Política do programa para desenvolvedores

(em vigor a partir de 15º de abril de 2026, salvo indicação em contrário)

Juntos, podemos criar a plataforma de apps e jogos mais confiável do mundo

Sua inovação impulsiona o sucesso de todos nós. No entanto, esse sucesso traz responsabilidades. As Políticas do programa para desenvolvedores e o Contrato de distribuição do desenvolvedor garantem que nossa parceria continue a oferecer os apps mais inovadores e confiáveis do mundo a mais de um bilhão de pessoas no Google Play. Conheça nossas políticas a seguir.

Conteúdo restrito

Pessoas de todo o mundo usam o Google Play para acessar apps e jogos todos os dias. Antes de enviar um app, verifique se ele é adequado para o Google Play e se está em conformidade com as legislações locais.

Conteúdo prejudicial a crianças

Os apps que não proíbem os usuários de criar, enviar ou distribuir conteúdo que facilite a exploração ou o abuso de crianças estão sujeitos à remoção imediata do Google Play. Isso inclui todos os materiais de abuso sexual infantil. Para denunciar esse tipo de conteúdo em um produto do Google, clique em **Denunciar abuso**. Se você encontrar algo desse tipo em qualquer local da Internet, entre em contato direto com as autoridades competentes do seu país.

Proibimos o uso de apps de modo que coloque crianças em risco. Isso inclui, entre outras práticas, o uso de apps para promover comportamentos predatórios em relação a crianças, por exemplo:

- Interação inadequada direcionada a uma criança, por exemplo, apalpar ou acariciar
- Aliciamento infantil, por exemplo, fazer amizade on-line para facilitar contato sexual on-line ou off-line e/ou trocar imagens sexuais com uma criança
- Sexualização de menores, por exemplo, imagens que retratam, incentivam ou promovem o abuso sexual de crianças ou a representação delas de alguma forma que possa resultar na exploração sexual infantil
- "Sextorção", por exemplo, ameaçar ou chantagear uma criança usando acesso real ou suposto a imagens íntimas dela
- Tráfico infantil, por exemplo, fazer propaganda de crianças ou propostas para exploração sexual comercial

Se identificarmos materiais de abuso sexual infantil, vamos adotar as medidas apropriadas, que podem incluir denúncias ao Centro Nacional para Crianças Desaparecidas e Exploradas dos Estados Unidos. Se você acredita que uma criança corre perigo ou foi alvo de abuso, exploração ou tráfico, entre em contato com as autoridades locais e com uma organização de segurança infantil indicada neste link.

Além disso, não são permitidos apps que tenham conteúdo interessante para crianças, mas apresentem temas adultos, incluindo, mas não se limitando a:

- apps com violência e sangue excessivos;
- apps que retratam ou incentivam atividades nocivas e perigosas.

Também não permitimos apps que promovam uma visão negativa da própria imagem ou do corpo, incluindo aqueles que retratam cirurgia plástica, perda de peso e outras modificações estéticas à aparência física de uma pessoa para fins de entretenimento.

Política de padrões de segurança infantil

O Google Play exige que os apps sociais e de encontros obedecam à nossa Política de padrões de segurança infantil.

Bin | 00:57:08 | Bin

Esses apps precisam:

- **Ter padrões publicados**: o app precisa proibir explicitamente o abuso e exploração sexual infantil (CSAE) em padrões acessíveis ao público, como os termos de serviço do app, as diretrizes da comunidade ou outra documentação de política do usuário disponível publicamente.
- **Fornecer um mecanismo no app para feedback dos usuários**: permita que os usuários enviem comentários, dúvidas ou denúncias no seu aplicativo.
- **Lidar com material de abuso sexual infantil**: adote as medidas adequadas no seu app, incluindo, mas não se limitando a, remoção de material de abuso sexual infantil, após o conhecimento real da ocorrência de acordo com seus padrões publicados e leis relevantes.
- **Obedecer às leis de proteção infantil**: seu app deve estar de acordo com as leis e regulamentações de segurança infantil aplicáveis, incluindo, mas não se limitando a, ter um processo em vigor para denunciar material de abuso sexual infantil confirmado ao Centro Nacional para Crianças Desaparecidas e Exploradas (NCMEC) ou à sua autoridade regional relevante.
- **Oferecer um ponto de contato de segurança infantil**: o app deve oferecer um ponto de contato designado para receber possíveis notificações do Google Play sobre conteúdo de CSAE encontrado no app ou na plataforma. Esse representante precisa estar posicionado para falar sobre seus procedimentos de restrição e revisão e para tomar medidas, se necessário.

Acesse nosso artigo da Central de Ajuda para ver mais sobre esses requisitos e saber como estar em conformidade.

Conteúdo inadequado

Para que o Google Play continue a ser uma plataforma segura e de respeito, criamos padrões que definem e proíbem conteúdos prejudiciais ou impróprios para nossos usuários.

Conteúdo sexual e linguagem obscena

Não são permitidos apps que tenham ou promovam conteúdo sexual ou linguagem obscena, incluindo pornografia ou qualquer conteúdo ou serviço com o objetivo de satisfação sexual. Apps ou conteúdo que aparentam promover ou solicitar atos sexuais em troca de remuneração também não são permitidos. Não permitimos apps que tenham ou promovam conteúdos associados a comportamento sexualmente predatório ou que distribuam conteúdo sexual não consensual. O conteúdo com nudez talvez seja permitido se for principalmente para fins educacionais, documentais, científicos ou artísticos, e não apenas uma exposição sem justificativa.

Os apps de catálogo (ou seja, aqueles que listam títulos de livros/vídeos como parte de um catálogo geral de conteúdos) podem distribuir títulos de livros, incluindo e-books e audiolivros, ou de vídeos que têm conteúdo sexual caso atendam aos seguintes requisitos:

- Os títulos de livros/vídeos que têm conteúdo sexual representam uma fração pequena do catálogo geral do app
- O app não promove ativamente títulos de livros/vídeos que têm conteúdo sexual. Esses títulos ainda poderão aparecer nas recomendações com base no histórico do usuário ou durante promoções gerais
- O app não distribui nenhum título de livro/vídeo que tem conteúdo de risco para crianças, pornográfico ou qualquer outro conteúdo sexual considerado ilegal pela legislação aplicável
- O app protege menores de idade restringindo o acesso a títulos de livros/vídeos que têm conteúdo sexual

Mesmo se tiver conteúdo que viole esta política e estiver indisponível em outras regiões, um app pode ser disponibilizado para os usuários de uma região específica caso o conteúdo seja considerado apropriado nesse local.

Bin | 00:57:08 | Bin

Veja alguns exemplos de violações comuns:

- Representações de nudez sexual ou posições sexualmente sugestivas em que há pessoas nuas, desfocadas ou seminuas e/ou em que a roupa seria inadequada em um contexto público apropriado
- Imagens, animações ou ilustrações de atos sexuais ou poses sexualmente sugestivas ou a representação sexual das partes do corpo
- Conteúdo que retrata ou funciona como acessório sexual, guias sexuais, temas sexuais ilegais e fetiches
- Conteúdo obsceno ou linguagem obscena, incluindo, mas não se limitando a, palavrões, insultos, texto explícito ou palavras-chave de conteúdo adulto/sexual na página "Detalhes do app" ou no app
- Conteúdo que retrata, descreve ou incentiva a zoofilia
- Apps que promovam entretenimento relacionado a sexo, serviços de acompanhantes ou outras atividades que possam ser interpretadas como realização ou solicitação de atos sexuais em troca de remuneração, incluindo, mas não se limitando a, serviços de namoro ou encontros sexuais compensados em que seja necessário ou esteja implícito que um participante dará dinheiro, presentes ou apoio financeiro a outro participante, como "sugar dating"
- Apps que degradam ou objetificam pessoas, como os que alegam despir ou permitir ver através das roupas, mesmo que estejam rotulados como apps de entretenimento ou brincadeira
- Conteúdo ou comportamento que tente ameaçar ou explorar pessoas de maneira sexual, como fotos íntimas sem consentimento, câmera escondida, conteúdo sexual não consensual criado com deepfake ou tecnologia semelhante ou conteúdo de agressão

Discurso de ódio

Não são permitidos apps que promovam a violência ou incitem ódio contra indivíduos ou grupos com base em raça ou origem étnica, religião, deficiência, idade, nacionalidade, condição de veterano, orientação sexual, gênero, identidade de gênero, casta, status de imigrante ou outras características associadas à discriminação sistêmica ou à marginalização.

Apps com conteúdo educacional, documental, científico ou artístico (EDCA) relacionado a nazistas podem ser bloqueados em determinados países, de acordo com as legislações e regulamentações locais.

Veja alguns exemplos de violações comuns:

- Conteúdo ou discurso que declara que um grupo protegido é desumano, inferior ou digno de ser odiado.
- Apps que contêm insultos, estereótipos ou teorias sobre um grupo protegido ter características negativas (por exemplo, ser mal-intencionado, corrupto, mau etc.) ou que afirmam, explícita ou implicitamente, que o grupo é considerado uma ameaça.
- Conteúdo ou discurso que incentiva os outros a acreditar que pessoas devem ser odiadas ou discriminadas porque são membros de um grupo protegido.
- Conteúdo que promove símbolos de ódio, como bandeiras, símbolos, insígnias, instrumentos ou comportamentos associados a grupos de ódio.

Violência

Não são permitidos apps que retratem ou promovam violência gratuita ou outras atividades perigosas. Apps que retratam violência fictícia no contexto de um jogo, como desenhos animados, caça ou pesca, geralmente são permitidos.

Veja alguns exemplos de violações comuns:

- São proibidas as representações gráficas ou descrições de violência realista ou ameaças violentas a qualquer pessoa ou animal.
- Não são permitidos apps que promovam automutil[illegible]mentares, jogos de asfixia nem outras ações que podem resultar em f[illegible]

Bin | 00:57:08 | Bin

Extremismo violento

Organizações terroristas ou outros grupos ou movimentos perigosos que participaram, coordenaram ou se responsabilizaram por atos de violência contra civis não podem publicar apps no Google Play para nenhum propósito, incluindo recrutamento.

