani poufnych użytkownika dotyczących finansów, płatności lub urzędowych numerów identyfikacyjnych.
Aplikacja obsługuje niepubliczne informacje z książki telefonicznej i kontaktów	Nie wolno bez upoważnienia publikować ani ujawniać niepublicznych danych kontaktowych innych osób.
Aplikacja zawiera funkcje antywirusowe, funkcje bezpieczeństwa, np. chroniące przed wirusami i złośliwym oprogramowaniem, lub funkcje zwiększające bezpieczeństwo	Aplikacja musi mieć opublikowaną politykę prywatności, która wraz z innymi objaśnieniami w aplikacji informuje o zakresie zbierania i przekazywania danych użytkownika, sposobie ich użycia oraz o tym, komu są one udostępniane.

EU-U.S. Privacy Shield (Tarcza Prywatności UE-USA)

Tarcza Prywatności

Jeśli uzyskujesz dostęp do danych osobowych udostępnionych przez Google, korzystasz z nich lub je przetwarzasz, przy czym dane te umożliwiają identyfikację określonych osób i pochodzą z Unii Europejskiej lub Szwajcarii („Dane osobowe pochodzące z UE"), musisz:

- zachować zgodność ze wszystkimi obowiązującymi przepisami prawa, dyrektywami, rozporządzeniami i zasadami dotyczącymi prywatności oraz bezpieczeństwa i ochrony danych;
- uzyskiwać dostęp do Danych osobowych pochodzących z UE oraz korzystać z nich i przetwarzać je tylko w takim celu, na jaki zgadza się osoba, której one dotyczą;
- stosować odpowiednie środki organizacyjne i techniczne, by zabezpieczyć Dane osobowe pochodzące z UE przed ich utratą, użyciem niezgodnym z przeznaczeniem oraz nieautoryzowanym lub nieuprawnionym dostępem, ujawnieniem, modyfikacją bądź zniszczeniem;
- zapewnić taki sam poziom ochrony, jakiego wymagają zasady programu Privacy Shield (Tarcza Prywatności).

Masz obowiązek regularnego monitorowania zgodności z wymienionymi warunkami. Jeśli w którymkolwiek momencie utracisz możliwość zachowania zgodności z tymi warunkami lub wystąpi poważne ryzyko, że tak się stanie, musisz natychmiast powiadomić nas o tym, wysyłając e-maila na adres data-protection-office@google.com, oraz niezwłocznie przerwać przetwarzanie danych osobowych pochodzących z UE lub podjąć uzasadnione i właściwe kroki w celu przywrócenia odpowiedniego poziomu ochrony.

Uprawnienia

Prośby o przyznanie uprawnień powinny być zrozumiałe dla użytkowników. Możesz prosić tylko o uprawnienia, które są konieczne do zaimplementowania bieżących funkcji lub usług wymienionych w informacjach o aplikacji w Sklepie Play. Nie można używać uprawnień, które przyznają dostęp do danych użytkownika lub urządzenia, na potrzeby funkcji lub działań, które są nieujawnione, niezaimplementowane albo niedozwolone. Nigdy nie wolno sprzedawać danych osobowych ani informacji poufnych, do których dostęp uzyskiwany jest po udzieleniu uprawnień.

Wyświetlaj prośby o dostęp do danych użytkownika w odpowiednim kontekście (stosując uwierzytelnianie stopniowe). Dzięki temu użytkownicy będą rozumieć, do czego aplikacji potrzebne są konkretne dane. Dane mogą być wykorzystywane wyłącznie w celach, na które użytkownik wyraził zgodę. Jeśli chcesz użyć danych w innych celach, zapytaj użytkowników, czy zgadzają się na dodatkowe sposoby korzystania z danych i uzyskaj od nich taką zgodę.

Uprawnienia z ograniczeniami

W uzupełnieniu powyższego – uprawnienia z ograniczeniami to takie, które są określane jako niebezpieczne, szczególne lub wymagające podpisu. Podlegają one tym dodatkowym wymaganiom i ograniczeniom:

- Poufne dane użytkownika lub urządzenia, do których uzyskano dostęp na podstawie uprawnień z ograniczeniami, mogą być przekazywane osobom trzecim tylko do zapewnienia działania bieżących funkcji lub usług aplikacji, w której zebrano te dane. Dane można też przekazać w razie potrzeby, gdy jest to wymagane przez obowiązujące prawo albo w ramach fuzji lub przejęcia firmy bądź sprzedaży jej aktywów. Konieczne jest wtedy zgodne z przepisami powiadomienie o tym użytkowników. Inne rodzaje przekazywania lub sprzedaży danych użytkownika są zabronione.
- Jeśli użytkownik odrzuci prośbę o przyznanie uprawnienia z ograniczeniami, musisz uszanować jego decyzję. Nie wolno fałszywie nakłaniać ani zmuszać użytkowników do przyznawania uprawnień, które nie mają krytycznego

znaczenia. Musisz podjąć uzasadnione działania, by dostosować funkcjonowanie aplikacji do użytkowników, którzy nie przyznali dostępu do uprawnień newralgicznych (np. umożliwiając ręczne wpisanie numeru telefonu użytkownikowi, który ograniczył dostęp aplikacji do rejestru połączeń).

Niektóre uprawnienia z ograniczeniami są objęte dodatkowymi wymaganiami (szczegóły znajdują się poniżej). Takie ograniczenia mają chronić prywatność użytkownika. W bardzo rzadkich przypadkach możemy zgodzić się na odstępstwa od podanych poniżej wymagań, gdy aplikacja oferuje funkcje, które są bardzo atrakcyjne lub mają znaczenie krytyczne i nie można ich zapewnić w inny sposób. Takie wyjątki rozważamy, biorąc pod uwagę potencjalne zagrożenia dla prywatności i bezpieczeństwa użytkowników.

Uprawnienia dostępu do SMS-ów i rejestru połączeń

Uprawnienia dostępu do SMS-ów i rejestru połączeń są traktowane jako osobowe i poufne dane użytkownika. Podlegają zasadom opisanym w sekcji Dane osobowe i poufne oraz tym ograniczeniom:

Uprawnienia z ograniczeniami	Wymaganie
Manifest aplikacji prosi o grupę uprawnień Rejestr połączeń (np. READ_CALL_LOG, WRITE_CALL_LOG czy PROCESS_OUTGOING_CALLS)	Musi być aktywnie zarejestrowana jako domyślna aplikacja telefonu lub pomocnicza na urządzeniu.
Manifest aplikacji prosi o grupę uprawnień SMS (np. READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH czy RECEIVE_MMS)	Musi być aktywnie zarejestrowana jako domyślna aplikacja do obsługi SMS-ów lub Asystenta na urządzeniu.

Aplikacje, których nie można ustawić jako domyślnej aplikacji do obsługi SMS-ów, telefonu lub Asystenta, nie mogą deklarować korzystania z powyższych uprawnień w manifeście. Obejmuje to tekst zastępczy w manifeście. Poza tym, zanim aplikacja wyświetli użytkownikowi prośbę o zaakceptowanie dowolnego z powyższych uprawnień, musi być aktywnie zarejestrowana jako domyślna aplikacja do obsługi SMS-ów, telefonu lub Asystenta. Musi też niezwłocznie przestać korzystać z danego uprawnienia, gdy straci status domyślnej aplikacji do obsługi. Dozwolone przypadki użycia i wyjątki są opisane na tej stronie w Centrum pomocy.

Aplikacja może korzystać z uprawnień (i dowolnych danych uzyskanych na ich podstawie) wyłącznie do udostępniania swoich zatwierdzonych, kluczowych funkcji. Kluczowa funkcja to podstawowe przeznaczenie aplikacji. Może to być zestaw podstawowych funkcji, z których każda musi być w widoczny sposób udokumentowana i wskazana w opisie aplikacji. Aplikacja bez kluczowych funkcji jest uważana za „zepsutą", czyli bezużyteczną. Przesyłanie, udostępnianie lub licencjonowane użycie tych danych może odbywać się wyłącznie w związku z zapewnianiem działania kluczowych funkcji i usług aplikacji. Nie wolno używać tych danych do innych celów (np. usprawniania innych aplikacji lub usług bądź w celach marketingowych). Do odczytywania danych uzyskiwanych na podstawie uprawnień dostępu do rejestru połączeń lub SMS-ów nie wolno używać alternatywnych rozwiązań (w tym innych uprawnień, interfejsów API ani źródeł zewnętrznych).

Dostęp do lokalizacji

Lokalizacja urządzenia jest traktowana jako osobowe i poufne dane użytkownika. Podlega ona zasadom opisanym w sekcji Dane osobowe i poufne oraz tym ograniczeniom:

- Aplikacja nie może korzystać z danych wymagających dostępu do lokalizacji (np. ACCESS_FINE_LOCATION, ACCESS_COARSE_LOCATION czy ACCESS_BACKGROUND_LOCATION), które nie są już konieczne do udostępniania bieżących funkcji lub usług aplikacji.
- Aplikacja nie powinna nigdy prosić użytkowników o dostęp do lokalizacji, jeśli ma to służyć tylko do wyświetlania reklam lub analizy danych. Aplikacje, w których dozwolone użycie tych danych jest poszerzone o wyświetlanie reklam, muszą być zgodne z naszymi Zasadami dotyczącymi reklam.
- Aplikacje powinny prosić o przyznanie dostępu na najniższym poziomie (np. do przybliżonej lokalizacji zamiast dokładnej oraz na pierwszym planie zamiast w tle) niezbędnym do zapewnienia działania funkcji lub usługi, która wymaga danych o lokalizacji. Użytkownicy powinni spodziewać się, że ta funkcja lub usługa potrzebuje żądanego poziomu dostępu do lokalizacji. Możemy odrzucić aplikacje, które proszą o dostęp do lokalizacji w tle lub z niej korzystają bez wystarczającego uzasadnienia.
- Lokalizacji w tle można używać wyłącznie do udostępniania użytkownikowi funkcji przynoszących mu korzyści i ściśle związanych z podstawowym przeznaczeniem aplikacji.

Aplikacja może korzystać z dostępu do lokalizacji jako usługa działająca na pierwszym planie (gdy aplikacja ma dostęp tylko na pierwszym planie, np. „podczas używania"), jeśli użycie to:

- jest kontynuacją wywołanego przez użytkownika działania w aplikacji;

- zostaje zakończone natychmiast po prawidłowym wykonaniu przez aplikację działania wywołanego przez użytkownika.

Aplikacje przeznaczone dla dzieci muszą być zgodne z zasadami programu Dla całej rodziny.

Uprawnienia dostępu do wszystkich plików

Atrybuty plików i katalogów na urządzeniu użytkownika są traktowane jako osobowe i poufne dane użytkownika. Podlegają zasadom opisanym w sekcji Dane osobowe i poufne oraz tym ograniczeniom:

- Aplikacje powinny prosić o dostęp do pamięci urządzenia, jeśli jest on niezbędny do działania aplikacji, i nie mogą prosić o dostęp do pamięci urządzenia w imieniu osób trzecich w żadnym celu niezwiązanym z niezbędnymi, widocznymi dla użytkownika funkcjami aplikacji.
- Urządzenia z Androidem w wersji R (Android 11, poziom API 30) lub nowszej wymagają uprawnień MANAGE_EXTERNAL_STORAGE, by zarządzać dostępem w pamięci udostępnionej. Wszystkie aplikacje kierowane na Androida R i żądające szerokiego dostępu do pamięci udostępnionej („Dostęp do wszystkich plików") muszą pomyślnie przejść odpowiednią kontrolę dostępu przed opublikowaniem. Aplikacje, które mogą korzystać z tych uprawnień, muszą wyraźnie informować użytkowników o włączeniu opcji „Dostęp do wszystkich plików" w ustawieniach „Aplikacje ze specjalnym dostępem". Więcej informacji o wymaganiach dotyczących Androida R znajdziesz w tym artykule pomocy.

Używanie urządzeń lub sieci niezgodnie z przeznaczeniem

Zabraniamy publikowania aplikacji, które zakłócają działanie lub powodują uszkodzenie urządzenia użytkownika, innych urządzeń bądź komputerów, serwerów, sieci, interfejsów programowania aplikacji (API) czy usług albo uzyskują do nich nieautoryzowany dostęp. Dotyczy to m.in. innych aplikacji na urządzeniu, wszelkich usług Google oraz autoryzowanych sieci operatorów komórkowych.

Aplikacje w Google Play muszą spełniać domyślne wymagania optymalizacji pod względem działania na systemie Android opisane w kluczowych wytycznych dotyczących jakości aplikacji w Google Play.

Aplikacja rozpowszechniana w Google Play nie może samodzielnie się modyfikować, zastępować ani aktualizować przy użyciu metody innej niż mechanizm aktualizacji Google Play. Aplikacja nie może też pobierać kodu wykonywalnego (np. plików .dex, .jar i .so) z innego źródła niż Google Play. Nie dotyczy to kodu, który jest uruchamiany na maszynie wirtualnej i ma ograniczony dostęp do interfejsu API Androida (na przykład JavaScript w WebView lub przeglądarce).

Zabraniamy wykorzystywania kodu, który wprowadza lub wykorzystuje luki w zabezpieczeniach. Zapoznaj się z naszym Programem ulepszania zabezpieczeń aplikacji, by dowiedzieć się, jakie problemy z zabezpieczeniami zostały ostatnio zgłoszone deweloperom.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje blokujące lub zakłócające działanie innych aplikacji wyświetlających reklamy;
- aplikacje do oszukiwania w grach, które wpływają na rozgrywkę w innych aplikacjach;
- aplikacje umożliwiające hakowanie usług, oprogramowania lub sprzętu albo omijanie zabezpieczeń lub aplikacje zawierające instrukcje wykonania tych czynności;
- aplikacje mające dostęp do usług lub interfejsów API albo używające ich w sposób niezgodny z ich warunkami korzystania;
- aplikacje próbujące obejść systemowe zarządzanie energią, które nie kwalifikują się do umieszczenia na białej liście;
- aplikacje umożliwiające dostęp do innych usług przez serwery proxy mogą działać w ten sposób tylko wtedy, gdy jest to ich główna funkcja widoczna dla użytkowników;
- aplikacje lub kod innej firmy (np. pakiety SDK) pobierające kod wykonywalny (np. pliki .dex lub kod natywny) ze źródła innego niż Google Play;
- aplikacje instalujące inne aplikacje na urządzeniu bez uprzedniej zgody użytkownika;
- aplikacje z linkami prowadzącymi do instalatorów złośliwego oprogramowania lub umożliwiające jego instalację bądź dystrybucję.

Wprowadzanie w błąd

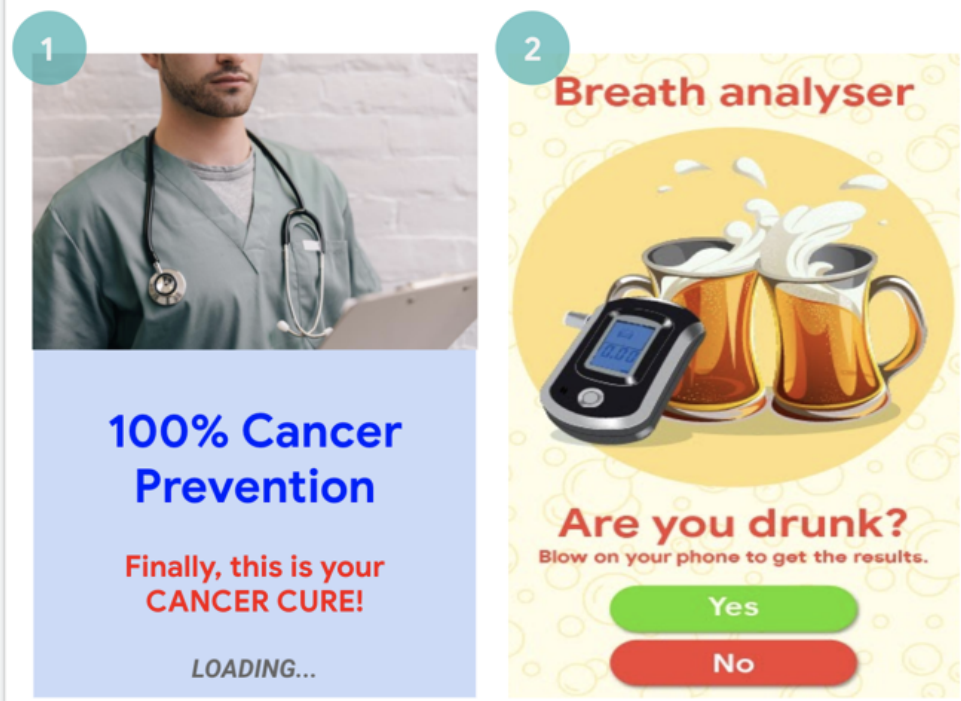
Zabraniamy publikowania aplikacji, które mogą wprowadzać użytkowników w błąd lub umożliwiać nieuczciwe postępowanie, w tym m.in. aplikacji, których działanie uznano za niemożliwe. Aplikacje muszą zawierać, opisywać i prezentować za pomocą zdjęć lub filmów swój sposób działania we wszystkich częściach metadanych. Nie mogą naśladować funkcji ani ostrzeżeń systemu operacyjnego lub innych aplikacji. Wszelkie zmiany w ustawieniach urządzenia muszą być wprowadzane za wiedzą i zgodą użytkownika. Powinny też dać się cofnąć.

Twierdzenia wprowadzające w błąd

Zabraniamy publikowania aplikacji zawierających fałszywe lub mylące informacje, m.in. w opisach, tytułach, ikonach i na zrzutach ekranu.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje z opisem niezgodnym z prawdą lub niedokładnym i niejasno przedstawiającym oferowane funkcje:
  - aplikacja, której opis i zrzuty ekranu wskazują, że jest grą wyścigową (obraz przedstawiający samochód), a w rzeczywistości jest grą logiczną;
  - aplikacja rzekomo będąca oprogramowaniem antywirusowym, ale zawierająca tylko poradnik dotyczący usuwania wirusów;
- mylące opisy dotyczące dewelopera lub aplikacji, które są niezgodne ze statusem lub popularnością w Google Play (np. „Wybór redakcji", „Najlepsza aplikacja", „Najlepsza płatna");
- aplikacje zawierające funkcje o charakterze medycznym lub związanym ze zdrowiem, które wprowadzają użytkowników w błąd i mogą wyrządzać szkody;
- aplikacje rzekomo zawierające funkcje, których zaimplementowanie nie jest możliwe (np. aplikacje zwalczające szkodniki), nawet jeśli wyraźnie zaznaczono, że jest to żart czy dowcip;
- aplikacje, które są nieprawidłowo skategoryzowane, m.in. w zakresie oceny lub kategorii;
- treści wyraźnie wprowadzające w błąd, które mogą wpływać na decyzje wyborcze użytkowników;
- aplikacje, które niezgodnie z prawdą twierdzą, że są powiązane z organem państwowym lub umożliwiają załatwianie spraw urzędowych, choć nie mają wymaganych uprawnień;
- aplikacje sugerujące, że są oficjalnymi aplikacjami uznanego podmiotu (tytuły takie jak „Oficjalna aplikacja Justina Biebera" nie są dozwolone, jeśli deweloper nie uzyskał potrzebnych pozwoleń lub praw).