Não são permitidos apps com conteúdo relacionado a extremismo violento ou ao planejamento, à organização ou à glorificação de violência contra civis, como promoção de atos terroristas, incitação à violência ou glorificação de ataques terroristas. Se você for postar algum conteúdo relacionado a extremismo violento para fins educacionais, documentais, científicos ou artísticos ("EDCA"), forneça informações relevantes sobre esse contexto.

Eventos sensíveis

Não são permitidos apps que lucrem com ou sejam insensíveis a um evento sensível com impacto social, cultural ou político significativo, como emergências civis, desastres naturais, emergências de saúde pública, conflitos, mortes ou outros eventos trágicos. Apps com conteúdo relacionado a um evento sensível geralmente são permitidos quando são relevantes para fins educacionais, documentais, científicos ou artísticos ou têm o objetivo de alertar os usuários ou conscientizar sobre esse acontecimento.

Veja alguns exemplos de violações comuns:

- Insensibilidade em relação à morte de uma ou mais pessoas reais devido a suicídio, overdose, causas naturais etc.
- Negação da ocorrência de um evento trágico significativo e bem documentado
- Lucro aparente com um evento sensível sem benefício perceptível para as vítimas

Bullying e assédio

Não são permitidos apps que tenham ou promovam ameaças, assédio ou bullying.

Veja alguns exemplos de violações comuns:

- Bullying com vítimas de conflitos internacionais ou religiosos
- Conteúdo com o objetivo de explorar pessoas, incluindo extorsão, chantagem etc.
- Postagem de conteúdo para humilhar um indivíduo publicamente
- Assédio a vítimas de um evento trágico ou a amigos e familiares dessas pessoas

Produtos perigosos

Não permitimos apps que possibilitem a venda de explosivos, armas de fogo, munição nem determinados acessórios para armas de fogo.

- Os acessórios restritos incluem aqueles que permitem que uma arma de fogo simule acionamento automático ou que converta uma arma de fogo em arma automática (por exemplo, coronhas com amortecimento, gatilhos com sistema Gatling, encaixes para trava de gatilho automática ou kits de conversão), além de carregadores ou cintas com mais de 30 cartuchos.

Não são permitidos apps que forneçam instruções para a fabricação de explosivos, armas de fogo, munição, acessórios restritos para armas de fogo ou outras armas. Isso inclui instruções sobre como converter uma arma de fogo em arma automática, ou de acionamento automático simulado.

Maconha

Não permitimos apps que facilitem a venda de maconha ou produtos derivados, independentemente da legalidade da substância.

Veja alguns exemplos de violações comuns:

Bin | 00:57:08 | Bin

- Permitir que os usuários solicitem maconha por meio de um recurso de carrinho de compras no app.
- Ajudar os usuários a organizar a entrega ou a retirada de maconha.
- Facilitar a venda de produtos que contenham THC (tetra-hidrocanabinol), incluindo óleos de CBD com THC.

Tabaco e bebidas alcoólicas

Não permitimos apps que facilitem a venda de tabaco ou de produtos que contêm nicotina (como cigarros eletrônicos, canetas vaporizadoras e bolsas de nicotina) ou incentivem o uso ilegal ou inadequado de álcool, tabaco ou nicotina.

Veja alguns exemplos de violações comuns:

- Não é permitido descrever ou incentivar o uso ou a venda de bebidas alcoólicas ou tabaco a menores.
- Não é permitido sugerir que o consumo de tabaco pode melhorar o comportamento social, sexual, profissional, intelectual ou atlético.
- Não é permitido retratar o uso excessivo de bebidas alcoólicas de maneira favorável, incluindo a representação de consumo compulsivo ou de competições.
- Não são permitidos anúncios, promoções ou destaques de produtos de tabaco, incluindo anúncios, banners, categorias e links para sites de venda de tabaco.
- A venda limitada de produtos de tabaco em apps de entrega de alimentos/mantimentos pode ser permitida em determinadas regiões, sujeita a salvaguardas de restrição de idade, como a verificação de identidade na entrega.
- Talvez seja permitida a venda de produtos comercializados para cessação do tabagismo, sujeita a salvaguardas de restrição de idade.

Conteúdo e funcionalidade com restrição de idade

Para garantir a segurança das crianças e evitar que elas tenham acesso a conteúdo potencialmente nocivo, é preciso usar as ferramentas e funcionalidades do Play Console para bloquear menores de idade nos seguintes casos:

1. Apps que dão acesso a jogos, concursos e jogos de azar com dinheiro real.
2. Apps que têm a funcionalidade principal de facilitar encontros e relacionamentos. Apps em que encontros ou relacionamentos sejam um recurso incidental não precisam bloquear menores, desde que implementem verificações de idade adequadas para impedir que eles acessem esses recursos específicos.

Serviços financeiros

Não permitimos apps que exponham os usuários a produtos e serviços financeiros enganosos ou nocivos.

Para os fins desta política, são considerados produtos e serviços financeiros aqueles que estão relacionados ao gerenciamento e investimento de moedas e criptomoedas, incluindo consultoria personalizada.

Caso seu app tenha ou promova produtos e serviços financeiros, será preciso obedecer a regulamentações estaduais e locais de todos os países ou regiões a que ele é destinado. Por exemplo, incluir a divulgação de informações específicas exigidas pela legislação local.

Para apps que oferecem qualquer tipo de recurso financeiro, preencher o formulário de declaração de tais funcionalidades no Play Console é um requisito obrigatório.

Bin | 00:57:08 | Bin

Opções binárias

Não são permitidos apps que ofereçam aos usuários a capacidade de negociar opções binárias.

Empréstimos

Empréstimos pessoais: é a concessão de crédito em dinheiro por um indivíduo, organização ou entidade a um consumidor individual de modo não recorrente e sem o propósito de financiamento estudantil ou compra de um ativo fixo. Os consumidores de empréstimos pessoais precisam de informações sobre a qualidade, as características, as taxas, o cronograma de repagamento, os riscos e as vantagens desses produtos para tomar decisões conscientes sobre a possibilidade de assumir o empréstimo.

- Alguns exemplos disso são os empréstimos pessoais, consignados, empréstimos peer-to-peer e com alienação da propriedade.
- Não estão incluídos: hipotecas, financiamentos para automóveis e linhas de crédito rotativo (como cartões de crédito ou linhas de crédito pessoal).

EWA: sigla em inglês para empréstimos de acesso ao salário (Earn Wage Access), é um serviço financeiro que permite que pessoas físicas acessem parte dos seus salários que já foram ganhos, mas ainda não foram pagos pelo empregador. Ao contrário dos empréstimos tradicionais, os serviços de EWA são caracterizados pelo seguinte:

- Mecanismo de repagamento: ocorre automaticamente por uma dedução na folha de pagamento ou por uma transação de pagamento automático vinculada à conta bancária do usuário. Em caso de falha no pagamento automático, não são cobrados juros, multas ou taxas adicionais.
- Acesso baseado na renda: a quantia disponível ao usuário é estritamente limitada aos salários a que ele tem direito durante o período de pagamento atual, garantindo que não haja empréstimos contra a renda futura.
- Estrutura de taxas: os serviços de EWA não cobram juros, e sim uma taxa baixa fixa ou uma porcentagem com base na taxa de transação para uso. Uma taxa razoável é mínima e transparente, refletindo o custo real de prestar o serviço sem sobrecarregar o usuário, provavelmente entre US$ 1 e US$ 5 por transação ou 1 a 5% do adiantamento.
- Sem criação de dívidas: os serviços de EWA geralmente não relatam as transações a agências de crédito, garantindo que não afetem o score de crédito do usuário nem contribuam para o acúmulo de dívidas a longo prazo.

Os apps que oferecem empréstimo pessoal, incluindo, mas não se limitando a, apps que oferecem empréstimos de maneira direta, geradores de leads e aqueles que conectam consumidores a credores terceirizados, precisam ter a categoria "Finanças" no Play Console e divulgar as seguintes informações nos próprios metadados:

- Períodos mínimo e máximo para repagamento.
- A taxa percentual anual (APR) máxima, que geralmente inclui juros, taxas e outros custos por um ano, ou outra taxa similar calculada de acordo com a legislação local.
- Um exemplo representativo do custo total do empréstimo, incluindo o valor inicial e todas as taxas aplicáveis.
- Uma Política de Privacidade que declare de maneira abrangente o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis dos usuários, sujeita às restrições descritas nesta política.

Não são permitidos apps de empréstimo pessoal que exijam quitação em até 60 dias a partir da data de emissão. Definimos esse serviço como "empréstimo pessoal de curto prazo".

Os apps que oferecem empréstimos de EWA, incluindo, mas não se limitando a, apps que oferecem esses empréstimos de maneira direta, geradores de leads e aqueles que conectam consumidores a credores terceirizados, precisam ter a categoria Fina[illegible]ar as seguintes informações nos próprios metadados:

Bin | 00:57:08 | Bin

- Termos e Condições de Repagamento.
- Todas as taxas, inclusive de assinatura, transação e relacionadas ao fornecimento do empréstimo.
- Um exemplo representativo do custo total do empréstimo, incluindo todas as taxas.
- Uma Política de Privacidade que declare de maneira abrangente o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis dos usuários, sujeita às restrições descritas nesta política.

O Google precisa conseguir associar sua conta de desenvolvedor às licenças e documentações enviadas que comprovam sua qualificação para prestar serviços de empréstimo pessoal. Em alguns casos, será necessário apresentar outras informações e documentações para confirmar que sua conta está em conformidade com as leis e regulamentações locais.

Os apps de empréstimo pessoal, apps que têm como função principal facilitar o acesso a esse serviço (como facilitadores ou geradores de leads), ou a linha de crédito, apps acessórios a empréstimo ou crédito (calculadoras de empréstimo, guias de empréstimo etc.) e apps de EWA não podem acessar dados sensíveis, como fotos e contatos. As seguintes permissões são proibidas:

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

Os apps que usam APIs ou informações sensíveis estão sujeitos a restrições e requisitos adicionais. Encontre mais informações na política de permissões.

Empréstimos pessoais com taxa percentual anual (APR) alta

Nos Estados Unidos, não são permitidos apps de concessão de empréstimo pessoal em que a taxa percentual anual (APR) seja igual ou maior que 36%. Os apps de empréstimo pessoal nos Estados Unidos precisam exibir a APR máxima, calculada de maneira consistente com a lei de transparência em empréstimos Truth in Lending Act (TILA) .

A política se aplica aos apps que oferecem empréstimos de maneira direta, aos geradores de leads e aos que conectam consumidores a credores terceirizados.

Requisitos específicos dos países

Os apps de empréstimo pessoal destinados aos países listados precisam obedecer a requisitos adicionais e apresentar documentação complementar como parte da Declaração de Recursos Financeiros no Play Console. Os apps que oferecem empréstimos de acesso antecipado ao salário (EWA, na sigla em inglês) estão sujeitos a esses requisitos na medida aplicável nas jurisdições relevantes. Caso o Google Play peça, você precisará enviar mais informações ou documentos relacionados à conformidade com os requisitos de regulamentação e licenciamento aplicáveis.

1. **Índia**
   - Somente os apps que enviarem uma licença e estiverem na lista de "Apps de Empréstimo Digital (DLAs, na sigla em inglês) implantados por Entidades Regulamentadas" do Reserve Bank of India (RBI) poderão enviar apps de empréstimo pessoal ao Google Play para análise. Consulte as orientações neste artigo da Central de Ajuda.

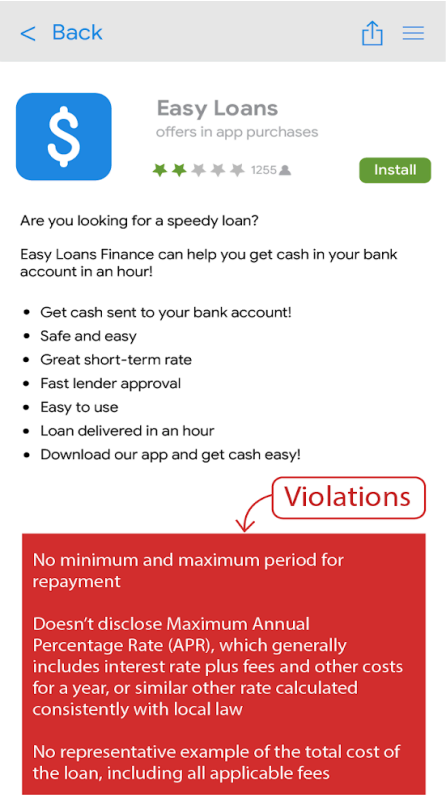
- Se você não tem envolvimento direto em atividades de empréstimo de dinheiro e apenas fornece uma plataforma para mediar essas operações entre usuários e bancos ou Instituições Financeiras Não Bancárias (NBFCs, na sigla em inglês) regis[illegible] adequadamente na declaração.
  - Além disso, os nomes de todas as NBFCs e bancos registrados precisam ser declarados em destaque na descrição do app.

Bin | 00:57:08 | Bin

2. **Indonésia**
   - Caso o app esteja envolvido com Serviços de Empréstimo de Dinheiro Baseados em Tecnologia da Informação, nos termos do Regulamento OJK nº 77/POJK.01/2016 (e alterações periódicas), será necessário enviar uma cópia da licença válida para nossa análise.
3. **Filipinas**
   - Todas as empresas de financiamento e empréstimo que oferecem Crédito por Plataformas de Empréstimo On-line (OLPs, na sigla em inglês) precisam ter os Números de Registro da Comissão de Valores Mobiliários (SEC, na sigla em inglês) e do Certificado de Autoridade (CA) da Comissão de Valores Mobiliários das Filipinas (PSEC, sigla em inglês).
     - Além disso, é preciso divulgar a Razão Social, o Nome da Empresa, o Número de Registro da PSEC e o Certificado de Autoridade (CA) para Operar uma Empresa de Financiamento/Empréstimo na descrição do app.
   - Os apps envolvidos em atividades de financiamento coletivo com base em crédito, como empréstimo entre pessoas (P2P), ou conforme definido nas Regras e nos Regulamentos que Regem o Financiamento Coletivo (Regras de CF), precisam processar transações com Intermediários de Financiamento Coletivo Registrados na PSEC.
4. **Nigéria**
   - Os Credores Digitais precisam seguir e preencher os PRINCÍPIOS E DIRETRIZES REGULAMENTARES/DE REGISTRO TEMPORÁRIOS E LIMITADOS PARA EMPRÉSTIMO DIGITAL DE 2022 (e alterações periódicas) da Comissão Federal de Proteção à Concorrência e ao Consumidor (FCCPC, na sigla em inglês) da Nigéria, além de ter uma carta de aprovação verificável da FCCPC.
   - Os Agregadores de Empréstimo precisam apresentar a documentação e/ou a certificação para serviços de empréstimo digital e os detalhes de contato de todos os credores digitais parceiros.
5. **Quênia**
   - As Provedoras de Crédito Digitais (DCPs) precisam concluir o processo de registro da DCP e ter uma licença do Banco Central do Quênia (CBK, siglas em inglês). É preciso enviar uma cópia da sua licença do CBK na declaração.
   - Se você não tem envolvimento direto em atividades de empréstimo de dinheiro e apenas fornece uma plataforma para facilitar essas operações entre as DCPs registradas e os usuários, informe isso de maneira explícita na declaração e envie uma cópia da licença da DCP dos parceiros em questão.
   - No momento, só aceitamos declarações e licenças de entidades publicadas de acordo com o Diretório de Provedoras de Crédito Digitais no site oficial do CBK.
6. **Paquistão**
   - Cada credor de uma Instituição Financeira Não Bancária (NBFC) só pode publicar um App de Empréstimo Digital (DLA, siglas em inglês). Os desenvolvedores que tentarem publicar mais de um DLA por NBFC poderão ter a conta de desenvolvedor e todas as outras associadas encerradas.
   - É necessário enviar um documento da Comissão de Valores Mobiliários do Paquistão (SECP, na sigla em inglês) que comprova sua qualificação para oferecer ou facilitar serviços de empréstimo digital no Paquistão. Os apps de empréstimo de curto prazo não são permitidos, mas pode haver raras exceções quando explicitamente permitido pelas leis e regulamentações do Paquistão.
7. **Tailândia**

- Os apps de empréstimo pessoal direcionados a usuários na Tailândia, com taxas de juros de 15% ou mais, precisam ter uma licença válida do Banco da Tailândia (BoT) ou do Ministério das Finanças (MoF, siglas em inglês). Os desenvolve[illegible] documentação que comprove a capacidade de oferecer ou facilitar [illegible] ândia. Essa documentação deve incluir o seguinte:
  - Uma cópia da licença emitida pelo Banco da Tailândia para operar como provedora de empréstimo pessoal ou organização financeira nano.
  - Uma cópia da licença comercial Pico Finance emitida pelo Ministério das Finanças para operar como um credor Pico ou Pico-plus.
- Todos os apps de empréstimo pessoal destinados à Tailândia precisam mostrar as seguintes informações na página de detalhes do Google Play:
  - O nome dos provedores de serviços de empréstimo licenciados pelo Banco da Tailândia (BoT) ou pelo Escritório de Política Fiscal (FPO, siglas em inglês).
  - Nome de pessoa jurídica do desenvolvedor.
  - Taxas de juros máximas e todas as taxas.
- Além das informações acima, os apps de empréstimo pessoal direcionados à Tailândia com taxas de juros abaixo de 15% também precisam incluir o seguinte:
  - A declaração "Este é um provedor de empréstimos não regulamentado de acordo com o BoT e o FPO".

Veja alguns exemplos de violações comuns:



Jogos de azar com dinheiro real, jogos e concursos

Permitimos apps de jogos de azar com dinheiro real, anúncios relacionados a esses tipos de jogos, programas de fidelidade com resultados gamificados e apps de fantasy games diários que atendam a determinados requisitos.

Apps de jogos de azar

Sujeito a restrições e conformidade com todas as políticas do Google Play, permitimos apps que viabilizem ou facilitem jogos de azar on-line em países selecionados, desde que o desenvolvedor conclua o processo de inscrição para apps de jog[illegible] Google Play, seja um operador governamental aprovado e/ou registrado c[illegible] pela autoridade governamental adequada no país especificado e apresente uma licença operacional válida no país especificado para o tipo de jogos de azar on-line que quer oferecer.

Bin | 00:57:08 | Bin

Só permitimos apps de jogos de azar licenciados ou autorizados que tenham os tipos de produtos de jogos de azar on-line a seguir.

- Jogos de cassino on-line
- Apostas esportivas
- Corrida de cavalos (onde regulamentada e licenciada separadamente das apostas esportivas)
- Loterias
- Fantasy games diários

Os apps precisam atender aos seguintes requisitos:

- O desenvolvedor precisa passar pelo processo de inscrição para distribuir o app no Google Play.
- O app precisa obedecer a todas as legislações e padrões do setor aplicáveis dos países em que é distribuído.
- O desenvolvedor precisa ter uma licença de jogos de azar válida para cada país ou estado/território em que o app é distribuído.
- O desenvolvedor não pode oferecer um tipo de jogos de azar que exceda o escopo da licença.
- O app precisa impedir que usuários menores de idade façam uso dele.
- O app precisa impedir o acesso e o uso em países, estados/territórios ou áreas geográficas não cobertos pela licença de jogos de azar fornecida ao desenvolvedor.
- O app NÃO pode ser publicado como pago no Google Play nem usar o Faturamento do Google Play no app.
- O app precisa ser gratuito para download e instalação na Google Play Store.
- O app precisa ter a classificação "AO" (Adult Only, "somente adultos") ou equivalente pela Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês).
- O app e a página de detalhes dele precisam mostrar informações claras sobre a participação responsável em jogos de azar.

Outros apps de jogos com dinheiro real, concursos e torneios

Para todos os outros apps que não atendem aos requisitos de qualificação de apps de jogos de azar mencionados acima e que não estão incluídos em "Outros testes de jogos com dinheiro real" abaixo, não permitimos conteúdo ou serviços que permitam ou facilitem a participação dos usuários em jogos de azar ou o uso de dinheiro real (incluindo itens no app comprados em dinheiro) para receber um prêmio de valor monetário real. Isso inclui, entre outros, cassinos on-line, apostas esportivas, loterias e jogos que aceitam dinheiro ou oferecem prêmios em dinheiro ou outros itens de valor real (exceto os programas permitidos nos requisitos dos programas de fidelidade gamificados descritos abaixo).