(1) Ta aplikacja zawiera twierdzenia o charakterze medycznym lub zdrowotnym (lek na raka), które wprowadzają w błąd.
(2) Ta aplikacja zawiera funkcje, których zaimplementowanie nie jest możliwe (użycie telefonu jako alkomatu).

Zmiany ustawień urządzenia wprowadzające w błąd

Zabronione jest publikowanie aplikacji wprowadzających zmiany poza samą aplikacją, w ustawieniach lub funkcjach urządzenia, bez wiedzy i zgody użytkownika. Ustawienia i funkcje urządzenia to między innymi ustawienia systemowe i ustawienia przeglądarki, a także zakładki, skróty, ikony, widżety oraz informacje określające wyświetlanie aplikacji na ekranie głównym.

Dodatkowo nie są dozwolone:

- aplikacje modyfikujące ustawienia lub funkcje urządzenia za zgodą użytkownika, ale robiące to tak, że zmiany te trudno cofnąć;
- aplikacje lub reklamy zmieniające ustawienia lub funkcje urządzenia, by prowadziły do usług innych firm lub służyły do celów reklamowych;

- aplikacje podstępem doprowadzające użytkowników do usunięcia lub wyłączenia aplikacji firm zewnętrznych lub zmiany ustawień urządzenia bądź funkcji;
- aplikacje zachęcające lub nakłaniające użytkowników do usunięcia lub wyłączenia aplikacji innych firm lub do zmiany ustawień bądź funkcji urządzenia, chyba że dzieje się to w ramach możliwej do zweryfikowania usługi zabezpieczeń.

Umożliwianie nieuczciwego postępowania

Zabraniamy publikowania aplikacji, które ułatwiają użytkownikom wprowadzanie w błąd innych osób lub powodują jakiekolwiek działania wprowadzające w błąd, w tym m.in. aplikacji generujących lub umożliwiających generowanie dowodów osobistych, numerów ubezpieczenia społecznego, paszportów, dyplomów, kart kredytowych czy praw jazdy. Aplikacje muszą prawidłowo ujawniać, tytułować, opisywać i prezentować za pomocą zdjęć lub filmów swój sposób działania lub swoją zawartość, a także działać w sposób, jakiego oczekuje użytkownik.

Dodatkowe zasoby aplikacji (na przykład zasoby gry) mogą być pobierane tylko wtedy, gdy są użytkownikowi niezbędne do korzystania z aplikacji. Pobrane zasoby muszą być zgodne ze wszystkimi zasadami Google Play. Przed rozpoczęciem pobierania aplikacja musi poprosić użytkownika o zgodę, jednoznacznie określając rozmiar pobieranego pliku.

Aplikacja musi przestrzegać naszych zasad, nawet jeśli powstała „dla żartu" lub „w celach rozrywkowych" (albo podobnych).

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje, które udają inne aplikacje bądź witryny w celu nakłonienia użytkowników do ujawnienia danych osobowych lub uwierzytelniających;
- aplikacje przedstawiające niezweryfikowane lub prawdziwe numery telefonu, kontakty, adresy bądź informacje umożliwiające identyfikację osób lub podmiotów, które nie wyraziły zgody na wykorzystanie takich informacji;
- aplikacje, których najważniejsze funkcje różnią się w zależności od lokalizacji geograficznej użytkownika, parametrów urządzenia lub innych danych zależnych od użytkownika, a różnice te nie są wyraźnie widoczne na stronie z informacjami o aplikacji;
- aplikacje, które zmieniają się znacznie z wersji na wersję bez powiadamiania o tym użytkownika (np. w sekcji „Co nowego") i aktualizowania strony z informacjami o aplikacji;
- aplikacje, które podczas sprawdzania próbują zmienić lub ukryć swoje zachowanie;
- aplikacje, którym sieć dystrybucji treści (CDN) umożliwia pobieranie plików bez pytania użytkownika o zgodę i informowania go o rozmiarze pliku przed rozpoczęciem pobierania.

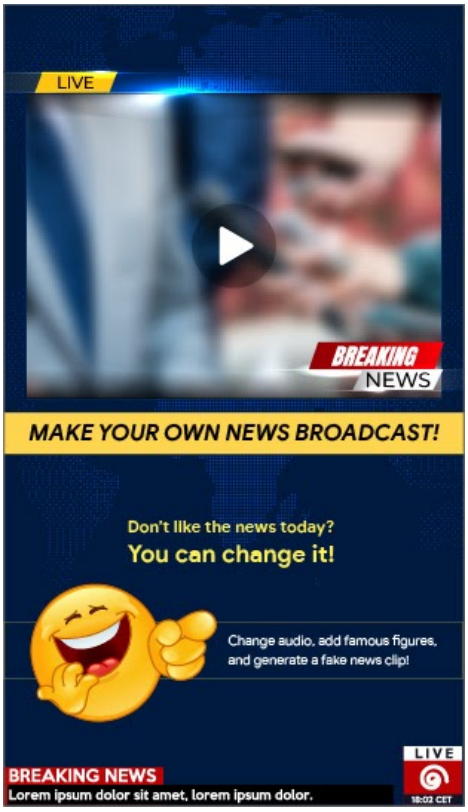
Modyfikacje plików multimedialnych

Zabraniamy publikowania aplikacji, które promują lub pomagają tworzyć fałszywe bądź wprowadzające w błąd informacje lub twierdzenia przy użyciu obrazów, filmów lub tekstu. Nie dopuszczamy aplikacji mających na celu promowanie lub podtrzymywanie niepodważalnie fałszywych lub wprowadzających w błąd obrazów, filmów bądź tekstów, które mogą powodować szkody, jeśli odnoszą się do dramatycznych wydarzeń, polityki, kwestii społecznych lub spraw istotnych z punktu widzenia zainteresowania publicznego.

Aplikacje, które modyfikują pliki multimedialne w zakresie wykraczającym poza typowe, akceptowalne z edytorskiego punktu widzenia poprawki ostrości lub jakości, muszą wyraźnie informować, że plik został zmieniony, lub dodawać do niego znak wodny w sytuacjach, gdy dla przeciętnego użytkownika mogłoby nie być oczywiste, że plik został zmieniony. Wyjątek może stanowić interes publiczny bądź oczywista satyra lub parodia.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje umożliwiające dodanie osoby publicznej do demonstracji w okresie napiętej sytuacji politycznej;
- aplikacje wykorzystujące osoby publiczne lub pliki multimedialne związane z ważnymi wydarzeniami politycznymi do reklamowania na stronie z informacjami o aplikacji możliwości modyfikowania treści multimedialnych;
- aplikacje umożliwiające modyfikowanie klipów multimedialnych, tak by przypominały transmisję wiadomości.



(1) Ta aplikacja umożliwia modyfikowanie klipów multimedialnych, tak by przypominały transmisję wiadomości, oraz dodawanie znanych lub publicznych osób do klipu bez zamieszczenia znaku wodnego.

Wprowadzanie w błąd

Nie dopuszczamy aplikacji ani kont deweloperów podszywających się pod jakąkolwiek osobę lub organizację albo fałszywie identyfikujących lub ukrywających swojego właściciela bądź główny cel. Zabronione są aplikacje i konta programistów, które współdziałają, by wprowadzić użytkowników w błąd. Dotyczy to m.in. aplikacji i kont deweloperów ukrywających lub fałszywie identyfikujących kraj, z którego pochodzą, a oferujących treści skierowane do użytkowników w innym kraju.

Złośliwe oprogramowanie

Złośliwe oprogramowanie to każdy kod, który mógłby narazić na ryzyko użytkownika albo jego dane lub urządzenie. Do tego typu oprogramowania zaliczamy m.in. potencjalnie szkodliwe aplikacje, pliki binarne i modyfikacje platform, wśród których wyróżniamy kategorie takie jak konie trojańskie, phishing czy aplikacje szpiegowskie – lista tych kategorii jest cały czas aktualizowana i uzupełniana.

Złośliwe oprogramowanie

Nasze zasady dotyczące złośliwego oprogramowania są proste: ekosystem Androida, łącznie ze Sklepem Google Play, oraz urządzenia użytkowników powinny być wolne od złośliwych działań (tj. wykonywanych przez złośliwe oprogramowanie). Kierując się tą podstawową zasadą, staramy się zapewnić użytkownikom i ich urządzeniom z Androidem bezpieczny ekosystem.

Złośliwe oprogramowanie ma różne formy i możliwości, jednak zwykle jest tworzone w jednym z tych celów:

- naruszenie integralności urządzenia użytkownika;
- przejęcie kontroli nad urządzeniem użytkownika;
- umożliwienie osobie przeprowadzającej atak podejmowania zdalnych działań mających na celu uzyskanie dostępu do zainfekowanego urządzenia, używanie go lub eksploatowanie go w jakikolwiek inny sposób;
- wysłanie z urządzenia danych osobowych lub danych logowania bez wiedzy i zgody użytkownika;
- rozsyłanie spamu lub poleceń z zainfekowanych urządzeń na inne urządzenia lub do sieci;
- oszukanie użytkownika.

Aplikacje, pliki binarne lub modyfikacje platformy mogą być szkodliwe, tzn. mogą wykazywać złośliwe zachowania, nawet jeśli nie taka była intencja ich twórców. Dzieje się tak, ponieważ aplikacje, pliki binarne i modyfikacje platformy mogą

działać inaczej w zależności od różnych zmiennych. Coś, co jednemu urządzeniu z Androidem szkodzi, dla innego może nie stanowić zagrożenia. Na przykład szkodliwe aplikacje, które wykorzystują do podejmowania złośliwych zachowań wycofane interfejsy API, nie zaszkodzą urządzeniu z najnowszą wersją Androida, jednak urządzenia z jego bardzo wczesną wersją mogą być narażone na ryzyko. Aplikacje, pliki binarne i modyfikacje platformy są oznaczane jako złośliwe oprogramowanie lub potencjalnie szkodliwe aplikacje, jeśli stwarzają wyraźne ryzyko dla niektórych lub wszystkich urządzeń z Androidem i ich użytkowników.

Poniższe kategorie złośliwego oprogramowania opracowaliśmy zgodnie z naszym głębokim przekonaniem, że użytkownicy powinni rozumieć, w jaki sposób ich urządzenia są wykorzystywane. Ułatwiają nam one tworzenie bezpiecznego ekosystemu, w którym możliwe jest wprowadzanie zdecydowanych innowacji i budowanie zaufania użytkowników.

Więcej informacji znajdziesz na stronie Google Play Protect.

Tajny dostęp

Jest to kod, który umożliwia przeprowadzenie na urządzeniu niechcianych, potencjalnie szkodliwych, kontrolowanych zdalnie operacji.

Mogą to być działania, których automatyczne wykonanie powodowałoby zaliczenie aplikacji, pliku binarnego lub modyfikacji platformy do jednej z kategorii złośliwego oprogramowania. Ogólnie rzecz biorąc, określenie „tajny dostęp” odnosi się do tego, w jaki sposób na urządzeniu może dojść do potencjalnie szkodliwych działań, dlatego nie można go do końca zakwalifikować do takich kategorii jak oszustwa związane z płatnościami czy komercyjne programy szpiegowskie. Z tego względu podkategoria tajnego dostępu jest czasem traktowana przez Google Play Protect jak luka w zabezpieczeniach.

Oszukańcze płatności

Jest to kod, który wprowadza użytkownika w błąd i powoduje automatyczne naliczanie opłat.

Wśród oszukańczych płatności mobilnych wyróżniamy oszukańcze SMS-y, połączenia i abonamenty.

Oszukańcze SMS-y

Jest to kod, który powoduje naliczanie dodatkowych opłat za wysyłanie specjalnych SMS-ów bez pytania użytkownika o zgodę lub próbuje zamaskować aktywność związaną z obsługą wiadomości SMS przez ukrywanie umów albo powiadomień od operatora informujących użytkownika o pobieraniu opłat lub potwierdzających rozpoczęcie subskrypcji.

Czasami kod, technicznie rzecz biorąc, nie ukrywa wysyłania SMS-ów, ale wprowadza dodatkowe zachowania umożliwiające oszustwo. Przykłady obejmują ukrywanie fragmentów umowy przed użytkownikiem i blokowanie powiadomień SMS od operatora sieci komórkowej, które informują użytkownika o naliczaniu opłat lub rozpoczęciu subskrypcji.

Oszukańcze połączenia

Jest to kod, który powoduje naliczanie dodatkowych opłat za specjalne połączenia telefoniczne bez uzyskania zgody użytkownika.

Oszukańcze abonamenty

Jest to kod, który wprowadza użytkownika w błąd i powoduje dokonywanie niezamierzonych zakupów (w tym subskrypcji) przy użyciu rozliczeń przez operatora.

Takie oszustwa obejmują dowolny rodzaj opłat poza specjalnymi SMS-ami i połączeniami. Mogą to być płatności bezpośrednio u operatora, jak również opłaty za korzystanie z bezprzewodowych punktów dostępu czy transmisję danych. Najczęściej stosowane są opłaty za bezprzewodowe punkty dostępu. Użytkownik jest zwykle nakłaniany, by kliknął przycisk na dyskretnie wczytanym, przezroczystym komponencie WebView. Po wykonaniu takiej czynności rozpoczyna się uruchomienie cyklicznie odnawianej subskrypcji, a potwierdzający to SMS lub e-mail jest często przechwytywany, by użytkownik nie zauważył transakcji.

Stalkerware

Kod, który przekazuje dane osobowe z urządzenia bez jawnego powiadomienia lub uzyskania zgody użytkownika oraz nie wyświetla stałego powiadomienia o takim przekazywaniu.

Aplikacje typu stalkerware zwykle przesyłają dane do podmiotu innego niż dostawca potencjalnie szkodliwej aplikacji.

Rodzice mogą używać aplikacji działających na podobnej zasadzie do monitorowania dzieci (jest to dozwolone). Należy jednak pamiętać, że tego rodzaju aplikacji nie wolno używać do śledzenia użytkownika (np. małżonka) bez jego wiedzy lub zgody, chyba że wyświetli się stałe powiadomienie o przesyłaniu danych.

W Sklepie Play można publikować aplikacje z funkcjami śledzenia i raportowania, które są zgodne z naszymi zasadami i zostały opracowane (oraz tak są przedstawiane) jako służące do monitorowania dzieci przez rodziców oraz na potrzeby zarządzania w firmach – pod warunkiem, że są w pełni zgodne z wymaganiami opisanymi poniżej.

Rozpowszechniane w Sklepie Play aplikacje monitorujące lub śledzące zachowanie użytkownika na urządzeniu, inne niż stalkerware, muszą spełniać te wymagania:

- Aplikacje nie mogą prezentować się jako rozwiązania służące do szpiegowania lub podglądania.
- Aplikacje nie mogą ukrywać lub maskować monitorowania ani próbować wprowadzić użytkowników w błąd w odniesieniu do takich funkcji.
- Aplikacje muszą wyświetlać unikalną ikonę, która je identyfikuje, oraz stałe powiadomienie.
- Aplikacje i ich strony w Google Play nie mogą w żaden sposób umożliwiać aktywowania lub użycia funkcji, które naruszają nasze warunki, np. nie mogą zawierać linków do niezgodnego pakietu APK spoza Google Play.
- Ponosisz pełną odpowiedzialność za to, by Twoja aplikacja była zgodna z przepisami docelowego kraju lub regionu. Usuniemy aplikacje, które w danym miejscu zostaną uznane za nielegalne.

Atak typu DoS

Jest to kod, który bez wiedzy użytkownika wykonuje atak typu DoS lub jest częścią rozproszonego ataku typu DoS kierowanego na inne systemy i zasoby.

Może to np. polegać na masowym wysyłaniu żądań HTTP w celu wygenerowania nadmiernego obciążenia zdalnych serwerów.

Szkodliwe programy pobierające

Jest to kod, który sam w sobie nie jest groźny, ale pobiera inne potencjalnie szkodliwe aplikacje.

Kod może być uznany za służący do pobierania szkodliwych elementów w tych przypadkach:

- Istnieje podejrzenie, że kod został utworzony do pobierania potencjalnie szkodliwych aplikacji, pobrał takie aplikacje lub zawiera kod, który może pobierać i instalować aplikacje.
- Co najmniej 5% aplikacji pobranych przez ten kod to potencjalnie szkodliwe aplikacje. Minimalny próg wyliczeń to 500 zarejestrowanych pobrań aplikacji (25 zarejestrowanych pobrań potencjalnie szkodliwych aplikacji).

Główne przeglądarki i aplikacje do udostępniania plików nie są uznawane za szkodliwe programy pobierające, jeśli spełniają te warunki:

- Nie pobierają plików bez interakcji użytkownika.
- Wszystkie pobrania potencjalnie szkodliwych aplikacji są uruchomione przez użytkowników wyrażających na to zgodę.

Zagrożenie, które nie obejmuje Androida

Jest to kod zawierający zagrożenia, które nie dotyczą Androida.

Takie aplikacje nie są zagrożeniem dla użytkownika urządzenia z Androidem ani samego urządzenia z tym systemem, ale zawierają komponenty, które mogą być szkodliwe na innych platformach.

Phishing

Jest to kod, który stwarza pozory, że pochodzi z zaufanego źródła, żądający od użytkownika danych uwierzytelniających lub informacji rozliczeniowych w celu wysłania ich do osoby trzeciej. Ta kategoria obejmuje również kod, który przechwytuje dane logowania użytkownika podczas ich przesyłania.

Częstym celem ataków phishingowych są dane logowania do banku, numery kart kredytowych i dane logowania na konta internetowe w sieciach społecznościowych lub grach.

Nadużywanie podwyższonych uprawnień

Jest to kod, który narusza integralność systemu przez uszkodzenie piaskownicy aplikacji, zdobycie podwyższonych uprawnień albo zmianę lub wyłączenie dostępu do podstawowych funkcji związanych z bezpieczeństwem.