Exemplos de violações

- Jogos que aceitam dinheiro em troca de uma oportunidade de ganhar um prêmio físico ou monetário
- Apps que têm elementos ou recursos de navegação (por exemplo, itens de menu, guias, botões, WebViews etc.) com uma "call-to-action" para apostar ou participar de jogos, concursos ou torneios que usam dinheiro real, como apps que convidam os usuários com palavras como "APOSTE!", "INSCREVA-SE!" ou "CONCORRA!" em um torneio para ter a chance de ganhar um prêmio em dinheiro

- Apps que aceitam ou gerenciam apostas, moedas no app, ganhos ou depósitos para apostar em ou ganhar um prêmio físico ou monetário

Outros pilotos de jogos com dinheiro real

Bin | 00:57:08 | Bin

Eventualmente, podemos lançar pilotos por tempo limitado para alguns tipos de jogos com dinheiro real em regiões específicas. Saiba mais nesta página da Central de Ajuda. O piloto de jogos de garra on-line no Japão foi encerrado em 11 de julho de 2023. A partir de 12 de julho de 2023, os apps de jogos de garra on-line poderão ser exibidos no Google Play, sujeitos à legislação aplicável e a determinados requisitos.

Programas de fidelidade gamificados

Quando for permitido por lei e não houver requisitos adicionais de licenciamento de jogos ou jogos de azar, permitimos programas de fidelidade que recompensam os usuários com prêmios reais ou o equivalente monetário, de acordo com os seguintes requisitos de qualificação da Play Store:

Para todos os apps (jogos e outros):

- Os benefícios, as cortesias ou as recompensas do programa de fidelidade precisam ser claramente complementares e subordinados a qualquer transação monetária qualificada no app (em que a transação monetária qualificada precisa ser uma transação separada real para fornecer produtos ou serviços independentes do programa de fidelidade) e não podem estar sujeitos a compras ou vinculados a modos de troca que violem as restrições da Política de jogos de azar com dinheiro real, jogos e concursos.
  - Por exemplo, nenhuma parte da transação monetária qualificada poderá representar uma tarifa ou um prêmio para participar do programa de fidelidade, e a transação monetária qualificada não poderá resultar na compra de bens ou serviços acima do preço normal.

Para apps de jogos :

- Os pontos de fidelidade ou as recompensas com benefícios, cortesias ou prêmios associados a uma transação monetária qualificada só podem ser concedidos e resgatados de forma fixa, em que a proporção é documentada de forma visível no app e também dentro das regras oficiais disponíveis publicamente para o programa. Além disso, o ganho de benefícios ou o valor de resgate **não** poderá ser apostado, concedido nem multiplicado de acordo com o desempenho no jogo ou em resultados baseados em probabilidades.

Para apps que não são de jogos:

- Os pontos de fidelidade ou as recompensas poderão ser vinculados a um concurso ou a resultados com base em probabilidades, desde que atendam aos requisitos indicados abaixo. Os programas de fidelidade com benefícios, cortesias ou recompensas associados a uma transação monetária qualificada precisam:
  - publicar as regras oficiais para o programa no app;
  - para programas que envolvam sistemas de recompensas variáveis, aleatórias ou baseadas em probabilidades, divulgar nos termos oficiais do programa 1) as chances dos programas que usam probabilidades fixas para determinar as recompensas e 2) o método de seleção (por exemplo, as variáveis usadas para determinar a recompensa) de todos os programas;
  - especificar um número fixo de vencedores, prazo fixo de inscrição e data de concessão do prêmio, por promoção, de acordo com os termos oficiais de um programa que oferece sorteios, prêmios ou outras promoções de estilo semelhante;
  - documentar todas as proporções fixas de acréscimo e resgate de pontos ou recompensas de fidelidade de maneira visível no app e nos termos oficiais do programa.

Tipo do app com programa de fidelidade	Programas de fidelidade gamificados e prêmios variáveis	Recompensas de fidelidade com base em uma proporção/programação fixa	Termos e Condições do programa de	Termos e Condições precisam divulgar as chances ou os métodos de seleção dos programas de fidelidade baseados em probabilidades
Jogo	Não permitidos	Permitidas	Obrigatórios	N/A (apps de jogos não contêm elementos baseados em probabilidades nos programas de fidelidade)
Outros	Permitidos	Permitidas	Obrigatórios	Sim

Bin | 00:57:08 | Bin

Anúncios de jogos de azar ou jogos, concursos e torneios com dinheiro real em apps distribuídos pelo Google Play

Permitimos apps com anúncios que promovem jogos de azar e jogos, concursos e torneios com dinheiro real caso atendam aos seguintes requisitos:

- O app, o anúncio e os anunciantes precisam obedecer a todas as legislações e padrões do setor aplicáveis nos locais em que o anúncio for exibido.
- O anúncio precisa atender a todos os requisitos locais de licenciamento aplicáveis a todos os produtos e serviços promovidos que sejam relacionados com jogos de azar.
- O app não pode exibir anúncios de jogos de azar para menores de 18 anos.
- O app não pode estar inscrito no programa Feito para Família.
- O app não pode segmentar pessoas menores de 18 anos.
- Se você promover um app de jogos de azar (conforme definido acima), o anúncio precisará mostrar claramente informações sobre como participar de jogos de azar de maneira responsável na página de destino, na página "Detalhes do app" ou no próprio app.
- O app não pode ter conteúdo de jogos de azar simulados (por exemplo, apps sociais de cassino ou caça-níqueis virtuais).
- O app não pode ter funções de suporte para jogos de azar nem para jogos, loterias ou torneios com dinheiro real (por exemplo, funcionalidades que ajudem com apostas, pagamentos, acompanhamento de placares/desempenho/prognósticos esportivos ou gerenciamento de fundos de jogos de azar).
- O conteúdo do app não pode promover ou direcionar os usuários a serviços de jogos de azar ou jogos, loterias ou torneios com dinheiro real.

Somente os apps que atendem a todos esses requisitos na seção listada (acima) podem incluir anúncios de jogos de azar e jogos, loterias ou torneios com dinheiro real. Os "Apps de jogos de azar" (conforme definido acima) ou os "Apps de fantasy games diários" (conforme definido abaixo) aceitos que atendem aos requisitos de 1 a 6 acima podem incluir anúncios de jogos de azar ou de jogos, loterias ou torneios com dinheiro real.

Exemplos de violações

- Um app criado para usuários menores de idade exibe um anúncio que promove serviços de jogos de azar.
- Um jogo de cassino simulado promove ou direciona os usuários para cassinos com dinheiro real.
- Um app dedicado ao acompanhamento de prognósticos esportivos contém anúncios de jogos de azar integrados com links para um site de apostas esportivas.

- Apps com anúncios de jogos de azar que violam nossa política de anúncios enganosos, como anúncios exibidos aos usuários na forma de botões, ícones ou outros elementos interativos no app.

Apps de fantasy sport diário (DFS, na sigla

Bin | 00:57:08 | Bin

Os apps de fantasy sports diários (DFS, na sigla em inglês), definidos conforme a lei local aplicável, só serão permitidos se cumprirem com os seguintes requisitos:

- O app 1) é distribuído apenas nos Estados Unidos ou 2) está qualificado de acordo com os requisitos para apps de jogos de azar e o processo de inscrição mencionados acima para países diferentes dos EUA.
- O desenvolvedor precisa passar pelo processo de inscrição para DFS e ser aceito para distribuir o app no Google Play.
- O app precisa estar em conformidade com todas as legislações e padrões do setor aplicáveis aos países em que é distribuído.
- O app precisa impedir que usuários menores de idade apostem ou façam transações monetárias por meio dele.
- O app NÃO pode ser publicado como pago no Google Play nem usar o Faturamento do Google Play no app.
- O app precisa ser gratuito para download e instalação na Play Store.
- O app precisa ter a classificação "AO" (Adult Only, "somente adultos") ou equivalente pela Coalizão Internacional de Classificação Indicativa (IARC, na sigla em inglês).
- O app e a página "Detalhes do app" precisam mostrar informações claras sobre a participação responsável em jogos de azar.
- O app precisa obedecer a todas as legislações e a todos os padrões do setor aplicáveis dos estados ou territórios dos EUA em que é distribuído.
- O desenvolvedor precisa ter uma licença válida em cada estado ou território dos EUA que exija isso para apps de fantasy sport diário.
- O app precisa impedir o uso em estados ou territórios dos EUA em que o desenvolvedor não tem a licença necessária para apps de fantasy sport diário.
- O app precisa impedir o uso em estados ou territórios dos EUA em que apps de fantasy sports diários são ilegais.

Atividades ilícitas

Apps que facilitem ou promovam atividades ilícitas não são permitidos.

Veja alguns exemplos de violações comuns:

- Facilitar a venda ou compra de drogas ilícitas
- Descrever ou incentivar o uso ou a venda de drogas, álcool ou tabaco para menores
- Dar instruções para o cultivo ou fabricação de drogas ilícitas

---

Conteúdo gerado pelo usuário

O conteúdo gerado pelo usuário (UGC) são as contribuições dos usuários para o app que ficam visíveis ou acessíveis para pelo menos um subconjunto de usuários.

Os apps que têm ou apresentam UGC, incluindo navegadores ou clientes especializados para direcionar os usuários a uma plataforma de UGC, precisam implementar uma moderação de UGC adequada, robusta, eficaz e contínua que:

- exija que os usuários aceitem os Termos de Uso e/ou a política do usuário do app antes de criarem ou fazerem o upload de UGC;

- defina o que são conteúdos e comportamentos questionáveis (de maneira compatível com as Políticas do programa para desenvolvedores do Google Play) e fazer a proibição deles nos Termos de Uso ou nas políticas do usuário do app;
- implemente uma moderação de UGC de maneira r[illegible] Bin | 00:57:08 | Bin [illegible]ipos de UGC hospedados pelo app. Isso inclui oferecer um sistema no app para denunciar e bloquear UGC e usuários questionáveis, além de tomar medidas contra eles quando apropriado; Diferentes experiências com UGC podem exigir diferentes esforços de moderação. Por exemplo:
  - Apps com UGC que identifiquem um grupo específico de usuários por meios como verificação do usuário ou registro off-line (por exemplo, apps usados exclusivamente dentro de uma escola ou empresa, etc.) precisam oferecer uma funcionalidade no app para denunciar conteúdo e usuários.
  - Recursos de UGC que permitem interações individuais entre usuários específicos (por exemplo, mensagens diretas, inclusão de tags, menções, etc.) precisam oferecer uma funcionalidade no app para bloquear usuários.
  - Apps que oferecem acesso UGC acessível publicamente, como apps de redes sociais e blogs, precisam implementar funcionalidades no app para bloquear e denunciar usuários e conteúdo.
  - No caso de apps de realidade aumentada (RA), a moderação de UGC (incluindo o sistema de denúncias no app) precisa considerar o UGC de RA questionável (por exemplo, uma imagem de RA sexualmente explícita) e o local confidencial de ancoragem do RA (por exemplo, conteúdo de RA ancorado em um área restrita, como uma base militar ou uma propriedade privada em que a ancoragem de RA pode causar problemas para o proprietário).
- Ter salvaguardas para evitar que a monetização no app incentive o comportamento questionável do usuário.

Conteúdo sexual incidental

O conteúdo sexual é considerado "incidental" quando aparece em um app de UGC que (1) oferece acesso principalmente a conteúdo não sexual e (2) não promove nem recomenda conteúdo sexual ativamente. Conteúdo sexual definido como ilegal pela legislação aplicável e de risco para crianças não é considerado "incidental" e não é permitido.

Os apps de UGC podem ter conteúdo sexual incidental quando todos os requisitos a seguir são atendidos:

- Esse conteúdo é ocultado por padrão por filtros que exigem pelo menos duas ações do usuário para desativação completa, por exemplo: material escondido por um intersticial ofuscante ou não visível por padrão, a menos que a "pesquisa segura" seja desativada.
- As crianças, conforme definidas pela Política para famílias, são expressamente proibidas de acessar o app por sistemas de verificação de idade, como uma tela neutra de informações de idade ou um sistema apropriado como disposto pela legislação aplicável.
- O app fornece respostas precisas ao questionário de classificação do conteúdo relacionado a UGC, conforme exigido pela política de classificação do conteúdo.

Os apps que tiverem como função principal a exibição de UGC questionável serão removidos do Google Play. Da mesma forma, os apps usados principalmente para hospedar UGC questionável ou que forem conhecidos pelos usuários por serem lugares onde esse tipo de conteúdo se desenvolve também serão removidos do Google Play.

Veja alguns exemplos de violações comuns:

- Promoção de conteúdo sexualmente explícito gerado pelo usuário, incluindo a implementação de recursos pagos que incentivam principalmente o compartilhamento de conteúdo questionável
- Apps com UGC que não tenham salvaguardas suficientes contra ameaças, assédio ou bullying, especialmente voltados a menores
- Postagens, comentários ou fotos em um app que tenham como objetivo principal assediar ou expor outra pessoa a abuso, ataque malicioso ou deboche
- Apps que não atendam às reclamações dos usuários sobre conteúdo questionável

Conteúdo e serviços relacionados à saúde

Não são permitidos apps que exponham os usuários a conteúdo e serviços prejudiciais à saúde.

Se você oferece um app que tem ou promove conteú [illegible] recisa obedecer às leis e regulamentações locais.

Bin | 00:57:08 | Bin

Apps de saúde e medicina

Se o app oferece informações ou recursos relativos à saúde como parte das funções ou acessa dados de saúde para viabilizar outros recursos não relacionados, ele precisa obedecer às atuais Políticas para Desenvolvedores do Google Play, inclusive a sobre Privacidade, Fraude e Uso Indevido de Dispositivos, além de cumprir os requisitos abaixo:

- **Declaração do Console:**
  - Todos os desenvolvedores precisam preencher o formulário de declaração de apps de saúde na página de conteúdo do app (Monitorar e aprimorar > Política > Conteúdo do app) no Play Console. Saiba mais sobre como dar as informações necessárias para o formulário de declaração de apps de saúde.
- **Requisitos para a Política de Privacidade e a Declaração em Destaque:**
  - O app precisa incluir um link para a Política de Privacidade no campo designado no Play Console e outro link ou texto da política no próprio app. Sua política precisa estar disponível de forma não editável em um URL ativo, publicamente acessível e sem fronteira geográfica virtual, conforme definido na seção "Segurança dos dados". Não use PDFs.
  - A Política de Privacidade, assim como outras declarações no app, precisa explicar claramente como o app acessa, coleta, usa e compartilha dados pessoais e sensíveis do usuário, sem se limitar aos dados divulgados na seção "Segurança dos dados" acima. Se o app tem recursos ou dados regulamentados por permissões perigosas ou de execução , ele precisa atender a todos os requisitos de solicitação de consentimento e declaração em destaque aplicáveis.
  - As permissões que não são necessárias para o app de saúde executar a funcionalidade principal não precisam ser solicitadas, e as permissões que não são usadas precisam ser removidas. Para ver a lista de permissões consideradas no escopo de dados sensíveis relacionados à saúde, veja Quais permissões estão no escopo da política de apps de saúde.
  - Quando o app não é principalmente de saúde, mas tem recursos relacionados e acessa dados de saúde, ele ainda entra no escopo da política de Apps de Saúde. A relação entre a funcionalidade principal do app e a coleta de dados relacionados à saúde precisa estar clara para o usuário, por exemplo: seguradoras, apps de jogos que coletam dados de atividade do usuário para avançar etc. A Política de Privacidade do app precisa refletir esse uso limitado.
- **Funções Relacionadas a Saúde e Medicina:**
  - Não permitimos apps com funções relacionadas a saúde e medicina que sejam enganosas ou potencialmente nocivas.
  - Apps que se conectam a hardware ou dispositivos externos (por exemplo, monitores de glicemia) para realizar funções médicas precisam divulgar claramente esses requisitos de hardware externo na descrição do app. O app não pode dar a entender que funciona de maneira independente do hardware externo necessário.
  - Apps que usam os sensores do dispositivo (por exemplo, a câmera) para funções de saúde precisam divulgar claramente as informações de compatibilidade com dispositivos na descrição do app. Por exemplo, apps com funções de oximetria que usam apenas os sensores dos dispositivos precisam divulgar corretamente quais modelos são compatíveis com essas funções.
  - Os apps regulamentados porque são classificados como dispositivos médicos precisam estar declarados corretamente e com as informações necessárias conforme este artigo. Esses apps serão identificados como "Dispositivo médico" no Google Play. Quando solicitado, os apps regulamentados por serem dispositivos médicos devem apresentar os documentos oficiais de aprovação, liberação e certificação pelas autoridades relevantes. Outros aplicativos médicos e de

saúde precisam incluir uma exoneração de responsabilidade na descrição, esclarecendo que o app "não é um dispositivo médico e não faz diagnósticos, tratamentos, não cura e não previne nenhuma condição médica".

- Os apps também precisam lembrar os usuários [illegible] profissional de saúde para orientações médicas, diagnóstico ou tratamento.

Bin | 00:57:08 | Bin

- **Requisitos adicionais:**
  Se o app de saúde se enquadra em alguma das classificações a seguir, é preciso obedecer aos requisitos relevantes:
  - **Apps de Saúde Governamentais**: caso você tenha autorização do governo ou de uma organização de saúde reconhecida para desenvolver e distribuir um app em colaboração com eles, será necessário apresentar um comprovante de qualificação no Formulário de Aviso com Antecedência.
  - **Apps de Monitoramento de Contatos/Estado de Saúde**: caso o app seja de monitoramento de contatos e/ou de estado de saúde, selecione "Prevenção de doenças e saúde pública" no Play Console e envie as informações necessárias (usando o formulário de aviso com antecedência acima).
  - **Apps de Pesquisa em Seres Humanos**: os apps que fazem pesquisas em seres humanos relacionadas à saúde precisam seguir todas as regras e regulamentos, incluindo, mas não se limitando a, receber o consentimento informado dos participantes ou, no caso de menores, do responsável. Os apps de Pesquisa em Saúde também precisam receber aprovação de um Conselho de Revisão Institucional e/ou de um comitê de ética independente equivalente, a menos que sejam isentos. Um comprovante dessa aprovação precisa ser enviado mediante solicitação.

Para saber mais sobre apps de saúde e medicina, consulte as Categorias de apps de saúde e informações adicionais.

Dados do app Conexão Saúde

As informações acessadas com as permissões do app Conexão Saúde são consideradas dados pessoais e sensíveis do usuário, sujeitas à política de dados do usuário e a requisitos adicionais .

Medicamentos controlados

Não permitimos apps que facilitem a venda ou compra de medicamentos controlados sem receita médica.

Substâncias não aprovadas

O Google Play não permite apps que promovam ou vendam substâncias não aprovadas, mesmo que apresentem argumentos de legalidade.

Veja alguns exemplos de violações comuns:

- Todos os itens desta lista de exemplos de suplementos e produtos farmacêuticos proibidos
- Produtos com efedrina
- Produtos com gonadotrofina coriônica humana (hCG) destinados à perda ou ao controle de peso ou promovidos em conjunto com esteroides anabolizantes
- Suplementos herbáceos e dietéticos com componentes farmacêuticos ativos ou ingredientes perigosos
- Declarações falsas ou enganosas sobre saúde, incluindo afirmações que implicam que um produto tem a mesma eficácia de substâncias controladas ou medicamentos vendidos sob prescrição médica

- Promoção de produtos não aprovados pelo governo insinuando que eles são seguros e eficazes para a prevenção, cura ou tratamento de doenças ou problemas de saúde específicos
- Produtos sujeitos a qualquer aviso ou ação regula

Bin | 00:57:08 | Bin

- Produtos com nomes muito semelhantes a uma substância farmacêutica, suplemento ou substância controlada não aprovada

Para saber mais sobre os suplementos e produtos farmacêuticos não aprovados ou enganosos que monitoramos, acesse www.legitscript.com (em inglês).