Przykłady:

- Aplikacja, która nie jest zgodna z modelem uprawnień Androida lub wykrada dane logowania (na przykład tokeny OAuth) z innych aplikacji.

- Aplikacje, które nadużywają różnych funkcji, by uniemożliwić ich odinstalowanie lub zatrzymanie.
- Aplikacja, która wyłącza SELinux.

Aplikacje eskalujące uprawnienia, które umożliwiają dostęp do roota urządzenia bez pytania użytkownika o zgodę, są klasyfikowane jako aplikacje umożliwiające dostęp do roota.

Ransomware

Jest to kod, który częściowo lub w znacznym stopniu przejmuje kontrolę nad urządzeniem bądź danymi na urządzeniu i żąda od użytkownika płatności lub wykonania jakiejś czynności w zamian za zwrócenie kontroli.

Niektóre programy typu ransomware szyfrują dane na urządzeniu i żądają płatności w zamian za ich odszyfrowanie lub wykorzystują funkcje administracyjne urządzenia, by typowy użytkownik nie był w stanie ich usunąć. Przykłady:

- Uniemożliwienie użytkownikowi dostępu do urządzenia i żądanie pieniędzy w zamian za zwrócenie kontroli.
- Szyfrowanie danych na urządzeniu i żądanie zapłaty, po której rzekomo ma nastąpić odszyfrowanie.
- Wykorzystywanie funkcji menedżera zasad urządzenia w celu uniemożliwienia użytkownikowi usunięcia aplikacji.

Kod rozpowszechniany razem z urządzeniem, którego głównym celem jest finansowanie zarządzania urządzeniem, może być wykluczony z kategorii ransomware, jeśli spełni wymagania dotyczące bezpiecznego blokowania urządzenia i zarządzania nim oraz odpowiedniego informowania użytkownika i uzyskiwania jego zgody.

Dostęp do roota

Jest to kod, który uzyskuje dostęp do roota na urządzeniu.

Kod umożliwiający dostęp do roota może być nieszkodliwy lub szkodliwy. Nieszkodliwe aplikacje z dostępem do roota powiadamiają użytkownika o zamiarze uzyskania dostępu do roota – nie wykonują groźnych działań, które są charakterystyczne dla innych potencjalnie szkodliwych aplikacji.

Złośliwe aplikacje z dostępem do roota nie informują użytkownika o zamiarze uzyskania takiego dostępu albo powiadamiają o tym użytkownika, ale wykonują też inne działania, które kwalifikują je jako potencjalnie szkodliwe.

Spam

Jest to kod, który wysyła niechciane wiadomości do kontaktów użytkownika lub wykorzystuje urządzenie jako narzędzie do wysyłania spamerskich e-maili.

Programy szpiegowskie

Jest to kod, który przekazuje dane osobowe z urządzenia bez wiedzy i zgody użytkownika.

Za działanie programu szpiegowskiego można uznać np. przekazywanie którychkolwiek z poniższych danych bez ujawniania tego faktu użytkownikowi lub w sposób, którego użytkownik się nie spodziewa:

- lista kontaktów,
- zdjęcia lub inne pliki pochodzące z karty SD bądź nienależące do aplikacji,
- treści z konta e-mail użytkownika,
- rejestr połączeń,
- rejestr SMS-ów,
- historia online lub zakładki z domyślnej przeglądarki,
- informacje z katalogów /data/ innych aplikacji.

Działania, które mogą uchodzić za szpiegowanie użytkownika, mogą też zostać oznaczone jako działanie programu szpiegowskiego. Jako przykład takich działań można podać nagrywanie dźwięku lub rozmów telefonicznych albo wykradanie danych aplikacji.

Koń trojański

Jest to kod, który stwarza wrażenie niegroźnego (np. gra rzekomo będąca zwykłą grą), ale w rzeczywistości wykonuje niepożądane działania skierowane przeciwko użytkownikowi.

Tej klasyfikacji używa się zwykle w połączeniu z innymi kategoriami potencjalnie szkodliwych aplikacji. Koń trojański zawiera element nieszkodliwy oraz ukryty komponent szkodliwy. Może to być na przykład gra, która bez wiedzy użytkownika wysyła w tle specjalne SMS-y z urządzenia.

Uwaga na temat nietypowych aplikacji

Nowe lub rzadkie aplikacje mogą zostać uznane za nietypowe, jeśli Google Play Protect nie ma dość informacji, by zagwarantować, że są bezpieczne. Nie znaczy to, że aplikacja jest na pewno szkodliwa, jednak bez dalszej weryfikacji nie można tego wykluczyć.

Uwaga dotycząca kategorii „Tajny dostęp”

Zaliczenie złośliwego oprogramowania do kategorii „Tajny dostęp” zależy od zachowania, jakie wykazuje kod. Warunkiem koniecznym do zaliczenia kodu do tej kategorii jest umożliwianie przez niego działań, których automatyczne wykonanie mogłoby powodować zaliczenie tego kodu do jednej z innych kategorii złośliwego oprogramowania. Za złośliwe oprogramowanie typu „tajny dostęp” można na przykład uznać aplikację umożliwiającą dynamiczne ładowanie kodu, który następnie zacznie wyodrębniać SMS-y.

Jeśli jednak aplikacja umożliwia wykonanie dowolnego kodu, ale nie mamy podstaw, by sądzić, że jego wykonanie zostało dodane w celu podjęcia złośliwych działań, nie uznamy tej aplikacji za złośliwe oprogramowanie typu „Tajny dostęp”, a jedynie stwierdzimy, że ma ona luki w zabezpieczeniach, i poprosimy dewelopera o wprowadzenie poprawki.

Niechciane oprogramowanie mobilne

Ta zasada uzupełnia nasze Zasady dotyczące niechcianego oprogramowania – określa wytyczne dotyczące ekosystemu Androida i Sklepu Google Play. Oprogramowanie naruszające te zasady może być szkodliwe, dlatego staramy się chronić przed nim użytkowników.

Niechciane oprogramowanie mobilne

W Google uważamy, że jeśli skoncentrujemy się na użytkowniku, reszta przyjdzie sama. W naszych Zasadach dotyczących oprogramowania i Zasadach dotyczących niechcianego oprogramowania podajemy ogólne zalecenia dotyczące oprogramowania, które zapewnia użytkownikom pozytywne wrażenia. Ta zasada uzupełnia nasze Zasady dotyczące niechcianego oprogramowania – określa wytyczne dotyczące ekosystemu Androida i Sklepu Google Play. Oprogramowanie naruszające te zasady może być szkodliwe, dlatego staramy się chronić przed nim użytkowników.

Jak wspominamy w Zasadach dotyczących niechcianego oprogramowania, odkryliśmy, że większość oprogramowania tego typu ma co najmniej 1 z tych cech:

- wprowadza w błąd, obiecując korzyści, których w rzeczywistości nie przynosi;
- próbuje nakłonić użytkownika do instalacji lub instaluje się razem z innym programem;
- nie informuje użytkownika o swoich głównych lub istotnych funkcjach;
- w nieoczekiwany sposób wpływa na system użytkownika;
- gromadzi lub przesyła prywatne informacje bez wiedzy użytkownika;
- gromadzi lub przesyła prywatne informacje, nie zabezpieczając ich (np. za pomocą HTTPS);
- jest w pakiecie z innym oprogramowaniem, a jego obecność nie jest ujawniana.

Na urządzeniach mobilnych oprogramowanie to kod w formie aplikacji, pliku binarnego, modyfikacji platformy itp. Nie dopuszczamy oprogramowania szkodliwego dla ekosystemu oprogramowania lub zaburzającego wygodę użytkownika, dlatego będziemy podejmować działania wobec kodu, który narusza te zasady.

Poniżej zamieszczamy uzupełnienie Zasad dotyczących niechcianego oprogramowania, które rozszerza ich zastosowanie na aplikacje mobilne. Podobnie jak w przypadku tych zasad, Zasady dotyczące niechcianych aplikacji mobilnych także będziemy dopracowywać, uwzględniając kolejne rodzaje nadużyć.

Przejrzyste zachowanie i jednoznaczne informacje

Cały kod powinien być zgodny z tym, co deweloper obiecał użytkownikom. Aplikacje powinny mieć wszystkie opisywane funkcje. Aplikacje nie mogą wprowadzać użytkowników w błąd.

- Aplikacje powinny mieć jasno określone funkcje i cele.
- Jasno i wyraźnie wyjaśnij użytkownikowi, jakie zmiany w systemie wprowadzi aplikacja. Pozwól użytkownikom przejrzeć i zaakceptować wszystkie istotne opcje instalacji i zmiany.
- Oprogramowanie nie może błędnie przedstawiać użytkownikowi stanu jego urządzenia, na przykład twierdząc, że system jest w stanie krytycznym lub został zainfekowany wirusami.
- Nie używaj nieprawidłowej aktywności, by zwiększyć ruch z reklam lub liczbę konwersji.
- Zabraniamy publikowania aplikacji, które wprowadzają użytkowników w błąd, podszywając się pod inną osobę (np. innego dewelopera, firmę, podmiot) lub inną aplikację. Nie sugeruj, że Twoja aplikacja jest z kimś powiązana lub przez kogoś autoryzowana, jeśli tak nie jest.

Przykłady naruszenia zasad:

- oszustwo reklamowe,

- podszywanie się pod inne osoby.

Ochrona danych użytkownika

Jasno i zrozumiale informuj użytkowników o dostępie do danych osobowych i poufnych oraz ich używaniu i udostępnianiu. Wykorzystując dane użytkownika, musisz przestrzegać wszystkich obowiązujących zasad dotyczących danych użytkownika i podejmować odpowiednie środki, by te dane chronić.

- Daj użytkownikom możliwość wyrażenia zgody na zbieranie ich danych, zanim zaczniesz te dane zbierać i wysyłać z urządzenia. Dotyczy to danych o kontach osób trzecich, adresach e-mail, numerach telefonów, zainstalowanych aplikacjach, plikach, lokalizacji oraz wszelkich innych danych osobowych i poufnych, których zbierania użytkownik się nie spodziewał.
- Ze wszystkimi danymi osobowymi i poufnymi użytkownika postępuj w bezpieczny sposób, używając nowoczesnych metod szyfrowania (np. protokołu HTTPS).
- Oprogramowanie, w tym aplikacje mobilne, może przesyłać na serwery tylko te dane osobowe i poufne użytkowników, które są powiązane z działaniem aplikacji.

Przykłady naruszenia zasad:

- zbieranie danych (program szpiegowski),
- nadużycie uprawnienia z ograniczeniami.

Przykładowe zasady dotyczące danych użytkownika:

- *Zasady dotyczące danych użytkownika w Google Play*
- *Wymagania GMS dotyczące danych użytkownika*
- *Zasady usług interfejsu API Google dotyczące danych użytkownika*

Niezakłócanie działania urządzeń mobilnych

Obsługa aplikacji powinna być prosta, zrozumiała i oparta na jednoznacznych wyborach użytkownika. Aplikacja powinna przedstawiać użytkownikowi wyraźną propozycję wartości, a jej reklamowane lub oczekiwane działanie nie powinno być zakłócane.

- Nie wyświetlaj reklam, które pojawiają się w nieoczekiwany sposób, np. zakłócając lub utrudniając korzystanie z funkcji urządzenia, albo pokazują się poza środowiskiem aplikacji i nie mają możliwości łatwego zamknięcia, zaakceptowania czy atrybucji.
- Aplikacje nie mogą zakłócać działania urządzenia ani innych aplikacji.
- Proces odinstalowania (jeśli jest możliwy) powinien być jasny i zrozumiały.
- Aplikacje mobilne nie mogą wyświetlać komunikatów przypominających te z systemu operacyjnego urządzenia lub innych aplikacji. Nie ukrywaj przed użytkownikiem alertów z innych aplikacji lub systemu operacyjnego, szczególnie tych informujących użytkownika o zmianach w systemie operacyjnym.

Przykłady naruszenia zasad:

- uciążliwe reklamy,
- nieautoryzowane używanie funkcji systemowych lub podszywanie się pod nie.

Oszustwo reklamowe

Oszustwa reklamowe są surowo zabronione. Interakcje z reklamami generowane w celu przekonania sieci reklamowej, że ruch jest efektem autentycznego zainteresowania użytkownika, to oszustwo reklamowe, które jest formą nieprawidłowego ruchu. Oszustwa reklamowe mogą być efektem ubocznym działań deweloperów, którzy implementują reklamy w niedozwolony sposób, np. wyświetlają ukryte lub klikane automatycznie reklamy, modyfikują informacje albo w inny sposób wykorzystują działania automatyczne (roboty, boty itp.) lub wykonywane przez ludzi, które mają na celu wygenerowanie nieprawidłowego ruchu z reklam. Nieprawidłowy ruch i oszustwa reklamowe są szkodliwe dla reklamodawców, deweloperów i użytkowników oraz prowadzą do utraty zaufania do ekosystemu reklam mobilnych.

Oto kilka często spotykanych przykładów naruszenia zasad:

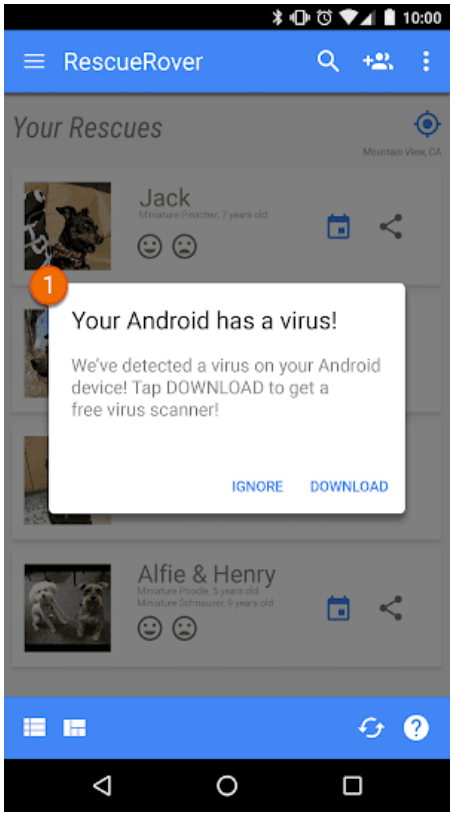
- aplikacja, która renderuje reklamy niewidoczne dla użytkownika;
- aplikacja, która automatycznie generuje niezamierzone przez użytkownika kliknięcia reklam albo generuje ruch w sieci pochodzący z fałszywego przypisywania kliknięć;
- aplikacja wysyłająca fałszywe informacje o atrybucji kliknięć przycisku instalacji, by otrzymać zapłatę za instalacje, które nie pochodzą z sieci nadawcy;
- aplikacja, która wyświetla wyskakujące reklamy, gdy użytkownik nie korzysta z jej interfejsu;
- aplikacja podająca fałszywe informacje o zasobach reklamowych, np. aplikacja informująca sieci reklamowe, że działa na urządzeniu z iOS, podczas gdy w rzeczywistości działa na urządzeniu z Androidem, albo aplikacja, która podaje nieprawdziwą nazwę pakietu, na którym zarabia deweloper.

Nieautoryzowane używanie funkcji systemowych lub podszywanie się pod nie

Niedozwolone są aplikacje i reklamy, które naśladują lub zakłócają funkcje systemowe, np. powiadomienia i ostrzeżenia. Powiadomienia na poziomie systemu mogą być używane tylko przez integralne funkcje aplikacji (np. aplikacja linii lotniczej może informować użytkowników o ofertach specjalnych, a gra powiadamiać o dostępnych w niej promocjach).

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje lub reklamy dostarczane przy użyciu powiadomienia lub alertu systemowego:



① Powiadomienie systemowe pokazane w tej aplikacji jest używane do wyświetlenia reklamy.

Więcej przykładów tego typu znajdziesz w zasadach dotyczących reklam.

Podszywanie się pod inne osoby

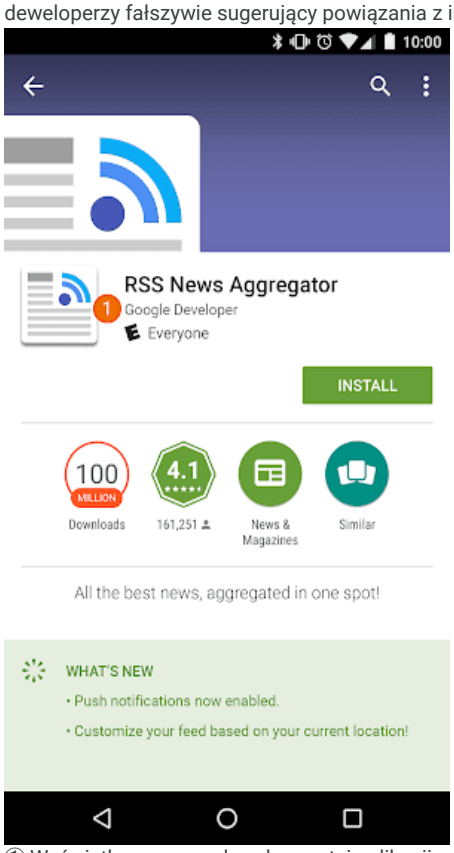
Gdy deweloperzy podszywają się pod inne osoby lub ich aplikacje, wprowadzają użytkowników w błąd i szkodzą społeczności deweloperów. Zabraniamy publikowania aplikacji, które wprowadzają użytkowników w błąd poprzez podszywanie się pod inne osoby.

Podszywanie się pod inne osoby

Zabraniamy publikowania aplikacji, które wprowadzają użytkowników w błąd, podszywając się pod inną osobę (np. innego dewelopera, firmę, podmiot) lub inną aplikację. Nie sugeruj, że Twoja aplikacja jest z kimś powiązana lub przez kogoś autoryzowana, jeśli tak nie jest.Uważaj, by nie używać ikon, opisów, tytułów ani elementów aplikacji, które mogą wprowadzać użytkowników w błąd co do relacji między Twoją aplikacją a inną osobą lub aplikacją.

Oto kilka często spotykanych przykładów naruszenia zasad:

- deweloperzy fałszywie sugerujący powiązania z inną firmą lub innym deweloperem:



① Wyświetlana nazwa dewelopera tej aplikacji sugeruje, że jest on oficjalnie powiązany z Google, co nie jest prawdą.

- Tytuły i ikony aplikacji bardzo podobne do tych, które są znane z istniejących produktów lub usług, co może wprowadzać użytkowników w błąd:

Zarabianie i reklamy

Google Play umożliwia stosowanie wielu strategii generowania przychodów, w tym dystrybucji płatnej i sprzedaży produktów w aplikacji, a także subskrypcji oraz modeli opartych na reklamach. Strategie te są korzystne zarówno dla deweloperów, jak i użytkowników. Dbając o komfort użytkowników, wymagamy od programistów przestrzegania naszych zasad.

Płatności

Aplikacje, które umożliwiają dokonywanie zakupów w sklepie lub aplikacji, muszą być zgodne z tymi wytycznymi:

Zakupy w sklepie: deweloperzy naliczający opłaty za aplikacje i pliki pobierane z Google Play muszą używać systemu płatności Google Play.

Zakupy w aplikacji:

- Deweloperzy, którzy w grach pobieranych z Google Play oferują możliwość zakupu produktów lub dostęp do treści, muszą jako formy płatności używać Rozliczeń w aplikacji przez Google Play.
- Deweloperzy, którzy w pobieranych z Google Play aplikacjach należących do innych kategorii oferują możliwość zakupu produktów, muszą jako formy płatności używać Rozliczeń w aplikacji przez Google Play. Wyjątkami są te sytuacje:

- Płatność dotyczy tylko produktów fizycznych.
- Płatność dotyczy treści cyfrowych, które można wykorzystać poza samą aplikacją (np. utworów, które można odtwarzać przy użyciu innych odtwarzaczy muzycznych).
- Wirtualnej waluty można używać tylko w aplikacji lub grze, w której została ona pierwotnie kupiona.
- Deweloperom nie wolno wprowadzać użytkowników w błąd w związku ze sprzedawanymi aplikacjami ani oferowanymi odpłatnie usługami, towarami, treściami i funkcjami w aplikacji. Jeśli opis produktu w Google Play dotyczy funkcji w aplikacji podlegających określonym lub dodatkowym opłatom, musi zawierać wyraźną informację, że dostęp do tych funkcji jest płatny.
- Aplikacje z mechanizmem otrzymywania losowych wirtualnych produktów po zakupie (tak zwane „skrzynki z łupami") muszą w wyraźny sposób zawierać informacje o szansie otrzymania takich produktów jeszcze przed dokonaniem zakupu.

Oto kilka przykładów produktów, których sprzedaż jest obsługiwana przez Rozliczenia w aplikacji przez Google Play:

- **Wirtualne produkty w grach** – w tym monety, klejnoty, dodatkowe życia lub ruchy, specjalne przedmioty lub wyposażenie, postacie lub awatary, dodatkowe poziomy czy czas gry.
- **Funkcje lub treści w aplikacji** – np. aplikacja w wersji bez reklam lub nowe funkcje niedostępne w jej bezpłatnej wersji.
- **Usługi subskrypcji** – np. strumieniowy dostęp do muzyki, filmów, książek i innych usług multimedialnych, publikacje cyfrowe (w tym sprzedawane razem z wersją drukowaną) czy usługi sieci społecznościowych.
- **Oprogramowanie działające w chmurze** – w tym usługi przechowywania danych, oprogramowanie biznesowe i programy do zarządzania finansami.

Oto kilka przykładów produktów, których sprzedaż nie jest aktualnie obsługiwana przez Rozliczenia w aplikacji przez Google Play:

- **Handel detaliczny** – np. artykuły spożywcze, ubrania, artykuły gospodarstwa domowego i elektronika.
- **Opłaty za usługi** – w tym usługi transportowe i taksówkowe, usługi porządkowe, dostawę jedzenia, bilety lotnicze i bilety na imprezy.
- **Jednorazowe opłaty za członkostwo lub opłaty cykliczne** – w tym karnety na siłownię, programy lojalnościowe, a także akcesoria, odzież i inne produkty oferowane przez kluby w postaci fizycznej.
- **Płatności jednorazowe** – w tym płatności P2P, aukcje internetowe oraz darowizny.
- **Opłata rachunków drogą elektroniczną** – w tym spłaty zadłużenia na karcie kredytowej, opłaty za usługi komunalne, telekomunikacyjne i telewizję kablową.

Na potrzeby aplikacji, w których jest prowadzona sprzedaż fizycznych produktów i usług, oferujemy interfejs API Google Pay. Więcej informacji znajdziesz na stronie dla deweloperów Google Pay.

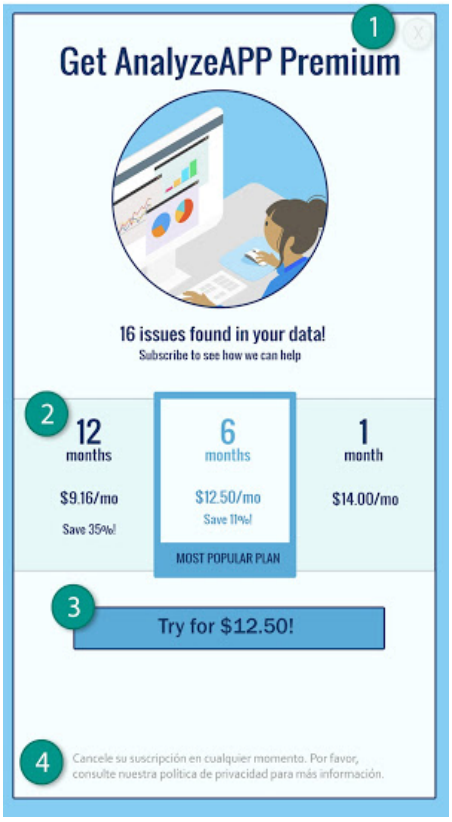
Subskrypcje

Deweloper nie może wprowadzać użytkowników w błąd, jeśli chodzi o usługi subskrypcji lub treści oferowane w aplikacji. Informacje o promocjach w aplikacji i na ekranach powitalnych należy przekazywać w sposób przejrzysty.

W Twojej aplikacji: informacje o ofercie muszą być przejrzyste. Dotyczy to wyraźnego przedstawienia warunków oferty, w tym kosztu subskrypcji, cyklu rozliczeniowego i tego, czy subskrypcja jest wymagana do używania aplikacji. Użytkownicy nie powinni być zmuszeni do wykonania dodatkowych czynności w celu sprawdzenia tych informacji.

Oto kilka często spotykanych przykładów naruszenia zasad:

- Subskrypcje miesięczne, w przypadku których użytkownicy nie są informowani o automatycznym, comiesięcznym obciążeniu płatnością.
- Subskrypcje roczne, w przypadku których najlepiej widoczna jest informacja o ich miesięcznym koszcie.
- Ceny i warunki subskrypcji, które nie są w pełni przetłumaczone.
- Promocje w aplikacji, które nie informują w jasny sposób, że użytkownik może korzystać z treści dostępnych w aplikacji bez kupowania subskrypcji (jeśli jest to możliwe).
- Nazwy SKU nieprawidłowo informujące o rodzaju subskrypcji, np. automatyczna subskrypcja cykliczna o nazwie „Bezpłatna wersja próbna".



① Przycisk zamykania nie jest wyraźnie widoczny, a użytkownicy mogą nie zrozumieć, że dostęp do funkcji nie wymaga akceptacji oferty subskrypcji.

② Oferta zawiera tylko informacje o koszcie miesięcznym, a użytkownicy mogą nie zrozumieć, że w momencie wykupienia subskrypcji zostaną obciążeni opłatą za 6 miesięcy.

③ Oferta zawiera tylko informacje o cenie początkowej, a użytkownicy mogą nie zrozumieć, jakie opłaty będą automatycznie naliczane po okresie początkowym.

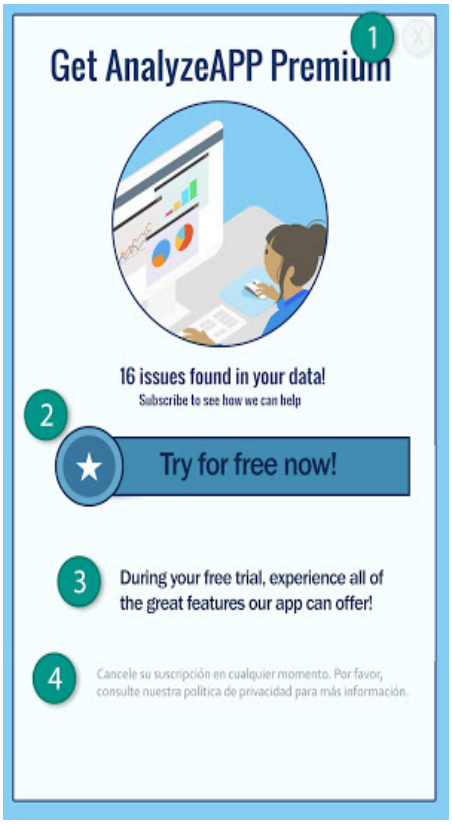
④ Oferta powinna być przetłumaczona na ten sam język co warunki usługi, by użytkownicy mogli wszystko zrozumieć.

Bezpłatne wersje próbne i oferty dla nowych subskrybentów

Zanim użytkownik rozpocznie subskrypcję: musisz w jasny i dokładny sposób przedstawić warunki oferty, w tym czas jej trwania i ceny, a także opisać, jakie treści lub usługi są udostępniane. Pamiętaj, by powiadomić użytkowników o momencie i sposobie przejścia z bezpłatnej wersji próbnej na płatną subskrypcję – dodaj też informacje o koszcie oraz możliwości anulowania subskrypcji (jeśli użytkownik nie chce przejść na jej płatną wersję).

Oto kilka często spotykanych przykładów naruszenia zasad:

- Oferty, które nie informują w jasny sposób o tym, jak długo obowiązuje bezpłatny okres próbny lub cena początkowa.
- Oferty, które nie informują w jasny sposób o tym, że użytkownik zostanie automatycznie przeniesiony na płatną subskrypcję po zakończeniu oferty.
- Oferty, które nie informują w jasny sposób, że użytkownik może korzystać z treści dostępnych w aplikacji bez korzystania z wersji próbnej (jeśli jest to możliwe).
- Ceny i warunki oferty nie są w pełni przetłumaczone.



① Przycisk zamykania nie jest wyraźnie widoczny, a użytkownicy mogą nie zrozumieć, że dostęp do funkcji nie wymaga rejestracji i skorzystania z bezpłatnego okresu próbnego.

② Oferta ma wyróżnioną informację o bezpłatnym okresie próbnym, a użytkownicy mogą nie zrozumieć, że po zakończeniu tego okresu będą automatycznie naliczane opłaty.

③ Oferta nie informuje o okresie próbnym, a użytkownicy mogą nie zrozumieć, jak długo będą mieć bezpłatny dostęp do subskrybowanych treści.

④ Oferta powinna być przetłumaczona na ten sam język co warunki usługi, by użytkownicy mogli wszystko zrozumieć.

Zarządzanie subskrypcjami i ich anulowanie

Deweloper jest zobowiązany do zamieszczenia jasnych informacji o tym, jak można zarządzać subskrypcją lub ją anulować.

Ponosisz odpowiedzialność za powiadomienie użytkowników o wszelkich zmianach dotyczących subskrypcji, anulowania i zasad zwrotów oraz za zgodność zasad z obowiązującym prawem.

Reklamy

Zabronione jest publikowanie aplikacji z reklamami, które są uciążliwe lub wprowadzają w błąd. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera. Reklamy wyświetlane w aplikacji traktujemy jako jej część. Muszą one być zgodne ze wszystkimi naszymi zasadami. Zasady dotyczące reklam związanych z hazardem znajdziesz tutaj.

Używanie danych o lokalizacji do wyświetlania reklam

Aplikacje, w których korzystanie z danych o lokalizacji urządzenia za pozwoleniem użytkownika zostaje poszerzone o wyświetlanie reklam, muszą być zgodne z zasadami opisanymi w sekcji Dane osobowe i poufne oraz dodatkowo z tymi wymaganiami:

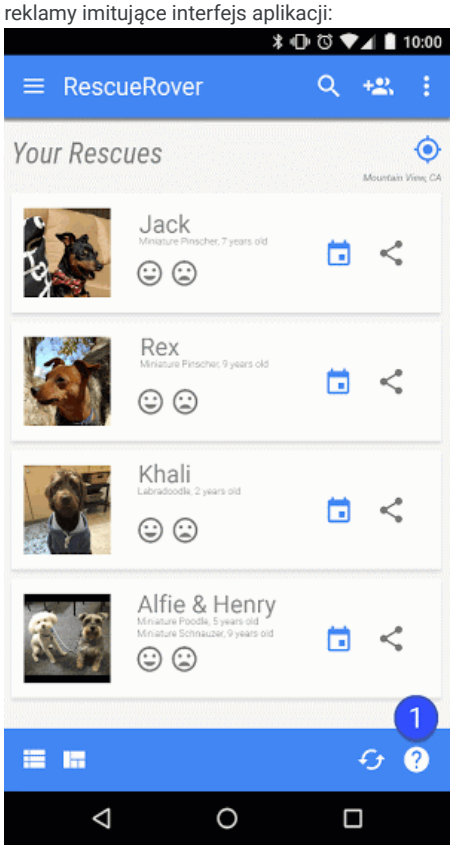
- Używanie lub zbieranie danych o lokalizacji urządzenia za pozwoleniem użytkownika do celów reklamowych musi być jasne dla użytkownika i udokumentowane w obowiązkowej polityce prywatności aplikacji. Obejmuje to podanie linków do polityki prywatności poszczególnych sieci reklamowych, w których są opisane zasady użycia danych o lokalizacji.
- Zgodnie z wymaganiami dotyczącymi dostępu do lokalizacji aplikacja może o niego prosić tylko w celu zastosowania bieżących funkcji lub usług i nie może o niego prosić wyłącznie na potrzeby wyświetlania reklam.

Reklamy wprowadzające w błąd

Reklamy nie mogą symulować ani udawać interfejsu użytkownika żadnej aplikacji ani powiadomień i ostrzeżeń systemowych. W przypadku każdej reklamy użytkownik musi dokładnie wiedzieć, jaka aplikacja ją wyświetla.

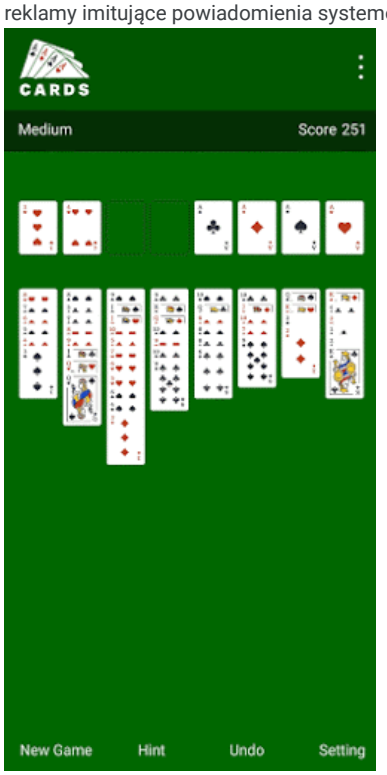
Oto kilka często spotykanych przykładów naruszenia zasad:

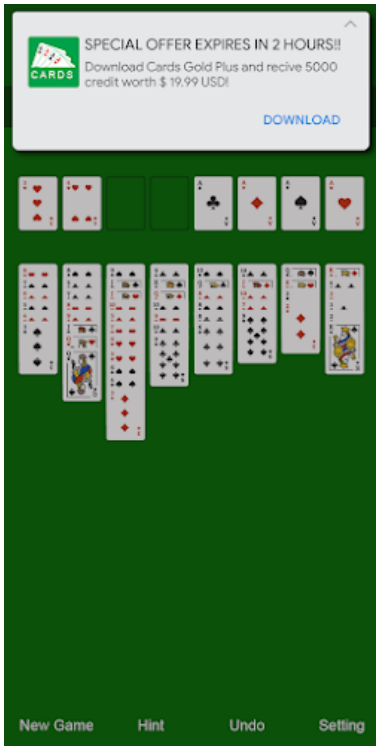
- reklamy imitujące interfejs aplikacji:



① Ikona znaku zapytania w tej aplikacji to reklama, która powoduje otwarcie zewnętrznej strony docelowej.

- reklamy imitujące powiadomienia systemowe:



- 

Te reklamy imitują różne powiadomienia systemowe.

Zarabianie na ekranie blokady

Jeśli jedynym celem aplikacji nie jest blokowanie ekranu, nie może ona wprowadzać na zablokowanym ekranie urządzenia reklam ani funkcji umożliwiających deweloperowi zarabianie.

Uciążliwe reklamy

Uciążliwe reklamy to reklamy wyświetlane użytkownikom w nieoczekiwany sposób, co może skutkować niezamierzonymi kliknięciami lub zakłócać działanie funkcji urządzenia.

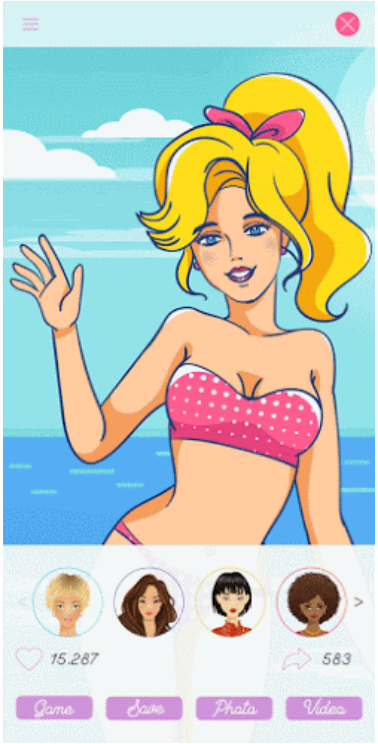
Zmuszanie użytkownika do kliknięcia reklamy lub przesłania danych osobowych w celach marketingowych, zanim może on w pełni korzystać z aplikacji, jest zabronione. Reklamy pełnoekranowe mogą wyświetlać się wyłącznie w aplikacji, która je zawiera. Jeśli aplikacja wyświetla reklamy pełnoekranowe lub inne reklamy, które zakłócają jej normalne działanie, użytkownik musi mieć możliwość ich łatwego zamknięcia bez żadnych negatywnych konsekwencji.

Oto kilka często spotykanych przykładów naruszenia zasad:

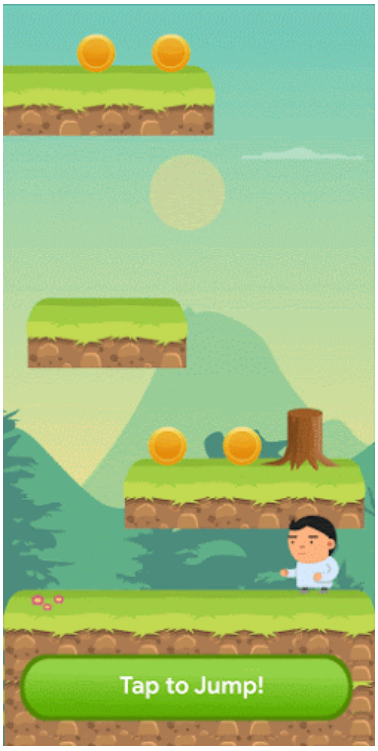
- reklamy zajmujące cały ekran lub zakłócające normalne działanie, które nie informują w jasny sposób, jak je zamknąć:

① Ta reklama nie zawiera przycisku zamykania.