Desinformação relacionada à saúde

Não são permitidos apps que tenham declarações enganosas relacionadas à saúde que contradigam o consenso médico atual ou possam prejudicar os usuários.

Veja alguns exemplos de violações comuns:

- Declarações enganosas sobre vacinas, como dizer que elas podem alterar o DNA de uma pessoa
- Defesa de tratamentos prejudiciais e não aprovados
- Defesa de outras práticas prejudiciais à saúde, como terapia de conversão

(1) O app faz declarações médicas ou relacionadas à saúde (cura do câncer) que são enganosas.

Pagamentos – Serviços clínicos

As transações que envolvem serviços clínicos regulamentados não devem usar o sistema de faturamento do Google Play. Para mais informações, consulte Noções básicas sobre a política de pagamentos do Google Play .

Conteúdo baseado em blockchain

Com a rápida evolução da tecnologia blockchain, pretendemos disponibilizar uma plataforma para que os desenvolvedores possam crescer com inovação e [illegible] das e imersivas aos usuários.

Bin | 00:57:08 | Bin

Para os fins desta política, a expressão "conteúdo baseado em blockchain" refere-se a ativos digitais tokenizados protegidos em um blockchain. Caso seu app tenha esse tipo de conteúdo, será preciso obedecer aos requisitos mencionados.

Corretoras de criptomoedas e carteiras de software

A compra, manutenção ou troca de criptomoedas deve ser realizada por serviços certificados em jurisdições regulamentadas.

Você precisa obedecer à regulamentação aplicável de cada região ou país segmentado pelo seu app. Além disso, evite publicar o app em locais onde seus produtos e serviços são proibidos. O Google Play pode solicitar informações ou documentos adicionais para garantir compliance com os requisitos de regulamentação ou licenciamento aplicáveis.

Para saber mais sobre os requisitos específicos ao país, consulte o artigo da Central de Ajuda.

Criptomineração

Não são permitidos apps que mineram criptomoeda nos dispositivos. Permitimos apps que gerenciam remotamente a mineração de criptomoeda.

Requisitos de transparência para distribuição de ativos digitais tokenizados

Caso seu app venda ou ofereça como prêmio ativos digitais tokenizados aos usuários, será preciso incluir essa informação no formulário de declaração de recursos financeiros na página "Conteúdo do app" no Play Console.

Ao criar um produto no app, você precisa informar que ele representa um ativo digital tokenizado na seção de detalhes. Para saber mais, confira o artigo Criar um produto no app.

Não é permitido promover nem exaltar qualquer ganho potencial proveniente de atividades de jogo ou negociação.

Requisitos adicionais para gamificação de NFTs

De acordo com a Política de jogos, concursos e jogos de azar com dinheiro real do Google Play, os apps de jogos de azar que integram ativos digitais tokenizados, como NFTs, devem concluir o processo de aplicação.

Para todos os outros apps que não atendem aos requisitos de qualificação relacionados a apps de jogos de azar e que não estão incluídos em outros pilotos de jogos com dinheiro real, nenhum valor monetário deve ser aceito em troca da chance de receber um NFT de valor desconhecido. Os NFTs comprados devem ser consumidos ou usados no jogo para aprimorar a experiência dos jogadores ou para ajudar os usuários a avançar no jogo. Não é permitido usar NFTs para apostar ou negociar a oportunidade de ganhar prêmios de valor monetário real (incluindo outros NFTs).

Veja alguns exemplos de violações comuns:

- Apps que vendem pacotes de NFTs sem divulgar o conteúdo específico e os valores dos tokens.
- Jogos sociais de cassino pagos, como caça-níqueis, que oferecem NFTs como recompensa.

Conteúdo gerado por IA

Com o maior acesso de desenvolvedores a modelos de IA generativa, é possível incorporar esses modelos nos apps para aumentar o engajamento e melhorar a experiência do usuário. O Google Play

quer garantir que o conteúdo gerado por IA seja seguro para todos os usuários e que o feedback seja incorporado para promover a inovação responsável.

Conteúdo gerado por IA

Bin | 00:57:08 | Bin

O conteúdo gerado por IA é criado por modelos de IA generativa com base em comandos de usuários. Exemplos de conteúdo gerado por IA:

- Chatbots de IA generativa de conversação de texto para texto, em que o principal recurso do app é interagir com o chatbot
- Imagens ou vídeos gerados por IA com base em comandos de texto, imagem ou voz

Para garantir a segurança dos usuários e obedecer à Cobertura da política do Google Play, os apps que geram conteúdo usando IA precisam estar em conformidade com as políticas para desenvolvedores do Google Play. Isso inclui proibir e impedir a geração de conteúdo restrito, como conteúdo que facilita a exploração ou o abuso de crianças e que permite comportamento enganoso.

Confira no artigo da Central de Ajuda recursos sobre as práticas recomendadas do setor para proteger os apps de IA generativa.

Os apps que geram conteúdo usando IA precisam oferecer recursos para que os usuários sinalizem ou denunciem aos desenvolvedores o conteúdo ofensivo sem precisar sair do app. Essas denúncias precisam ser usadas por desenvolvedores para ajustar os filtros de conteúdo e a moderação nos apps.

Propriedade intelectual

Não são permitidos apps ou contas de desenvolvedor que violam direitos de propriedade intelectual de outras pessoas (incluindo marcas registradas, direitos autorais, patentes, segredos comerciais e outros direitos de propriedade). Também são proibidos os apps que incentivam a violação de direitos de propriedade intelectual ou levam a esse tipo de infração.

Responderemos a notificações claras de suposta violação de direitos autorais. Para receber mais informações ou preencher uma solicitação da DMCA, visite nossa página de procedimentos sobre direitos autorais .

Para enviar uma reclamação sobre a venda ou promoção de produtos falsificados em um app, envie um aviso de falsificação .

Se você for proprietário de uma marca registrada e acreditar que há um app no Google Play que viole seus direitos de marca registrada, entre em contato diretamente com o desenvolvedor para resolver o problema. Se não for possível chegar a uma solução, envie uma reclamação de marca registrada por meio deste formulário .

Se você tiver documentação por escrito comprovando sua permissão para usar a propriedade intelectual de terceiros no app ou na página "Detalhes do app" (como nomes de marcas, logotipos e recursos gráficos), entre em contato com a equipe do Google Play antes do envio para garantir que o app não seja rejeitado por violação de propriedade intelectual.

Uso não autorizado de conteúdo protegido por direitos autorais

Apps que violem direitos autorais não são permitidos. Modificar conteúdo protegido por direitos autorais ainda pode ser considerado uma violação. Pode ser solicitado que os desenvolvedores forneçam evidências dos direitos deles sobre conteúdo protegido por direitos autorais.

Tenha cuidado ao usar conteúdo protegido por direitos autorais para demonstrar a funcionalidade do seu app. Em geral, a abordagem mais segura é criar algo original.

Veja alguns exemplos de violações comuns:

- Arte da capa de álbuns de música, videogames e livros

- Imagens de publicidade para filmes, programas de TV e jogos de video game.
- Pôsteres ou imagens de quadrinhos, desenhos animados, filmes, clipes musicais ou programas de TV.
- Logotipos de times profissionais ou de universidades.
- Fotos tiradas da conta de mídia social de uma figura pública.
- Imagens profissionais de figuras públicas.
- Reproduções ou "artes de fãs" indistinguíveis de uma obra original protegida por direitos autorais.
- Apps de sons que reproduzam clipes de áudio de conteúdo protegido por direitos autorais.
- Reproduções completas ou traduções de livros que não sejam de domínio público

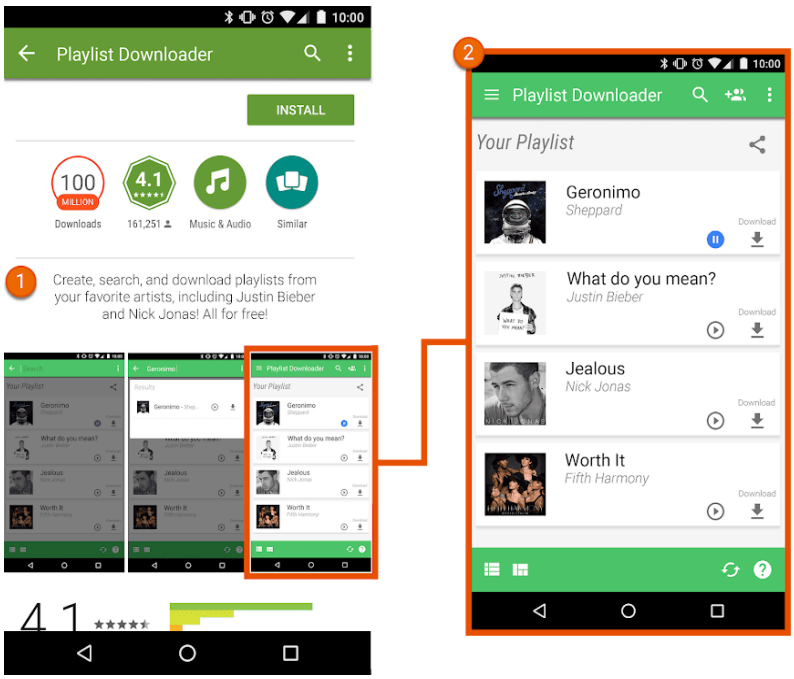
Bin | 00:57:08 | Bin

Incentivo à violação de direitos autorais

Apps que incentivem a violação de direitos autorais ou estimulem tal prática não são permitidos. Antes de publicar seu app, verifique se ele não incentiva a violação de direitos autorais de alguma forma e, se necessário, busque orientação jurídica.

Veja alguns exemplos de violações comuns:

- Apps de streaming que permitem aos usuários fazer o download de uma cópia local de conteúdo protegido por direitos autorais sem autorização
- Apps que incentivem os usuários a fazer streaming e download de obras protegidas por direitos autorais, incluindo músicas e vídeos, em violação a uma legislação de direitos autorais aplicável:



① A descrição nesta página "Detalhes do app" incentiva os usuários a fazer o download de conteúdo protegido por direitos autorais sem autorização.
② A captura de tela nesta página "Detalhes do app" incentiva os usuários a fazer o download de conteúdo protegido por direitos autorais sem autorização.