- reklamy, które wymuszają na użytkowniku kliknięcie, wyświetlając fałszywy przycisk zamykania lub pojawiając się nagle w obszarach aplikacji, które użytkownik zwykle klika, by użyć innej funkcji;



reklama korzystająca z fałszywego przycisku zamknięcia;



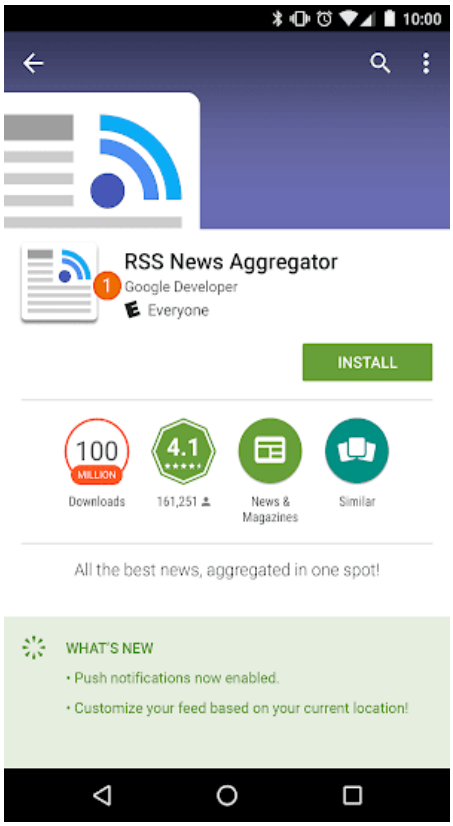
reklama, która nagle pojawia się w miejscu, które użytkownik z przyzwyczajenia klika, by skorzystać z funkcji aplikacji.

Zakłócanie działania aplikacji, reklam innych firm lub funkcji urządzenia

Reklamy powiązane z Twoją aplikacją nie mogą zakłócać działania innych aplikacji, reklam ani pracy urządzenia, w tym jego systemu, przycisków i portów. Dotyczy to też nakładek, funkcji towarzyszących i reklam w formie widżetów. Reklamy mogą wyświetlać się tylko w aplikacji, która je zawiera.

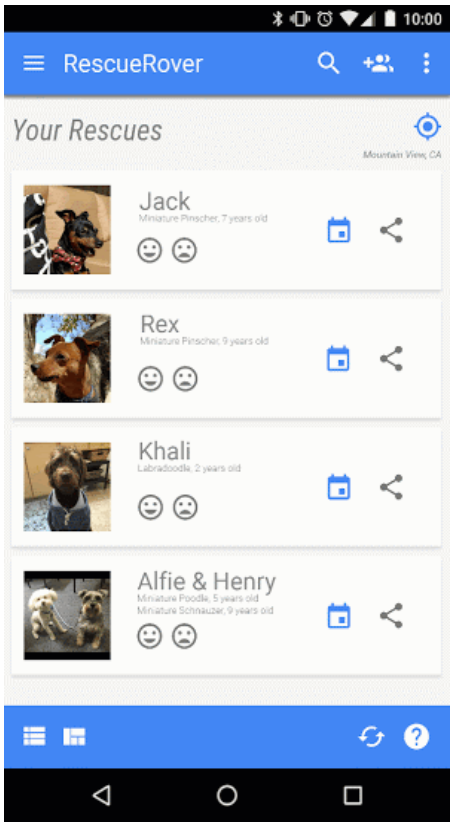
Oto kilka często spotykanych przykładów naruszenia zasad:

- Reklamy wyświetlane poza aplikacją, która je zawiera.



Opis: gdy przechodzi się z aplikacji do ekranu głównego, nagle pojawia się na nim reklama.

- Reklamy wyświetlane po naciśnięciu przycisku ekranu głównego lub użyciu innych funkcji wyraźnie zaprojektowanych do zamykania aplikacji.

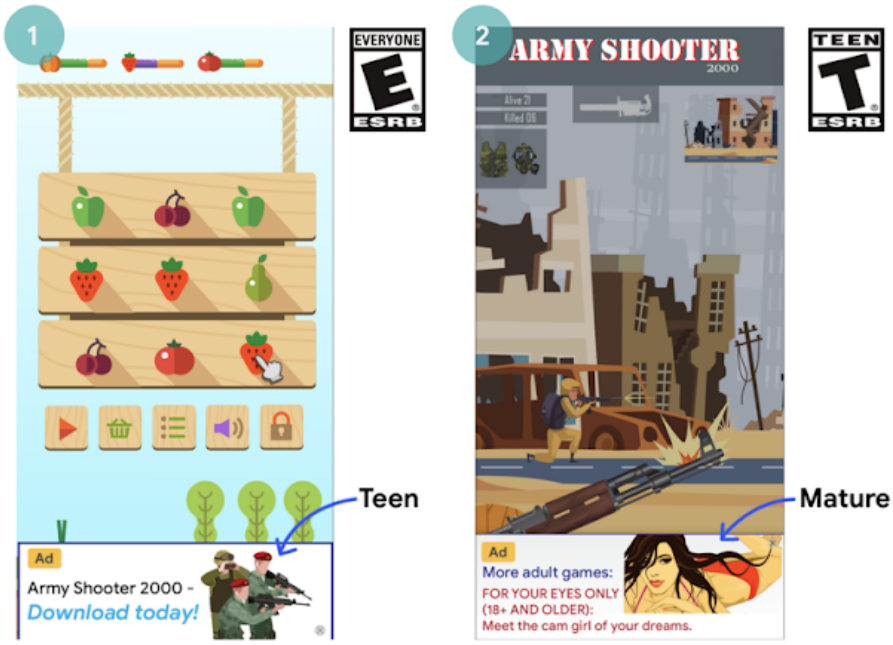


Opis: użytkownik chce wyjść z aplikacji i przejść do ekranu głównego, ale czynność ta jest niespodziewanie przerwana przez wyświetlenie się reklamy.

Nieodpowiednie reklamy

Oprócz tego, że treść reklam wyświetlanych w aplikacji musi być zgodna z naszymi zasadami, reklamy muszą też być odpowiednie dla docelowej grupy odbiorców aplikacji.

Oto najczęstsze przykłady naruszenia zasad:



① Ta reklama (zawierająca treści dla nastolatków) jest nieodpowiednia dla docelowej grupy odbiorców aplikacji (7+).
② Ta reklama (zawierająca treści dla dorosłych) jest nieodpowiednia dla docelowej grupy odbiorców aplikacji (12+).

Używanie identyfikatora wyświetlania reklam na urządzeniach z Androidem

W Usługach Google Play w wersji 4.0 wprowadziliśmy nowe interfejsy API i identyfikator na użytek dostawców usług reklamowych i analitycznych. Warunki korzystania z tego identyfikatora znajdziesz poniżej.

- **Wykorzystanie.** Identyfikatora wyświetlania reklam na urządzeniach z Androidem można używać wyłącznie do celów reklamowych i do analizowania informacji o użytkownikach. Stan ustawienia rezygnacji z reklam opartych na zainteresowaniach lub reklam spersonalizowanych musi być weryfikowany przy każdym dostępie do identyfikatora.
- **Powiązanie z informacjami umożliwiającymi identyfikację osoby lub z innymi identyfikatorami**
  - Wykorzystanie na potrzeby reklam: identyfikatora wyświetlania reklam nie wolno łączyć z trwałymi identyfikatorami urządzeń (takimi jak SSAID, adres MAC, IMEI itp.) na potrzeby jakiejkolwiek formy reklamy. Identyfikator wyświetlania reklam może być połączony z informacjami umożliwiającymi identyfikację tylko za wyraźną zgodą użytkownika.
  - Wykorzystanie na potrzeby analiz: identyfikatora wyświetlania reklam nie wolno łączyć z informacjami umożliwiającymi identyfikację ani wiązać z żadnym stałym identyfikatorem urządzenia (np. identyfikatorem SSAID, adresem MAC, numerem IMEI itp.) bez wyraźnej zgody użytkownika.
- **Szanowanie decyzji użytkownika.** Po zresetowaniu nowego identyfikatora wyświetlania reklam nie można połączyć z poprzednim ani z danymi uzyskanymi na podstawie poprzedniego identyfikatora bez wyraźnej zgody użytkownika. Poza tym należy się stosować do wybranego przez użytkowników ustawienia rezygnacji z reklam opartych na zainteresowaniach lub reklam spersonalizowanych. Jeśli użytkownik włączył to ustawienie, nie wolno używać identyfikatora wyświetlania reklam do tworzenia profili użytkowników do celów reklamowych ani do kierowania na użytkowników reklam spersonalizowanych. Dozwolone zastosowania obejmują reklamę kontekstową, ograniczanie liczby wyświetleń, śledzenie konwersji, raportowanie, wykrywanie oszustw oraz bezpieczeństwo.
- **Przejrzystość dla użytkowników.** Informacje o zbieraniu danych i wykorzystaniu identyfikatora wyświetlania reklam oraz zobowiązanie do przestrzegania tych warunków należy przedstawić użytkownikom w informacjach na temat ochrony prywatności w formie dokumentu prawnego. Więcej informacji o naszych standardach w zakresie prywatności znajdziesz w zasadach dotyczących danych użytkownika.
- **Przestrzeganie warunków korzystania z identyfikatora.** Identyfikatora wyświetlania reklam można używać tylko zgodnie z tymi warunkami. Obowiązują one też wszystkie firmy, którym udostępniasz identyfikator w ramach prowadzenia działalności. Wszystkie aplikacje przesłane w Google Play lub opublikowane w tej usłudze muszą do celów reklamowych używać identyfikatora wyświetlania reklam (jeśli jest dostępny na urządzeniu) zamiast jakichkolwiek innych identyfikatorów urządzenia.

Program reklam odpowiednich dla rodzin

Jeśli Twoja aplikacja jest przeznaczona tylko dla dzieci (zgodnie z definicją zawartą w Zasadach dotyczących aplikacji dla rodzin) i wyświetla reklamy, musisz korzystać z pakietów SDK reklam, które samodzielnie uzyskały certyfikat zgodności z zasadami Google Play, w tym również z poniższymi wymaganiami certyfikacji pakietów SDK reklam. Jeśli

aplikacja jest skierowana do dzieci, ale też starszych użytkowników, zaimplementuj mechanizm sprawdzania wieku. Dodatkowo dopilnuj, by reklamy wyświetlane dzieciom pochodziły wyłącznie z jednego z tych samodzielnie certyfikowanych pakietów SDK reklam. Aplikacje uczestniczące w programie Dla całej rodziny mogą korzystać wyłącznie z samodzielnie certyfikowanych pakietów SDK reklam.

Korzystanie z pakietów SDK reklam z certyfikatem Google Play jest wymagane tylko wtedy, gdy używasz w swojej aplikacji pakietów SDK, by wyświetlać reklamy dzieciom. Wymienione poniżej sposoby promocji są dozwolone bez samodzielnej certyfikacji pakietu SDK reklam w Google Play. Nadal jednak odpowiadasz za to, by treści Twoich reklam i metody gromadzenia danych były zgodne z zasadami zbierania danych użytkowników i Zasadami dotyczącymi aplikacji dla rodzin w Google Play:

- reklamy wewnętrzne, w przypadku których używasz pakietów SDK do zarządzania wzajemną promocją swoich aplikacji lub innych należących do Ciebie mediów i towarów;
- zawieranie umów bezpośrednich z reklamodawcami, gdy korzystasz z pakietów SDK do zarządzania zasobami reklamowymi.

Wymagania dotyczące certyfikacji pakietów SDK reklam

- Określ nieodpowiednie treści i zachowania reklam i zakaż ich wyświetlania w warunkach lub zasadach pakietu SDK reklam. Definicje powinny być zgodne z Zasadami programu dla deweloperów w Google Play.
- Utwórz metodę oceny reklam w zależności od tego, do jakich grup wiekowych są kierowane. Musisz uwzględnić co najmniej grupy Dla wszystkich i Dla dorosłych. Metoda oceniania musi odpowiadać tej, którą Google przekazuje dostawcom pakietów SDK po wypełnieniu przez nich formularza zainteresowania (poniżej).
- Zezwól wydawcom, by mogli prosić o traktowanie reklam jako skierowanych do dzieci (jednorazowo lub w całej aplikacji). Takie traktowanie musi być zgodne z obowiązującymi przepisami i regulacjami, takimi jak amerykańska ustawa o ochronie prywatności dzieci w internecie (Children's Online Privacy and Protection Act, COPPA) i unijne Ogólne rozporządzenie o ochronie danych (RODO). Google Play wymaga również w takim przypadku wyłączenia reklam spersonalizowanych, reklam opartych na zainteresowaniach i remarketingu.
- Pozwól wydawcom wybrać formaty reklam zgodne z zasadami Google Play dotyczącymi reklam i zarabiania oraz Programu aplikacji zatwierdzonych przez nauczycieli.
- Jeśli przy wyświetlaniu reklam dzieciom używane jest określanie stawek w czasie rzeczywistym, upewnij się, że kreacje zostały zatwierdzone, a wskaźniki prywatności zostały przekazane do systemów licytujących.
- Przekaż Google informacje wystarczające do sprawdzenia zgodności pakietu SDK reklam ze wszystkimi wymogami certyfikacji, np. informacje wskazane w poniższym formularzu zainteresowania, oraz w wyznaczonym czasie odpowiadaj na wszelkie prośby o dodatkowe informacje.

Uwaga: pakiety SDK reklam muszą wyświetlać reklamy zgodnie ze wszystkimi odpowiednimi przepisami i regulacjami dotyczącymi dzieci (które mogą obowiązywać wydawców reklam).

Wymagania dotyczące zapośredniczenia w przypadku platform wyświetlających reklamy dzieciom:

- Używaj wyłącznie pakietów SDK reklam certyfikowanych przez Google Play lub zaimplementuj środki ochrony, które zagwarantują spełnianie wszystkich tych wymagań przez reklamy pochodzące z zapośredniczenia.
- Przekaż informacje potrzebne platformom zapośredniczania do wskazania oceny treści reklam i (jeśli ma to zastosowanie) oznaczenia reklamy jako skierowanej do dzieci.

Lista samodzielnie certyfikowanych pakietów SDK reklam znajduje się tutaj.

Możesz też udostępnić ten formularz zainteresowania dostawcom pakietów SDK reklam, którzy chcą przejść samodzielną certyfikację.

Informacje o aplikacji i promocja

Promocja i widoczność aplikacji w znacznym stopniu wpływają na jakość sklepu. Nie publikuj spamu w informacjach o aplikacji, nie wyświetlaj reklam niskiej jakości i nie próbuj sztucznie zwiększać widoczności aplikacji w Google Play.

Promowanie aplikacji

Zabronione jest publikowanie aplikacji biorących w sposób bezpośredni lub pośredni udział w praktykach promocyjnych (lub czerpiących z nich korzyści), które wprowadzają w błąd użytkownika albo programistę bądź są dla nich szkodliwe. Dotyczy to między innymi aplikacji, które:

- wyświetlają w witrynach, aplikacjach i usługach reklamy wprowadzające w błąd, w tym takie, które symulują powiadomienia lub alerty systemu;
- stosują metody promocji lub instalacji przekierowujące użytkowników do Google Play lub powodujące pobieranie aplikacji bez świadomego udziału użytkownika;
- rozsyłają niechciane SMS-y promocyjne.

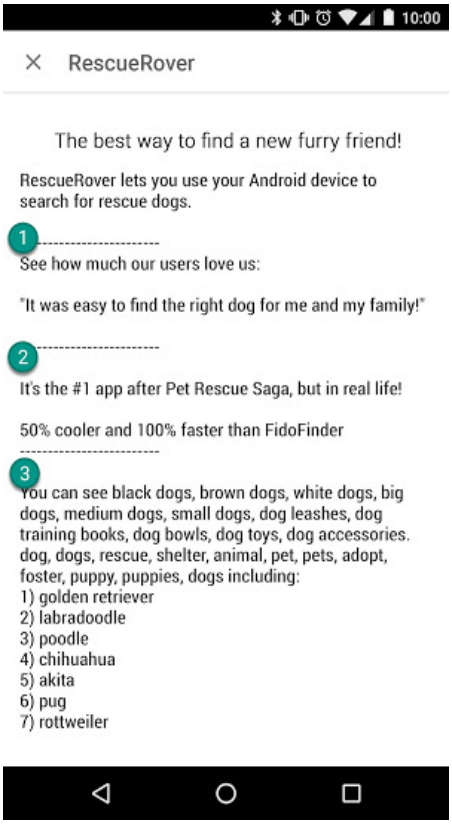
Obowiązkiem dewelopera jest dopilnowanie, by wszelkie sieci reklamowe oraz podmioty stowarzyszone z aplikacją przestrzegały naszych zasad i nie stosowały żadnych niedozwolonych metod promocji.

Metadane

Zabraniamy publikowania aplikacji z wprowadzającymi w błąd, nieprawidłowo sformatowanymi, nieopisowymi, nieistotnymi, nadmiernymi lub nieodpowiednimi metadanymi. Dotyczy to m.in. opisu aplikacji, nazwy dewelopera, tytułu, ikony, zrzutów ekranu i grafiki promocyjnej. Deweloperzy muszą przekazać zrozumiały i poprawnie sformułowany opis. Niedozwolone są również niepodpisane lub anonimowe opinie użytkowników w opisie aplikacji.

Oprócz wymienionych tutaj wymagań określone zasady dla deweloperów Google Play mogą wymagać podania dodatkowych informacji o metadanych.

Oto kilka często spotykanych przykładów naruszenia zasad:



① Niepodpisane lub anonimowe opinie użytkowników.
② Porównanie danych o aplikacjach lub markach.
③ Bloki słów i pionowe/poziome listy słów.

Oto kilka przykładów nieodpowiednich tekstów, obrazów lub filmów w informacjach o aplikacji:

- obrazy lub filmy z podtekstem seksualnym (unikaj materiałów graficznych – zarówno ilustracji, jak i zdjęć czy filmów – oraz innych treści przedstawiających w dwuznaczny sposób piersi, pośladki, genitalia lub inne części ciała występujące w roli fetysza);
- używanie w informacjach o aplikacji wulgaryzmów, przekleństw lub innych określeń nieodpowiednich dla wszystkich odbiorców;
- drastyczna przemoc wyeksponowana w ikonach aplikacji lub promocyjnych obrazach czy filmach;
- przedstawianie zażywania narkotyków i innych nielegalnych substancji (nawet treści popularnonaukowe, dokumentalne, naukowe i artystyczne zawarte w informacjach o aplikacji muszą być odpowiednie dla wszystkich odbiorców).

Oto kilka sprawdzonych metod:

- Podkreśl zalety aplikacji. Podziel się z użytkownikami ciekawymi, zachęcającymi uwagami o niej, by pokazać im, co ją wyróżnia.
- Dopilnuj, by tytuł i opis aplikacji dokładnie informowały o jej funkcjach.
- Unikaj powtarzających się lub niepowiązanych z aplikacją słów kluczowych i odwołań.

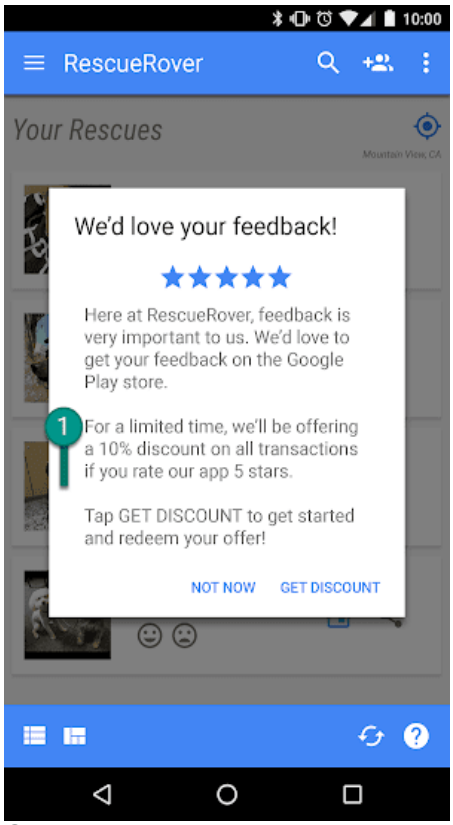
- Opis aplikacji powinien być jasny i zwięzły. Na urządzeniach z mniejszymi ekranami z reguły lepiej sprawdzają się krótsze opisy. Zbyt długi, szczegółowy, nieprawidłowo sformatowany lub pełen powtórzeń opis może naruszać nasze zasady.
- Pamiętaj, że informacje o aplikacji muszą być odpowiednie dla ogółu odbiorców. Nie zamieszczaj w nich nieodpowiednich tekstów, obrazów ani filmów. Pamiętaj też o konieczności przestrzegania wymienionych wyżej wytycznych.

Instalacje, opinie i oceny użytkowników

Deweloperom nie wolno próbować zmienić pozycji żadnej aplikacji w Google Play. Obejmuje to między innymi podwyższanie ocen produktów i liczby instalacji oraz zamieszczanie opinii przy użyciu nielegalnych praktyk, takich jak fałszywe lub generowane przez zachęty instalacje, opinie czy oceny.

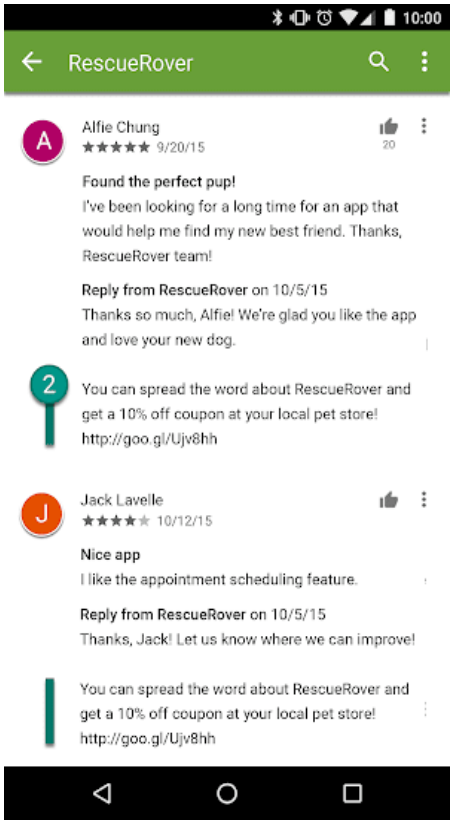
Oto kilka często spotykanych przykładów naruszenia zasad:

- Oferowanie użytkownikom korzyści w zamian za wystawienie oceny:



① To powiadomienie proponuje użytkownikom zniżkę w zamian za wysoką ocenę.

- Wielokrotne przesyłanie ocen, by wpłynąć na pozycję aplikacji w Google Play.
- Zgłaszanie lub zachęcanie użytkowników do zamieszczania opinii z nieodpowiednimi treściami, w tym poprzez informacje o podmiotach stowarzyszonych, kupony, kody do gier, adresy e-mail czy linki do witryn lub innych aplikacji:



② Ta opinia zachęca użytkowników do promowania aplikacji RescueRover przez oferowanie kuponów.

Oceny i opinie są wskaźnikami jakości aplikacji. Użytkownicy oczekują, że będą one autentyczne i wiarygodne. Oto niektóre ze sprawdzonych metod odpowiadania na opinie użytkowników:

- Skup się na problemach wskazanych w komentarzu użytkownika i nie proś o wyższą ocenę.
- Wskaż materiały, które mogą się przydać – np. e-mail do pomocy technicznej czy adres strony z najczęstszymi pytaniami.

Oceny treści

System oceny treści w Google Play powstał, by deweloperzy mogli udostępniać użytkownikom na całym świecie wiarygodne oceny uwzględniające uwarunkowania lokalne. Systemem ocen zarządza organizacja International Age Rating Coalition (IARC). Regionalne oddziały IARC publikują wytyczne, które służą do określania poziomu dojrzałości użytkowników aplikacji. W Google Play nie wolno publikować aplikacji bez oceny treści.

Do czego używane są oceny treści

Oceny treści mają za zadanie informować klientów (zwłaszcza rodziców) o potencjalnie nieodpowiednich treściach w aplikacjach. Pomagają też blokować i odfiltrowywać treści w niektórych krajach/regionach lub dla określonych użytkowników, gdy wymaga tego prawo, oraz ocenić możliwość włączenia aplikacji do specjalnych programów dla deweloperów.

W jaki sposób nadawane są oceny

Aby otrzymać ocenę treści, musisz wypełnić ten kwestionariusz w Konsoli Play na temat rodzaju treści dostępnych w aplikacji. Na podstawie odpowiedzi udzielonych w kwestionariuszu różne organizacje oceniające nadają Twojej aplikacji ocenę treści. Fałszywe przedstawienie zawartości aplikacji może spowodować jej usunięcie lub zawieszenie – odpowiedz jak najdokładniej na pytania w kwestionariuszu oceny treści.

Aby uniknąć wyświetlania aplikacji „Bez oceny”, wypełnij kwestionariusz oceny treści w przypadku każdej nowej aplikacji przesłanej do Konsoli Play, a także wszystkich dotychczas opublikowanych aplikacji, które są aktywne w Google Play.

Jeśli wprowadzisz w aplikacji aktualizacje, które zmienią jej zawartość lub funkcje i mogą wpłynąć na odpowiedzi udzielone w kwestionariuszu oceny treści w Konsoli Play, musisz przesłać nowy kwestionariusz.

Więcej informacji o różnych organizacjach oceniających oraz instrukcje wypełniania kwestionariusza oceny treści znajdziesz w Centrum pomocy.

Zgłaszanie odwołań od ocen

Jeśli nie zgadzasz się z oceną nadaną Twojej aplikacji, możesz odwołać się bezpośrednio do organizacji oceniającej IARC, korzystając z linku podanego w e-mailu z certyfikatem.

Wiadomości

W kategorii Wiadomości w Sklepie Play nie wolno umieszczać aplikacji oznaczonych jako Wiadomości, które wyświetlają treści niespełniające wymagań tej kategorii. Aplikacje prezentujące wiadomości, które wymagają od użytkownika wykupienia subskrypcji, muszą przed zakupem umożliwiać użytkownikom wyświetlenie podglądu treści.

Aplikacje prezentujące wiadomości MUSZĄ:

- zawierać odpowiednie informacje na temat wydawcy wiadomości i ich współtwórców, w tym jednoznaczne informacje o własności;
- mieć witrynę lub stronę w aplikacji zawierającą prawidłowe informacje kontaktowe wydawcy wiadomości.

Aplikacje prezentujące wiadomości NIE MOGĄ:

- zawierać poważnych błędów ortograficznych i gramatycznych;
- zawierać tylko treści statycznych;
- mieć za główny cel marketingu afiliacyjnego ani generowania przychodów z reklam.

Aplikacje gromadzące wiadomości muszą jasno informować o źródle publikującym treści przedstawiane w aplikacji, a każde ze źródeł musi spełniać wymagania określone w zasadach kategorii Wiadomości.

Spam i minimalna funkcjonalność

Aplikacje powinny zapewniać użytkownikom przynajmniej minimalny poziom funkcjonalności i wygody użytkowania. Aplikacje zawierające błędy, odznaczające się niską wygodą obsługi albo służące tylko do rozpowszechniania spamu wśród użytkowników lub w Google Play nie przyczyniają się do znaczącego wzbogacenia katalogu.

Spam

Zabraniamy publikowania aplikacji rozpowszechniających spam wśród użytkowników lub w Google Play, w tym aplikacji, które wysyłają niechciane wiadomości oraz takich, które są powieleniem innych i charakteryzują się niską jakością.

Spam w wiadomościach

Zabronione jest publikowanie aplikacji wysyłających SMS-y, e-maile lub inne wiadomości w imieniu użytkownika bez możliwości potwierdzenia przez niego ich treści i adresatów.

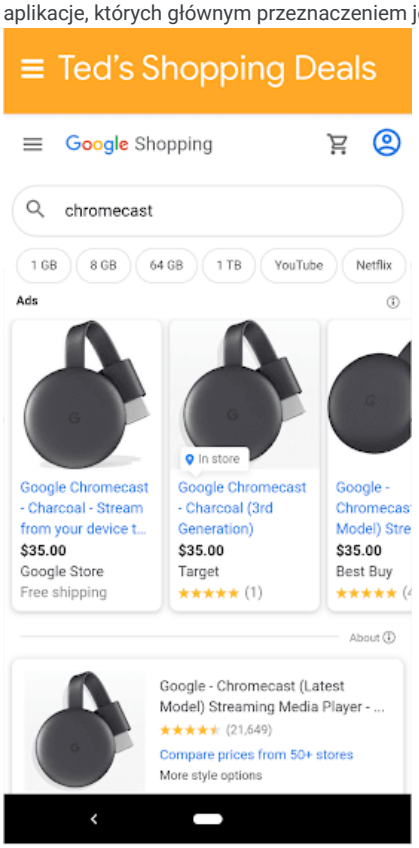
Spam związany z wyświetleniami witryn i podmiotami stowarzyszonymi

Zabraniamy publikowania aplikacji, których głównym przeznaczeniem jest zwiększanie ruchu w powiązanej z nią witrynie lub generowanie widoku witryny bez pozwolenia jej właściciela lub administratora.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacja, której głównym celem jest zwiększenie ruchu z witryn odsyłających w celu otrzymywania środków za rejestracje użytkowników lub zakupy w tej witrynie;

- aplikacje, których głównym przeznaczeniem jest generowanie widoku witryny bez pozwolenia:



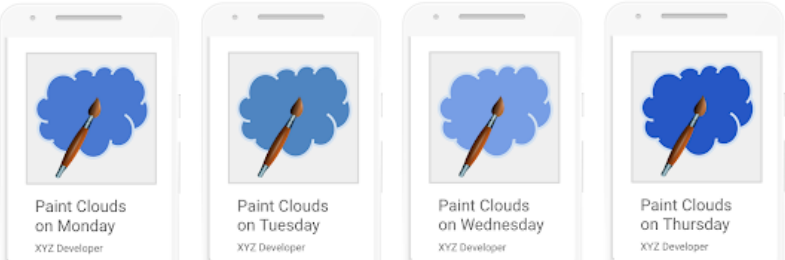
Aplikacja o nazwie „Ted's Shopping Deals" generuje jedynie widok strony z Zakupów Google.

Powielanie treści

Zabraniamy publikowania aplikacji, które jedynie powielają treści i funkcje innych aplikacji dostępnych już w Google Play. Aplikacje muszą oferować użytkownikom unikalne treści, funkcje lub usługi.

Oto kilka często spotykanych przykładów naruszenia zasad:

- kopiowanie treści z innych aplikacji bez dodania czegoś oryginalnego;
- tworzenie wielu aplikacji o bardzo podobnej zawartości i sposobie działania czy funkcjach (jeśli każda z aplikacji zawiera niewiele treści, deweloperzy powinni raczej udostępnić wszystkie treści w jednej aplikacji).



Aplikacje, które mają przede wszystkim wyświetlać reklamy

Zabraniamy publikowania aplikacji, których głównym celem jest wyświetlanie reklam.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje, w których po każdym działaniu użytkownika (kliknięciu, przesunięciu itd.) wyświetlana jest reklama pełnoekranowa.

Minimalna funkcjonalność

Zadbaj o to, by aplikacja działała stabilnie i dostatecznie szybko, a sposób prezentowania treści był atrakcyjny i angażujący.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje, które zostały opracowane tak, by nie wykonywać żadnych działań, lub które nie oferują żadnych funkcji.

Nieprawidłowe działanie

Zabraniamy publikowania aplikacji z błędami, wymuszających zamknięcia, blokujących się lub działających nieprawidłowo.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje, których **nie można zainstalować**;
- aplikacje, które się instalują, ale **się nie ładują**;
- aplikacje, które się ładują, ale **nie reagują**.

Inne programy

Poza zgodnością z zasadami dotyczącymi treści określonymi w innych miejscach w tym Centrum zasad aplikacje stworzone z myślą o innych sposobach korzystania z Androida i udostępniane w Google Play mogą również podlegać wymogom dotyczącym konkretnego programu. Zapoznaj się z poniższą listą, by sprawdzić, czy któreś z tych zasad dotyczą Twojej aplikacji.

Aplikacje błyskawiczne na Androida

Chcemy, by aplikacje błyskawiczne na Androida były wygodne i bezproblemowe w obsłudze, a jednocześnie zgodne z najwyższymi standardami prywatności i bezpieczeństwa. Właśnie w tym celu opracowaliśmy nasze zasady.

Deweloperzy, którzy decydują się udostępniać aplikacje błyskawiczne na Androida w Google Play, oprócz pozostałych Zasad programu dla deweloperów w Google Play muszą przestrzegać tych zasad.

Tożsamość

W aplikacjach, które zawierają funkcję logowania, deweloperzy muszą zastosować Smart Lock na hasła.

Obsługa linków

Deweloperzy aplikacji błyskawicznych na Androida muszą zapewnić prawidłową obsługę linków do innych aplikacji. Jeśli aplikacje błyskawiczne lub instalowane zawierają linki, które mogą prowadzić do aplikacji błyskawicznej, deweloper musi kierować użytkowników do tej aplikacji błyskawicznej, a nie np. rejestrować linki w WebView.

Specyfikacje techniczne

Deweloperzy muszą przestrzegać specyfikacji technicznych aplikacji błyskawicznych na Androida i określonych przez Google wymagań (również tych wymienionych w naszej dokumentacji publicznej), które co jakiś czas mogą się zmieniać.

Opcja zainstalowania aplikacji

Aplikacja błyskawiczna może oferować użytkownikowi wersję do zainstalowania, ale nie może to być jej głównym przeznaczeniem. Oferując wersję instalowaną, deweloperzy:

- muszą użyć ikony „Pobierz aplikację” w stylu Material Design i etykiety „Zainstaluj” na przycisku instalacji;
- nie mogą zamieszczać w aplikacji błyskawicznej więcej niż 2–3 wiadomości nakłaniających do instalacji;
- nie mogą używać banerów ani innych technik reklamowych do przedstawiania użytkownikom wiadomości zachęcających do instalacji.

Dodatkowe informacje o aplikacjach błyskawicznych i wskazówki dotyczące UX znajdziesz w artykule o sprawdzonych metodach zwiększania wygody użytkowników.

Zmiana stanu urządzenia

Aplikacje błyskawiczne nie mogą wprowadzać na urządzeniu zmian, które utrzymują się dłużej niż sesja aplikacji błyskawicznej. Przykładowo aplikacje nie mogą zmieniać tapety użytkownika ani tworzyć widżetów na ekranie głównym.

Widoczność aplikacji

Programiści muszą zapewnić użytkownikom widoczność aplikacji błyskawicznych, tak aby użytkownik przez cały czas wiedział, że na urządzeniu działa taka aplikacja.

Identyfikatory urządzeń

Aplikacje błyskawiczne nie mogą uzyskiwać dostępu do identyfikatorów urządzeń, które: (1) utrzymują się po zakończeniu działania aplikacji błyskawicznej; (2) nie mogą być resetowane przez użytkownika. Wybrane przykłady:

- numery seryjne kompilacji,
- adresy MAC jakichkolwiek układów sieciowych,
- numery IMEI lub IMSI.

Aplikacje błyskawiczne mogą uzyskiwać dostęp do numeru telefonu, który został uzyskany na podstawie uprawnień podczas działania. Programista nie może próbować identyfikować użytkownika za pomocą takich identyfikatorów lub innych metod.

Ruch w sieci

Ruch sieciowy wychodzący z aplikacji błyskawicznej musi być szyfrowany przy użyciu protokołu TLS, takiego jak HTTPS.

Dla rodzin

Google Play to miejsce, w którym deweloperzy mogą publikować różnego rodzaju wartościowe treści przeznaczone dla całej rodziny. Przed zgłoszeniem aplikacji do programu Dla całej rodziny lub przesłaniem aplikacji skierowanej do dzieci do Sklepu Google Play, musisz się upewnić, że jest ona odpowiednia dla dzieci i zgodna ze stosownymi przepisami.

Dowiedz się więcej o procesie publikowania aplikacji dla rodzin i przejrzyj interaktywną listę kontrolną w Akademii dla deweloperów aplikacji.

Tworzenie aplikacji dla dzieci i rodzin

Technologia stała się narzędziem, które zapewnia rodzinie coraz więcej możliwości i rozrywki, dlatego rodzice szukają bezpiecznych treści o wysokiej jakości, które byłyby odpowiednie dla ich dzieci. Aplikacje mogą być opracowane specjalnie dla dzieci albo po prostu atrakcyjne dla młodszego odbiorcy. W obydwu przypadkach zespół Google Play pomaga deweloperom zapewnić, że aplikacje są bezpieczne dla wszystkich użytkowników, w tym całych rodzin.