Violação de marca registrada

Apps que violem marcas registradas alheias não são permitidos. A marca registrada pode ser uma palavra, um símbolo ou uma combinação destes que identifique a origem de um produto ou serviço. Uma vez adquirida, a marca registrada oferece ao proprietário direitos exclusivos de uso da marca no que se refere a certos produtos ou serviços.

A violação de marca registrada se dá pelo uso indevido ou não autorizado de marca registrada idêntica ou semelhante de modo a confundir o usuário no que se refere à origem do produto. Se usar marcas registradas de terceiros de maneira que poss poderá ser suspenso.

Bin | 00:57:08 | Bin

Falsificação

Não permitimos apps que vendem ou promovem produtos falsificados. Esses produtos exibem marcas registradas ou logotipos idênticos ou extremamente semelhantes a outra marca registrada. Eles imitam as características da marca para tentar se passar por produtos originais do proprietário.

Privacidade, fraude e uso indevido de dispositivos

Estamos comprometidos em proteger a privacidade dos usuários e oferecer um ambiente seguro para eles. Apps maliciosos que abusam ou fazem uso indevido de redes, dispositivos ou dados pessoais são expressamente proibidos.

Dados do usuário

Você precisa ser transparente sobre como lida com os dados do usuário (por exemplo, dados coletados do usuário ou sobre ele, incluindo informações do dispositivo). Isso significa divulgar o acesso, a coleta, o uso, o tratamento e o compartilhamento dos dados do usuário do seu app e limitar o uso dos dados às finalidades divulgadas em conformidade com a política. Qualquer tratamento de dados pessoais e sensíveis do usuário também está sujeito aos requisitos adicionais da seção "Dados pessoais e sensíveis do usuário" abaixo. Além disso, e de seguir as outras Políticas do programa para desenvolvedores, sempre obedeça às leis aplicáveis de proteção e privacidade de dados nas jurisdições onde você oferece seus produtos ou serviços. Por exemplo, se você oferece seus serviços para usuários na União Europeia, confira as diretrizes sobre práticas recomendadas para proteção de dados pessoais (em inglês e francês) no ambiente de dispositivos móveis, adotadas pela autoridade de proteção de dados da França (CNIL).

Se você inclui código de terceiros, como um SDK, no seu app, é necessário garantir que o código usado e as práticas do terceiro em relação aos dados do usuário do app obedeçam às Políticas do programa para desenvolvedores do Google Play, incluindo os requisitos de uso e divulgação. Por exemplo, você precisa garantir que os fornecedores de SDK não vendam os dados pessoais e sensíveis dos usuários do app. Esse requisito se aplica mesmo se a transferência dos dados do usuário for após o envio ao servidor ou ao incorporar código de terceiros no app.

Dados pessoais e sensíveis do usuário

Os dados pessoais e sensíveis de usuários incluem, entre outros, informações de identificação pessoal, financeiras e de pagamento; dados de autenticação; agenda; contatos; localização do dispositivo ; dados de SMS e chamadas; dados de saúde ; dados do Conexão Saúde ; inventário de outros apps no dispositivo; conteúdo do microfone e da câmera; e outros dados sensíveis de uso ou do dispositivo. Caso seu app lide com dados pessoais e sensíveis de usuários, você precisa fazer o seguinte:

- Limite o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis coletados pelo app à funcionalidade do app e do serviço e às finalidades que estão em conformidade com a política e atendem às expectativas do usuário.
  - Os apps que estendem o uso de dados pessoais e sensíveis do usuário para veiculação de anúncios precisam obedecer à política de anúncios do Google Play.
  - Você também pode transferir dados necessários para provedores de serviços ou por motivos legais, como obedecer a uma solicitação governamental válida, à legislação aplicável ou como parte de uma fusão ou aquisição com o aviso legalmente adequado aos usuários.

- Lide com todos os dados pessoais ou sensíveis de usuários de maneira segura, incluindo a transmissão desses dados com criptografia moderna, como HTTPS.
- Use uma solicitação de permissões de execução s[illegible]de acessar os dados controlados por permissões do Android .
- Não venda dados pessoais e sensíveis do usuário.
  - "Venda" significa a troca ou transferência de dados sensíveis e pessoais do usuário para um terceiro por compensação monetária.
    - A transferência de dados pessoais e sensíveis iniciada pelo usuário (por exemplo, quando o usuário está usando um recurso do app para transferir um arquivo a um terceiro ou quando o usuário escolhe usar um app de pesquisa de finalidade dedicada) não é considerada como venda.

Bin | 00:57:08 | Bin

Requisito de consentimento e divulgação em destaque

Quando o app acessar, coletar, usar ou compartilhar dados pessoais e sensíveis do usuário de maneira que não corresponda às expectativas do usuário do produto ou recurso em questão (por exemplo, se a coleta de dados ocorrer em segundo plano quando o usuário não está interagindo com o app), você precisa atender aos seguintes requisitos:

Divulgação em destaque: é necessário fornecer uma divulgação no app a respeito da coleta, do uso e do compartilhamento de dados. Essa divulgação:

- precisa estar dentro do próprio app, não somente na descrição dele ou em um site;
- precisa ser exibida no uso normal do app e não pode exigir que o usuário navegue até um menu ou até as configurações;
- precisa descrever os dados que são acessados ou coletados;
- precisa explicar como os dados serão usados e/ou compartilhados;
- não pode ser colocada somente na Política de Privacidade ou nos Termos de Serviço;
- não pode ser incluída em outras divulgações não relacionadas à coleta de dados pessoais e sensíveis de usuários.

Consentimento e permissões de execução: as solicitações de consentimento do usuário no app e de permissões de execução precisam ser imediatamente precedidas por uma divulgação no app que atende aos requisitos dessa política. Essa solicitação:

- precisa apresentar a caixa de diálogo de consentimento de uma maneira clara e inequívoca;
- precisa exigir do usuário uma ação de confirmação, como um toque para aceitar ou a marcação de uma caixa de seleção;
- não pode interpretar como consentimento o ato de fechar a divulgação e ir para outra tela (por exemplo, tocar na tela para sair ou pressionar os botões home ou "Voltar");
- não pode usar mensagens que expiram ou são dispensadas automaticamente como modo de receber o consentimento do usuário; e
- precisa ser concedida pelo usuário antes do app começar a coletar ou acessar os dados pessoais e sensíveis do usuário.

Os apps que contam com outros fundamentos jurídicos para tratar dados pessoais e sensíveis do usuário sem consentimento, como um interesse legítimo de acordo com o GDPR da UE, precisam obedecer a todos os requisitos legais aplicáveis e ter divulgações apropriadas aos usuários, incluindo no app, conforme exigido pela política.

Para atender aos requisitos da política, recomendamos que você use o modelo de divulgação em destaque a seguir quando necessário:

- "[O app] coleta/transmite/sincroniza/armazena [tipo de dados] para ativar ["recurso"], [em qual contexto]."
- *Exemplo: "O Fitness Funds coleta dados de local para ativar o monitoramento de atividades físicas, mesmo quando o app está fechado ou não está em uso, e para veicular publicidade."*

- *Exemplo: "O Call Buddy coleta dados de registro de chamadas de leitura e gravação para ativar o gerenciamento de contatos, mesmo quando o app não está em uso."*

Se o app integrar código de terceiro, como, por exem[illegible]ar dados pessoais e sensíveis do usuário por padrão, você precisa, até duas semanas após receber uma solicitação do Google Play (ou, se o pedido do Google Play oferecer um prazo mais longo, dentro desse período), oferecer evidência suficiente mostrando que o app obedece à solicitação de consentimento e declaração em destaque da política, incluindo em relação ao acesso, à coleta, ao uso ou ao compartilhamento de dados por código de terceiro.

Bin | 00:57:08 | Bin

Veja alguns exemplos de violações comuns:

- Um app que coleta a localização do dispositivo, mas não tem uma divulgação em destaque que explique qual recurso usa esses dados e/ou que indique o uso do app em segundo plano
- Um app com uma permissão de execução que solicita acesso aos dados antes de exibir a divulgação em destaque especificando para que as informações são usadas
- Um app que acessa o inventário de apps instalados do usuário e não trata essas informações como dados pessoais ou sensíveis sujeitos aos requisitos da Política de Privacidade, de tratamento de dados e de solicitação de consentimento e declaração em destaque
- Um app que acessa os dados do smartphone ou dos contatos de um usuário e não os trata como informações pessoais ou sensíveis sujeitas aos requisitos da Política de Privacidade, de tratamento de dados e de solicitação de consentimento e declaração em destaque
- Um app que registra a tela do usuário e não trata as informações como dados pessoais ou sensíveis sujeitos a essa política
- Um app que coleta a localização do dispositivo e não divulga de maneira detalhada o uso desses dados nem obtém o consentimento de acordo com os requisitos acima
- Um app que usa permissões restritas em segundo plano, inclusive para fins de rastreamento, pesquisa ou marketing, e não divulga de forma abrangente esse uso nem obtém consentimento de acordo com os requisitos acima
- Um app com um SDK que coleta informações pessoais e sensíveis do usuário e não as trata como sujeitas aos requisitos da política de dados do usuário, de acesso, de tratamento de dados (incluindo a proibição de venda) e de solicitação de consentimento e declaração em destaque

Consulte este artigo para saber mais sobre a solicitação de consentimento e declaração em destaque.

Restrições de acesso a dados pessoais e sensíveis

Além dos requisitos acima, a tabela abaixo descreve as obrigações para atividades específicas.