Słowo „dziecko” może mieć wiele znaczeń w zależności od regionu i kontekstu. Dlatego ważne jest, by skonsultować się z radcą prawnym i określić zobowiązania oraz ograniczenia wynikające z kierowania treści do użytkowników z określonych kategorii wiekowych. To Ty najlepiej znasz swoje aplikacje, dlatego przy określaniu, czy mogą pojawić się w Sklepie Google i są odpowiednie dla rodzin, polegamy na Twoim osądzie.

Aplikacje przeznaczone dla dzieci muszą uczestniczyć w programie Dla całej rodziny. Jeśli Twoja aplikacja jest skierowana zarówno do dzieci, jak i do starszych odbiorców, nadal możesz uczestniczyć w programie Dla całej rodziny. Wszystkie aplikacje zarejestrowane w tym programie mogą zostać zgłoszone do Programu aplikacji zatwierdzonych przez nauczycieli, jednak nie możemy zagwarantować, że Twoja aplikacja zostanie do niego zakwalifikowana. Jeśli nie chcesz uczestniczyć w programie Dla całej rodziny, nadal obowiązują Cię Zasady dotyczące aplikacji dla rodzin w Google Play (znajdziesz je poniżej), a także pozostałe Zasady programu dla deweloperów w Google Play oraz Umowa dystrybucyjna dla deweloperów.

Wymagania dotyczące Konsoli Play

Docelowi odbiorcy i treści

Przed opublikowaniem aplikacji musisz wskazać jej docelowych odbiorców w sekcji Docelowi odbiorcy i treści w Konsoli Google Play. Aby to zrobić, wybierz z listy odpowiednie grupy wiekowe. Jeśli w aplikacji zamieszczane są obrazy i sformułowania, które mogą zostać uznane za skierowane do dzieci, może to wpłynąć na ocenę deklarowanych docelowych odbiorców przez Google Play – niezależnie od tych określonych przez Ciebie w Konsoli Google Play. Google Play zastrzega sobie prawo do sprawdzenia podanych informacji o aplikacji, by określić, czy docelowi odbiorcy zostali właściwie wskazani.

Jeśli wskazanymi odbiorcami docelowymi są tylko osoby dorosłe, ale Google ustali, że ta informacja jest niedokładna, ponieważ aplikacja jest skierowana zarówno do dzieci, jak i do dorosłych, dostępna będzie możliwość jasnego poinformowania użytkowników, że aplikacja nie jest przeznaczona dla dzieci. W tym celu musisz wyrazić zgodę na przypisanie jej etykiety ostrzegawczej.

Więcej niż 1 grupę wiekową docelowych odbiorców aplikacji możesz wybrać tylko wtedy, gdy aplikacja została opracowana z myślą o użytkownikach w różnym wieku. Na przykład aplikacje przeznaczone dla małych dzieci i przedszkolaków powinny mieć tylko grupę wiekową „Do 5 lat”. Jeśli aplikacja jest przeznaczona dla uczniów

z określonych klas, musisz wybrać grupę wiekową, która najlepiej do nich pasuje. Przedziały wiekowe, które uwzględniają dorosłych i dzieci, należy uwzględniać tylko wtedy, jeśli aplikacja rzeczywiście została opracowana dla wszystkich grup wiekowych.

Aktualizacje w sekcji Docelowi odbiorcy i treści

Informacje w sekcji Docelowi odbiorcy i treści w Konsoli Google Play możesz aktualizować w dowolnym momencie. Przed opublikowaniem tych informacji w Sklepie Google Play wymagana jest aktualizacja aplikacji. Pamiętaj, że wszelkie zmiany w tej sekcji Konsoli Google Play mogą zostać sprawdzone pod kątem zgodności z zasadami jeszcze przed przesłaniem aktualizacji aplikacji.

Zdecydowanie zalecamy poinformowanie dotychczasowych użytkowników o zmianie grupy wiekowej odbiorców aplikacji lub rozpoczęciu korzystania z reklam albo zakupów w aplikacji. Aby to zrobić, skorzystaj z powiadomień w aplikacji lub sekcji „Nowości" na stronie z informacjami o aplikacji.

Wprowadzanie w błąd przy użyciu Konsoli Play

Fałszywe przedstawianie informacji o aplikacji w Konsoli Play, w tym w sekcji Docelowi odbiorcy i treści, może spowodować jej usunięcie lub zawieszenie, dlatego ważne jest podanie właściwych informacji.

Wymagania dotyczące aplikacji dla rodzin

Jeśli jedną z grup docelowych odbiorców aplikacji są dzieci, musisz spełnić te wymagania. Niezastosowanie się do nich może skutkować usunięciem lub zawieszeniem aplikacji.

1. **Treść aplikacji:** treść aplikacji, do której mają dostęp dzieci, musi być dla nich odpowiednia.
2. **Odpowiedzi w Konsoli Google Play:** dokładnie odpowiadaj na pytania na temat aplikacji w Konsoli Google Play i na bieżąco aktualizuj odpowiedzi, by odzwierciedlały zmiany w aplikacji.
3. **Reklamy:** jeśli aplikacja wyświetla reklamy dzieciom lub użytkownikom w nieznanym wieku:
   - do wyświetlania reklam takim użytkownikom używaj wyłącznie pakietów SDK reklam z certyfikatem Google Play;
   - dopilnuj, by reklamy wyświetlane takim użytkownikom nie były oparte na zainteresowaniach (reklamy kierowane na indywidualnych użytkowników, którzy mają określone cechy, na podstawie ich zachowań podczas przeglądania internetu) ani remarketingu (reklamy kierowane na poszczególnych użytkowników na podstawie ich wcześniejszej interakcji z aplikacją lub witryną);
   - dopilnuj, by reklamy wyświetlane takim użytkownikom zawierały treści odpowiednie dla tego typu odbiorców;
   - dopilnuj, by reklamy wyświetlane takim użytkownikom spełniały wymagania formatu reklam dla rodzin;
   - zapewnij zgodność ze stosownymi przepisami prawa i standardami branżowymi dotyczącymi wyświetlania reklam dzieciom.
4. **Zbieranie danych:** musisz zamieścić informację o gromadzeniu przez aplikację (w tym przez używane w niej interfejsy API i pakiety SDK) wszelkich danych osobowych i informacji poufnych o dzieciach. Informacje poufne o dzieciach to m.in. dane uwierzytelniające, dane rejestrowane za pomocą mikrofonu i aparatu, dane o urządzeniu, identyfikator Androida, dane o korzystaniu z reklam i identyfikator wyświetlania reklam.
5. **Interfejsy API i pakiety SDK:** dopilnuj, by interfejsy API i pakiety SDK były prawidłowo zaimplementowane w aplikacji.
   - Aplikacje skierowane wyłącznie do dzieci nie mogą zawierać żadnych interfejsów API ani pakietów SDK, które nie zostały zatwierdzone do używania w usługach przeznaczonych dla dzieci. Obejmuje to Logowanie przez Google (lub dowolne usługi API Google, które mają dostęp do danych powiązanych z kontem Google), Usługi gier Google Play oraz inne usługi API korzystające z protokołu OAuth do uwierzytelniania i autoryzacji.
   - Aplikacje skierowane zarówno do dzieci, jak i starszych odbiorców nie powinny zawierać interfejsów API ani pakietów SDK, które nie zostały zatwierdzone do używania w usługach przeznaczonych dla dzieci. Są jednak dozwolone, jeśli dostępu do nich chroni neutralny ekran wyboru wieku lub są zaimplementowane w sposób, który nie skutkuje zbieraniem danych o dzieciach (np. poprzez udostępnienie opcjonalnej funkcji Logowania przez Google). Aplikacje skierowane zarówno do dzieci, jak i do starszych odbiorców nie mogą wymagać od użytkowników logowania się ani dostępu do treści aplikacji za pomocą interfejsu API lub pakietu SDK, który nie został zatwierdzony do użytku w usługach przeznaczonych dla dzieci.
6. **Polityka prywatności:** na stronie z informacjami o aplikacji musisz umieścić link do polityki prywatności. Link ten musi znajdować się na tej stronie przez cały czas, gdy aplikacja jest dostępna w Sklepie Play. Musi też prowadzić do polityki prywatności, która m.in. dokładnie opisuje, jakie dane zbiera aplikacja i jak z nich korzysta.
7. **Szczególne ograniczenia:**
   - Jeśli aplikacja wykorzystuje rzeczywistość rozszerzoną, tuż przed jej uruchomieniem powinno się wyświetlić stosowne ostrzeżenie. Powinny tam być zawarte te informacje:
     - stosowny komunikat informujący o tym, jak ważny jest nadzór rodzicielski;
     - przypomnienie, by zwracać uwagę na zagrożenia w świecie rzeczywistym (np. na otoczenie);
   - aplikacja nie może wymagać użycia urządzenia, z którego korzystanie nie jest zalecane w przypadku dzieci (takiego jak Daydream czy Oculus).

8. **Zgodność z prawem:** dopilnuj, by aplikacja, w tym używane przez nią interfejsy API i pakiety SDK, była zgodna z amerykańską ustawą Children's Online Privacy and Protection Act (COPPA), unijnym Ogólnym rozporządzeniem o ochronie danych (RODO), a także wszystkimi innymi obowiązującymi przepisami i regulacjami.

Oto kilka często spotykanych przykładów naruszenia zasad:

- aplikacje, które w opisie są promowane jako przeznaczone dla dzieci, ale w rzeczywistości ich treści są odpowiednie tylko dla osób dorosłych;
- aplikacje zawierające interfejsy API, których warunki korzystania zabraniają ich użycia w aplikacjach skierowanych do dzieci;
- aplikacje w sposób pozytywny przedstawiające spożywanie alkoholu, używanie tytoniu lub substancji kontrolowanych;
- aplikacje umożliwiające uprawianie realnego lub symulowanego hazardu;
- aplikacje prezentujące przemoc bądź treści drastyczne lub szokujące, które nie są odpowiednie dla dzieci;
- aplikacje oferujące serwisy randkowe albo porady seksualne lub małżeńskie;
- aplikacje zawierające linki do witryn prezentujących treści naruszające Zasady programu dla deweloperów w Google Play;
- aplikacje, które wyświetlają dzieciom reklamy dla dorosłych (np. prezentujące przemoc, treści erotyczne, hazard). Więcej informacji o zasadach Google Play związanych z reklamami, zakupami w aplikacji i treściami komercyjnymi dla dzieci znajdziesz w zasadach dotyczących reklam odpowiednich dla rodzin i zarabiania na nich.

Program Dla całej rodziny

Aplikacje przeznaczone dla dzieci muszą uczestniczyć w programie Dla całej rodziny. Do programu możesz zgłosić też aplikacje przeznaczone dla wszystkich grup odbiorców, w tym dzieci i całych rodzin.

Aby Twoja aplikacja mogła zostać zaakceptowana w programie, musisz przestrzegać Zasad programu dla deweloperów w Google Play oraz Umowy dystrybucyjnej dla deweloperów. Oprócz tego aplikacja musi być zgodna ze wszystkimi Zasadami dotyczącymi aplikacji dla rodzin oraz spełniać wymagania programu Dla całej rodziny.

Więcej informacji o procesie zgłaszania aplikacji do programu znajdziesz tutaj.

Kwalifikacja do programu

Wszystkie aplikacje uczestniczące w programie Dla całej rodziny i zawarte w nich treści (w tym treści reklam) muszą być odpowiednie dla dzieci i spełniać opisane poniżej wymagania. Aplikacje przyjęte do programu Dla całej rodziny muszą zachować zgodność ze wszystkimi jego wymaganiami. Google Play może odrzucić, usunąć lub zawiesić dowolną aplikację, którą uzna za niezgodną z zasadami programu Dla całej rodziny.

Wymagania programu Dla całej rodziny

1. Aplikacje muszą mieć ocenę Dla wszystkich lub Dla wszystkich od 10 lat w systemie ESRB albo równoważną w innym systemie ocen.
2. W kwestionariuszu oceny treści w Konsoli Google Play należy właściwie opisać interaktywne elementy aplikacji, w tym:
   - czy aplikacja umożliwia interakcje lub wymianę informacji między użytkownikami,
   - czy aplikacja udostępnia firmom zewnętrznym dane osobowe podane przez użytkownika,
   - czy aplikacja udostępnia innym fizyczną lokalizację użytkownika.
3. Jeśli aplikacja używa interfejsu API Android Speech, jej parametr RecognizerIntent.EXTRA_CALLING_PACKAGE należy ustawić na PackageName.
4. Aplikacje mogą korzystać wyłącznie z pakietów SDK reklam z certyfikatem Google Play.
5. Aplikacje przeznaczone dla dzieci nie mogą żądać przyznania dostępu do lokalizacji.
6. Żądając połączenia Bluetooth, aplikacje muszą używać Menedżera urządzeń towarzyszących, chyba że są przeznaczone na urządzenia z systemem operacyjnym w wersji, która go nie obsługuje.

Oto przykłady popularnych aplikacji, które nie kwalifikują się do udziału w programie:

- aplikacje, które mają ocenę Dla wszystkich w systemie ESRB, ale zawierają reklamy promujące hazard;
- aplikacje dla rodziców i opiekunów (np. służące do monitorowania karmienia piersią czy zawierające poradniki na temat prawidłowego rozwoju dziecka);
- poradniki dla rodziców i aplikacje do zarządzania urządzeniem, które są przeznaczone wyłącznie dla rodziców lub opiekunów;
- aplikacje mające ikonę aplikacji lub ikonę programu uruchamiającego, która jest nieodpowiednia dla dzieci.

Kategorie

W przypadku przyjęcia do programu Dla całej rodziny możesz wybrać drugą kategorię związaną z programem, która także opisuje aplikację. Oto kategorie aplikacji dostępne w programie Dla całej rodziny:

Akcja i przygoda: aplikacje i gry pełne akcji, w tym proste wyścigi, przygody w świecie baśni i inne aplikacje oraz gry, które zostały opracowane z myślą o wzbudzaniu ekscytacji.

Gry logiczne: gry, które wymagają myślenia, w tym łamigłówki, układanki, quizy i inne gry stanowiące wyzwanie dla pamięci lub intelektu bądź opierające się na umiejętności logicznego myślenia.

Kreatywność: aplikacje i gry pobudzające kreatywność, które umożliwiają np. rysowanie, malowanie, programowanie lub budowanie różnych rzeczy.

Edukacja: aplikacje i gry opracowane pod okiem ekspertów (pedagogów, specjalistów ds. nauczania czy naukowców), które mają za cel promowanie uczenia się, w tym zdobywania wiedzy, nabywania umiejętności społeczno-emocjonalnych lub fizycznych czy rozwijania kreatywnego myślenia, a także pomagają w zdobyciu elementarnych umiejętności życiowych oraz zachęcają do krytycznego myślenia i rozwiązywania problemów.

Muzyka i film: aplikacje i gry zawierające komponent muzyczny lub filmowy, od aplikacji symulujących instrumenty po takie, które dostarczają muzyczne treści audio i wideo.

Zabawa w udawanie: aplikacje i gry, w których użytkownik może wcielać się w różne role, np. udawać, że jest kucharzem, opiekunem, księciem/księżniczką, strażakiem, policjantem lub postacią fikcyjną.

Reklamy i zarabianie

Zawarte poniżej zasady obowiązują w przypadku wszelkich reklam (zarówno promujących Twoje aplikacje, jak i te autorstwa innych deweloperów), ofert zakupu w aplikacji oraz innych treści komercyjnych (np. płatnego lokowania produktu), które są wyświetlane w aplikacjach podlegających Zasadom dotyczącym aplikacji dla rodzin lub wymaganiom programu Dla całej rodziny. Wszystkie reklamy, oferty zakupu w aplikacji i treści komercyjne w tych aplikacjach muszą być zgodne ze wszystkimi obowiązującymi przepisami (w tym ze wszelkimi wytycznymi branżowymi i regulacjami wewnętrznymi).

Google Play zastrzega sobie prawo do odrzucenia, usunięcia lub zawieszenia aplikacji, która stosuje zbyt agresywne praktyki promocyjne.

Wymagania dotyczące formatów reklam

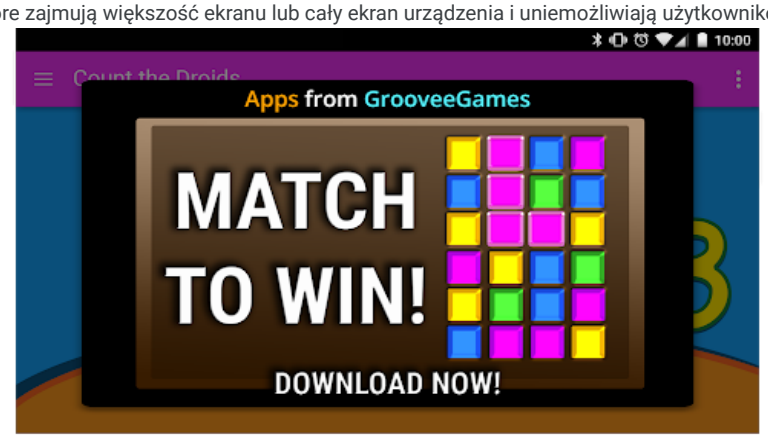
Reklamy i oferty zakupów w aplikacji nie mogą zawierać treści wprowadzających w błąd i nie mogą być zaprojektowane w sposób, który będzie powodował niezamierzone klikanie ich przez dzieci. Zabronione są:

- uciążliwe reklamy, w tym reklamy zajmujące pełny ekran lub zakłócające normalne działanie, które nie informują w jasny sposób, jak je zamknąć (np. ściany reklamowe);
- reklamy, które zakłócają zwykłe korzystanie z aplikacji lub gry i których nie można zamknąć po 5 sekundach (reklamy, które nie zakłócają normalnego korzystania z aplikacji lub gry, mogą być wyświetlane przez ponad 5 sekund – np. treści wideo z reklamami zintegrowanymi);
- reklamy pełnoekranowe lub oferty zakupu w aplikacji wyświetlane tuż po jej uruchomieniu;
- umieszczanie wielu reklam na stronie (np. stosowanie banerów reklamowych, które wyświetlają wiele ofert w jednym miejscu docelowym, lub wyświetlanie więcej niż 1 baneru lub reklamy wideo);
- reklamy lub oferty zakupu w aplikacji, których nie można łatwo odróżnić od treści aplikacji;
- szokujące lub oddziałujące na emocje taktyki zachęcania do wyświetlenia reklamy lub zakupu w aplikacji;
- brak rozróżnienia między wirtualnymi środkami w grze a rzeczywistymi pieniędzmi, które można przeznaczyć na zakupy w aplikacji.

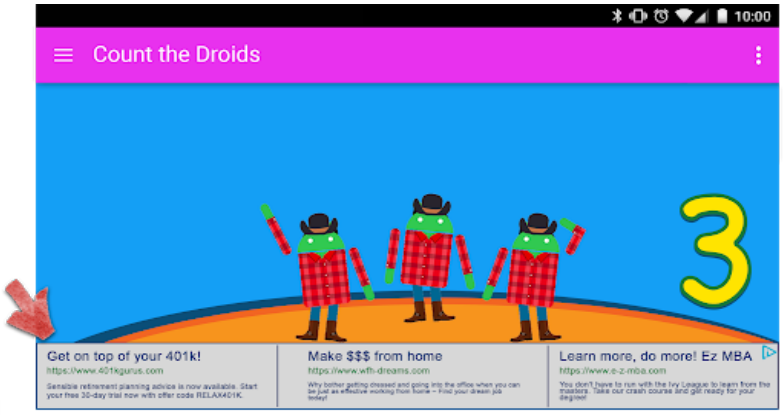
Oto kilka przykładów częstych naruszeń zasad dotyczących formatu reklamy:

- reklamy, które przesuwają się tak, by nie można było ich kliknąć w celu zamknięcia;

- reklamy, które zajmują większość ekranu lub cały ekran urządzenia i uniemożliwiają użytkownikowi ich zamknięcie, na przykład:



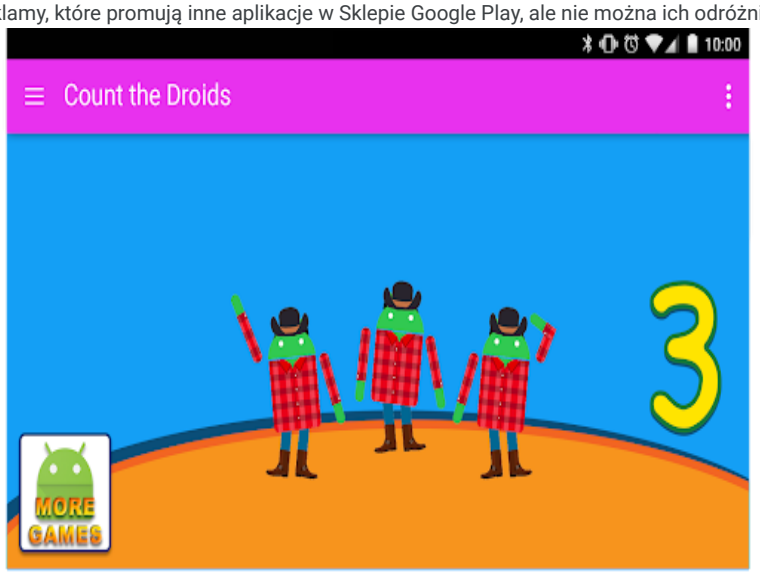
- banery reklamowe z wieloma ofertami, na przykład:



- reklamy, które można pomylić z treścią aplikacji, na przykład:

- przyciski lub reklamy, które promują inne aplikacje w Sklepie Google Play, ale nie można ich odróżnić od treści aplikacji,

  na przykład:



Oto kilka przykładów nieodpowiednich treści reklam, których nie należy wyświetlać dzieciom:

- **Nieodpowiednie treści multimedialne:** reklamy seriali, filmów, albumów muzycznych i innych produktów multimedialnych nieodpowiednich dla dzieci.
- **Nieodpowiednie gry wideo i oprogramowanie do pobrania:** reklamy programów do pobrania i elektronicznych gier wideo nieodpowiednich dla dzieci.
- **Substancje kontrolowane lub szkodliwe:** reklamy alkoholu, tytoniu, substancji kontrolowanych lub dowolnych innych szkodliwych substancji.
- **Hazard:** reklamy symulowanego hazardu, promocyjne konkursy i loterie (nawet takie, w których można uczestniczyć bezpłatnie).
- **Treści dla dorosłych i treści o charakterze erotycznym:** reklamy zawierające treści erotyczne, dwuznaczne i przeznaczone dla dorosłych.
- **Randki i związki:** reklamy serwisów randkowych lub witryn dla dorosłych szukających związku.
- **Przemoc:** reklamy prezentujące przemoc i treści drastyczne nieodpowiednie dla dzieci.

Pakiety SDK reklam

Jeśli wyświetlasz w aplikacji reklamy, a docelowi odbiorcy to wyłącznie dzieci, musisz używać pakietów SDK reklam z certyfikatem Google Play. Jeśli aplikacja jest skierowana do dzieci, ale też starszych użytkowników, zaimplementuj mechanizm sprawdzania wieku, np. neutralny ekran wyboru wieku. Dodatkowo dopilnuj, by reklamy wyświetlane dzieciom pochodziły wyłącznie z pakietów SDK reklam z certyfikatem Google Play. Aplikacje uczestniczące w programie Dla całej rodziny mogą korzystać wyłącznie z samodzielnie certyfikowanych pakietów SDK reklam.

Więcej informacji o tych wymaganiach i listę aktualnie zatwierdzonych pakietów SDK reklam znajdziesz na stronie z zasadami Programu reklam odpowiednich dla rodzin.

Jeśli korzystasz z AdMob, szczegółowe informacje o dostępnych usługach znajdziesz w Centrum pomocy AdMob.

To Ty odpowiadasz za to, by aplikacja spełniała wszystkie wymagania związane z reklamami, zakupami w aplikacji i treściami komercyjnymi. Aby dowiedzieć się więcej o polityce treści i metodach stosowanych przez dostawcę pakietu SDK reklam, skontaktuj się z nim.

Zakupy w aplikacji

Przed dokonaniem zakupu w aplikacji uczestniczącej w programie Dla całej rodziny, Google Play każdorazowo przeprowadza uwierzytelnienie użytkownika. Dzięki temu mamy pewność, że zakup zatwierdza osoba odpowiedzialna finansowo, a nie dziecko.

Egzekwowanie zasad

Deweloperzy nie powinni naruszać naszych zasad, jednak gdy już się to zdarzy, chętnie przekażemy im informacje, które pomogą poprawić aplikację tak, by spełniała nasze wymagania. Jeśli napotkasz jakiekolwiek naruszenia zasad lub masz pytania o to, co z nimi zrobić, skontaktuj się z nami.

Zakres zasad

Nasze zasady obejmują wszystkie materiały, które aplikacja programisty wyświetla lub udostępnia w postaci linków, w tym reklamy pokazywane użytkownikom oraz treści użytkowników umieszczone w aplikacji lub dostępne w niej przez linki. Obowiązują one także w odniesieniu do wszystkich treści pochodzących z Twojego konta dewelopera, które są wyświetlane publicznie w Google Play – w tym Twojej nazwy dewelopera oraz strony docelowej w Twojej publicznej witrynie dewelopera.

Zabraniamy publikowania aplikacji, które umożliwiają użytkownikom instalowanie innych aplikacji na urządzeniach. W przypadku aplikacji, które umożliwiają dostęp do innych aplikacji, gier lub programów bez instalacji, w tym funkcji i usług zapewnianych przez firmy zewnętrzne, musisz dopilnować, by wszystkie udostępniane w ten sposób treści były zgodne ze wszystkimi zasadami Google Play – mogą one podlegać dodatkowej weryfikacji.

Definicje terminów użytych w tych zasadach są takie same jak w Umowie dystrybucyjnej dla deweloperów. Oprócz zachowania zgodności z tymi zasadami i Umową dystrybucyjną dla deweloperów musisz ocenić zawartość swojej aplikacji zgodnie z naszymi Wytycznymi dotyczącymi oceny treści.

Decydując, czy aplikacja powinna być udostępniona w Sklepie Google Play czy z niego usunięta, bierzemy pod uwagę wiele czynników, na przykład potencjalnie szkodliwe działanie czy wysokie ryzyko nadużycia. Ryzyko nadużycia określamy, korzystając z wielu elementów, takich jak historia naruszeń, opinie użytkowników oraz wykorzystanie popularnych marek, postaci i innych zasobów.

Jak działa Google Play Protect

Google Play Protect sprawdza aplikacje, gdy je instalujesz. Oprócz tego okresowo skanuje urządzenie. Jeśli znajdzie potencjalnie szkodliwą aplikację, może:

- wysłać powiadomienie – aby usunąć aplikację, kliknij powiadomienie, a potem Odinstaluj;
- wyłączyć aplikację, dopóki jej nie odinstalujesz;
- automatycznie usunąć aplikację – w większości przypadków po wykryciu szkodliwej aplikacji zobaczysz powiadomienie, że została ona usunięta.

Jak działa ochrona przed złośliwym oprogramowaniem

Aby chronić Cię przed złośliwym oprogramowaniem innych firm, adresami URL i innymi problemami związanymi z bezpieczeństwem, Google może otrzymywać takie informacje:

- połączenia sieciowe urządzenia,
- potencjalnie szkodliwe adresy URL,
- system operacyjny i aplikacje zainstalowane na urządzeniu przez Google Play lub z innych źródeł.

Jeśli dana aplikacja lub URL są potencjalnie niebezpieczne, możesz zobaczyć ostrzeżenie od Google. Aplikacja lub URL mogą zostać usunięte lub zablokowane przez Google, jeśli będziemy mieli pewność, że są szkodliwe dla urządzeń, danych lub użytkowników.

Możesz wyłączyć niektóre z tych zabezpieczeń w ustawieniach urządzenia. Nadal jednak możemy otrzymywać informacje o aplikacjach instalowanych z Google Play, a aplikacje instalowane z innych źródeł mogą być wciąż sprawdzane pod kątem problemów z zabezpieczeniami – informacje na ten temat nie będą przesyłane do Google.

Jak działają alerty o prywatności

Google Play Protect wyśle alert, jeśli aplikacja zostanie usunięta ze Sklepu Google Play ze względu na możliwość dostępu do Twoich danych osobowych. Będziesz mieć możliwość odinstalowania aplikacji.

Proces egzekwowania zasad

Jeśli Twoja aplikacja narusza nasze zasady, podejmiemy odpowiednie działania opisane poniżej.Poza tym dostaniesz od nas e-maila z informacją o podjętym działaniu oraz instrukcją odwołania się od tej decyzji, jeśli uważasz, że popełniliśmy błąd.

Powiadomienia o usunięciu lub powiadomienia administracyjne mogą nie wskazywać każdego z naruszeń zasad występujących w związku z aplikacją lub grupą aplikacji. Deweloperzy muszą rozwiązać problemy związane z naruszeniami i dokładnie sprawdzić, czy pozostała część aplikacji jest w pełni zgodna z naszymi zasadami. Jeśli nie rozwiążesz problemu niezgodności z zasadami we wszystkich aplikacjach, możemy podjąć dalsze działania mające na celu wyegzekwowanie stosowania się do naszych zasad.

Powtarzające się lub poważne naruszenia tych zasad (np. złośliwe oprogramowanie, oszustwo lub aplikacje mogące uszkodzić urządzenie lub wyrządzić inne szkody użytkownikowi) lub Umowy dystrybucyjnej dla deweloperów skutkują zamknięciem danego konta dewelopera w Google Play lub kont z nim powiązanych.

Działania związane z egzekwowaniem zasad

Różne działania związane z egzekwowaniem zasad mogą mieć różny wpływ na Twoją aplikację.W tej sekcji opisujemy różne działania, jakie może podjąć Google Play, oraz ich wpływ na aplikację lub konto dewelopera w Google Play.Te informacje omówiliśmy również w tym filmie.

Odrzucenie

- Nowa aplikacja lub aktualizacja aplikacji przesłana do sprawdzenia nie będzie dostępna w Google Play.
- Jeśli odrzuciliśmy aktualizację już dostępnej aplikacji, wersja opublikowana przed tą aktualizacją pozostanie dostępna w Google Play.
- Odrzucenia nie mają wpływu na dostęp do dotychczas zebranych danych takich jak instalacje, statystyki czy oceny odrzuconej aplikacji.
- Odrzucenia nie mają wpływu na opinię o Twoim koncie dewelopera w Google Play.

Uwaga: nie próbuj ponownie przesłać odrzuconej aplikacji, dopóki nie usuniesz wszystkich naruszeń zasad.

Usunięcie

- Aplikacja wraz z jej wcześniejszymi wersjami zostanie usunięta z Google Play i nie będzie dłużej dostępna do pobrania dla użytkowników.
- Ponieważ aplikacja zostanie usunięta, użytkownicy nie będą mogli zobaczyć strony z informacjami o niej, liczby instalacji, statystyk ani ocen. Te informacje zostaną przywrócone po przesłaniu zgodnej z zasadami aktualizacji usuniętej aplikacji.
- Użytkownicy mogą nie mieć możliwości robienia zakupów w aplikacji ani korzystania z funkcji rozliczeń w aplikacji do czasu zatwierdzenia jej przez Google Play.
- Usunięcie nie wpływa od razu na opinię o Twoim koncie dewelopera w Google Play, jednak wielokrotne usunięcia mogą spowodować jego zawieszenie.

Uwaga: nie próbuj ponownie publikować usuniętej aplikacji, dopóki nie usuniesz wszystkich naruszeń zasad.

Zawieszenie

- Aplikacja wraz z jej wcześniejszymi wersjami zostanie usunięta z Google Play i nie będzie dłużej dostępna do pobrania dla użytkowników.
- Zawieszenie może nastąpić w wyniku rażącego lub wielokrotnego naruszenia zasad albo wielokrotnego odrzucania lub usuwania aplikacji.
- Ponieważ aplikacja zostanie zawieszona, użytkownicy nie będą mogli zobaczyć strony z informacjami o niej, liczby dotychczasowych instalacji, statystyk ani ocen.Te informacje zostaną przywrócone po przesłaniu zgodnej z zasadami aktualizacji usuniętej aplikacji.
- Nie możesz dłużej używać tego samego pliku APK ani pakietu aplikacji.
- Użytkownicy nie będą mieli możliwości robienia zakupów w aplikacji ani korzystania z funkcji rozliczeń w aplikacji do czasu zatwierdzenia jej przez Google Play.
- Zawieszenie ma niekorzystny wpływ na opinię o koncie dewelopera w Google Play.Kolejne zdarzenia tego typu mogą spowodować zamknięcie konta danego dewelopera w Google Play i jego kont powiązanych.

Uwaga: nie próbuj ponownie publikować zawieszonej aplikacji, dopóki Google Play nie poinformuje Cię, że możesz to zrobić.

Ograniczona widoczność

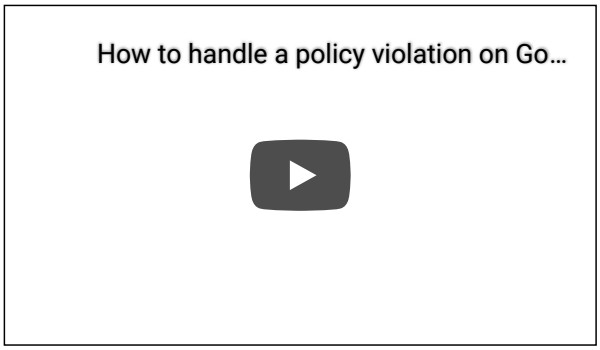
- Możliwość znalezienia Twojej aplikacji w Google Play zostanie ograniczona. Twoja aplikacja pozostanie dostępna w Google Play – będą mieć do niej dostęp użytkownicy dysponujący bezpośrednim linkiem do strony z informacjami o aplikacji w Google Play.
- Nadanie aplikacji stanu ograniczonej widoczności nie ma wpływu na opinię o Twoim koncie dewelopera w Google Play.
- Nadanie aplikacji stanu ograniczonej widoczności nie ma wpływu na możliwość wyświetlania dotychczasowych informacji o aplikacji, liczby instalacji, statystyk czy ocen.

Zamknięcie konta

- W przypadku zamknięcia Twojego konta dewelopera wszystkie aplikacje z Twojego katalogu zostaną usunięte z Google Play i nie będziesz już mieć możliwości publikowania nowych aplikacji. Wszystkie powiązane konta dewelopera w Google Play również zostaną trwale zawieszone.
- Wielokrotne zawieszenia lub zawieszenia wynikające z rażącego naruszenia zasad również mogą spowodować zamknięcie konta w Konsoli Play.
- Ponieważ aplikacje powiązane z zamkniętym kontem zostaną usunięte, użytkownicy nie będą mogli wyświetlić informacji o nich, ich liczby dotychczasowych instalacji, statystyk ani ocen.

Uwaga: każde nowe konto, które spróbujesz otworzyć, również zostanie zamknięte (bez zwrotu opłaty za rejestrację dewelopera) – nie próbuj rejestrować w Konsoli Play nowego konta, jeśli inne Twoje konto zostało zamknięte.

Przypadki naruszenia zasad i ich zgłaszanie



Odwołanie od działań związanych z egzekwowaniem zasad

Przywracamy aplikacje w przypadku popełnienia błędu – jeśli okaże się, że aplikacja nie narusza Zasad programu Google Play ani Umowy dystrybucyjnej dla deweloperów. Jeśli po uważnym przeczytaniu zasad uznasz, że nasza decyzja mogła być błędna, możesz się od niej odwołać, postępując zgodnie z instrukcjami podanymi w e-mailu z powiadomieniem o naszym działaniu.

Dodatkowe materiały

Jeśli potrzebujesz więcej informacji na temat jakiegoś działania związanego z egzekwowaniem zasad lub oceny/komentarza użytkownika, możesz skorzystać z tych materiałów lub skontaktować się z nami przez Centrum pomocy Google Play. Nie możemy zaproponować w tym zakresie żadnej pomocy prawnej. W takich sprawach skontaktuj się z radcą prawnym.

- Weryfikacja aplikacji i odwołania
- Jak zgłosić naruszenie zasad
- Kontakt z Google Play w sprawie zamknięcia konta lub usunięcia aplikacji
- Wyraźne ostrzeżenia
- Zgłaszanie nieodpowiednich aplikacji i komentarzy
- Moja aplikacja została usunięta z Google Play
- Zamykanie konta dewelopera w Google Play

Prześlij opinię na temat tego artykułu

Czy to było pomocne?

Tak Nie

Potrzebujesz dodatkowej pomocy?

Wykonaj te czynności:

Kontakt z nami

Przekaż więcej informacji, byśmy mogli Ci pomóc