Atividade	Requisito
O app lida com informações financeiras, de pagamento ou números de documentos de identidade.	O app jamais poderá divulgar dados pessoais e sensíveis do usuário relacionados a atividades financeiras ou de pagamento, assim como números de documentos de identidade.
O app lida com dados privados de agenda ou de contatos.	Não permitimos a publicação ou divulgação não autorizada de contatos privados de pessoas.
O app tem funcionalidade de segurança ou antivírus, como antimalware ou recursos relacionados a proteção.	Será necessário postar uma Política de Privacidade que, assim como outras divulgações no app, explique os dados do usuário que o app coleta e transmite, como eles são usados e com quem são compartilhados.
O público-alvo do seu app inclui crianças.	Seu app não pode incluir um SDK que não foi aprovado para uso em serviços feitos para crianças. Acesse Como criar apps para crianças e famílias para ver a linguagem e os requisitos completos da política.
Seu app coleta ou vincula identificadores de dispositivo persistentes (por exemplo, IMEI, IMSI, número de série do chip etc.).	Identificadores de dispositivo persistentes não podem ser vinculados a outros dados pessoais e sensíveis de usuários ou identificadores de dispositivo reconfiguráveis, exceto em casos de

	• telefonia vinculada a uma identidade do chip (por exemplo, chamada de Wi-Fi vinculada à conta da operadora); • apps de gerenciamento de dispositivos corporativos que usam o modo p Bin | 00:57:08 | Bin Esses usos precisam ser divulgados com destaque aos usuários, conforme especificado na política de Dados do usuário . Consulte este recurso para identificadores únicos alternativos. Acesse a política de Anúncios para ver diretrizes adicionais sobre o ID de publicidade do Android.

Seção "Segurança dos dados"

Todos os desenvolvedores precisam ter uma seção de segurança de dados clara e precisa em cada app, detalhando a coleta, o uso e o compartilhamento de dados do usuário. O desenvolvedor é responsável pela precisão do marcador e por manter as informações atualizadas. Quando relevante, essa seção precisa ser consistente com as divulgações feitas na Política de Privacidade do app.

Consulte este artigo para ver mais informações sobre como preencher a seção "Segurança dos dados".

Política de Privacidade

Todos os apps precisam incluir um link para a Política de Privacidade no campo designado no Play Console e outro link ou texto da política no próprio app. A Política de Privacidade e as declarações no app precisam descrever de maneira detalhada como o app acessa, coleta, usa e compartilha os dados do usuário, sem se limitar aos dados divulgados na seção "Segurança dos dados". Isso precisa incluir:

- informações sobre o desenvolvedor e um ponto de contato de privacidade ou mecanismo para o envio de consultas;
- a divulgação dos tipos de dados pessoais e sensíveis dos usuários que o app acessa, coleta, usa e compartilha, além de qualquer grupo com que esses dados são compartilhados;
- procedimentos seguros de tratamento de dados pessoais e sensíveis do usuário;
- a política de retenção e exclusão de dados do desenvolvedor;
- uma indicação clara do tipo de política (por exemplo, colocar "Política de Privacidade" no título).

A entidade (por exemplo, o desenvolvedor ou a empresa) indicada na página "Detalhes do app" da Google Play Store ou o nome do app precisa aparecer na Política de Privacidade. Apps que não acessam dados pessoais e sensíveis de usuários também precisam enviar uma Política de Privacidade.

Sua política precisa estar disponível de forma não editável em um URL ativo, publicamente acessível e sem fronteira geográfica virtual. Não use PDFs.

Requisito de exclusão de contas

Se o app permite que os usuários criem uma conta, também precisa permitir que eles solicitem a exclusão dela. Os usuários precisam ter uma opção facilmente identificável para iniciar a exclusão da conta de dentro do app ou fora dele, por exemplo, acessando seu site. É necessário inserir um link para esse recurso da Web no campo de formulário de URL designado no Play Console.

Ao excluir uma conta do app com base na solicitação de um usuário, também é preciso excluir os dados do usuário associados a essa conta. O "congelamento" ou a desativação temporária da conta não se qualifica como exclusão. Se for necessário reter determinados dados por motivos legítimos, como segurança, prevenção de fraudes ou compliance regulatória, você precisará informar claramente aos usuários sobre suas práticas de retenção de dados (por exemplo, na sua Política de Privacidade).

Para saber mais sobre os requisitos da política de exclusão de contas, consulte o artigo da Central de Ajuda. Para mais informações sobre como atualizar seu formulário de Segurança dos dados, consulte

este artigo.

Uso do ID definido pelo app

Bin | 00:57:08 | Bin

O Android apresentará um novo ID para oferecer compatibilidade com casos de uso essenciais, como análise e prevenção de fraudes. Os termos para o uso desse ID estão disponíveis abaixo.

- **Uso**: o ID definido pelo app não pode ser usado para personalização e avaliação de anúncios.
- **Associação com informações de identificação pessoal ou outros identificadores**: o ID do conjunto de apps não pode ser conectado a outros identificadores do Android (por exemplo, AAID) ou a dados pessoais e sensíveis para fins publicitários.
- **Transparência e consentimento**: a coleta e o uso do ID definido pelo app e o compromisso com estes termos precisam ser divulgados aos usuários em uma notificação de privacidade legalmente adequada, incluindo na sua Política de Privacidade. É necessário receber o consentimento legalmente válido dos usuários quando necessário. Para saber mais sobre nossos padrões de privacidade, consulte a política de Dados do usuário .

Estruturas de Privacidade de Dados UE-EUA, Reino Unido-EUA e Suíça-EUA

Se você acessar, usar ou processar informações pessoais disponibilizadas pelo Google que identificarem direta ou indiretamente um indivíduo e tiverem origem no Espaço Econômico Europeu, no Reino Unido ou na Suíça, ("Informações pessoais da UE"), será preciso:

- agir em conformidade com todos os regulamentos, legislações, regras e diretrizes referentes à privacidade, segurança e proteção de dados;
- acessar, usar ou processar as informações pessoais da UE somente para fins compatíveis com o consentimento recebido do indivíduo relacionado a esses dados;
- implementar medidas técnicas e organizacionais adequadas para proteger as Informações pessoais da UE contra perda e uso indevido, assim como divulgação, alteração, destruição ou acesso não autorizados ou ilegais;
- fornecer o nível de proteção exigido pelos Princípios da Estrutura de Privacidade de Dados ou pelo mecanismo de transferência aplicável, conforme descrito nos Termos de Proteção de Dados entre Controladores do Google (links em inglês).

Monitore a conformidade com essas condições regularmente. Se em algum momento você não atender a essas condições ou se houver uma grande possibilidade de isso acontecer, notifique nossa equipe imediatamente enviando um e-mail para data-protection-office@google.com . Além disso, interrompa o tratamento de informações pessoais da UE ou tome medidas razoáveis e apropriadas para restabelecer um nível adequado de proteção.

Permissões e APIs que acessam informações sensíveis

As solicitações de permissões e de APIs que acessam informações sensíveis precisam fazer sentido para os usuários. O app só pode solicitar permissões e APIs que acessam informações sensíveis necessárias para implementar recursos ou serviços atuais promovidos na página "Detalhes do app". Não use permissões ou APIs que acessam informações sensíveis com acesso a dados do usuário ou do dispositivo para finalidades ou recursos não revelados, não implementados ou não permitidos. Dados pessoais ou sensíveis acessados por permissões ou APIs que acessam informações sensíveis não podem ser vendidos nem compartilhados com a finalidade de facilitar uma venda.

Solicite permissões e APIs que acessam informações sensíveis para acessar dados de acordo com o contexto (via solicitações incrementais). Isso ajuda os usuários a entender por que a permissão é necessária. Use os dados somente para as finalidades consentidas pelo usuário. Posteriormente, se você quiser usar os dados para outros fins, será necessário pedir permissão aos usuários e receber a confirmação deles para os usos adicionais.

Permissões restritas

Além do indicado acima, as permissões restritas são aquelas designadas como perigosas, especiais, de assinatura ou conforme documentado aba[illegible] guintes requisitos e restrições adicionais:

Bin | 00:57:08 | Bin

- Os dados do dispositivo ou do usuário acessados por permissões restritas são considerados dados pessoais e sensíveis do usuário. Os requisitos da política de dados do usuário se aplicam.
- Respeite a decisão dos usuários se eles recusarem uma solicitação de permissão restrita. Eles não podem ser manipulados nem forçados a consentir com permissões que não sejam essenciais. Faça o possível para atender os usuários que não concedem acesso a permissões sensíveis. Por exemplo, você pode permitir que o usuário insira manualmente um número de telefone, caso ele tenha restringido o acesso aos registros de chamadas.
- É expressamente proibido usar permissões que violam as políticas de malware do Google Play, o que inclui o abuso de privilégios elevados.

Algumas permissões restritas podem estar sujeitas a requisitos adicionais, conforme detalhado abaixo. O objetivo dessas restrições é proteger a privacidade do usuário. Podemos fazer exceções limitadas aos requisitos abaixo em casos muito raros em que os apps fornecem um recurso de alto interesse ou essencial ao usuário sem que haja algum método alternativo disponível para isso. Avaliamos as exceções propostas em relação aos possíveis efeitos sobre a privacidade ou segurança dos usuários.

Permissões restritas com alternativas de escopo mínimo

Os seletores de sistema e alternativas como o Sharesheet ajudam os desenvolvedores a priorizar a privacidade. Fotos, Vídeos, Contatos e outros dados pessoais e sensíveis protegidos por permissões restritas devem ser tratados com as práticas recomendadas de privacidade. O app só deve solicitar e usar as permissões sensíveis abaixo se as alternativas de escopo mínimo não forem suficientes para oferecer a funcionalidade principal. Saiba mais na Central de Ajuda.

Permissões de acesso a fotos e vídeos

Todas as Fotos do usuário são dados pessoais e sensíveis sujeitos à política de Dados do Usuário.

Os apps destinados ao Android 13 ou versões mais recentes (nível 33 da API ou superior) só podem solicitar as permissões `READ_MEDIA_IMAGES` e `READ_MEDIA_VIDEO` se os seletores de sistema (como o Seletor de Fotos do Android) não forem suficientes para fornecer a funcionalidade principal do app. Os apps que ainda solicitam as permissões `READ_MEDIA_IMAGES` e `READ_MEDIA_VIDEO` precisam enviar uma declaração no Play Console para demonstrar a necessidade de acesso às Fotos e por que o Seletor de Fotos do Android (ou alternativas) não é suficiente.

Permissões de SMS e registro de chamadas

As permissões de SMS e registro de chamadas são consideradas dados pessoais e sensíveis de usuários sujeitos à política de Informações pessoais e sensíveis e às seguintes restrições:

Permissão restrita	Requisito
Grupo de permissões "Registro de chamadas". Por exemplo, READ_CALL_LOG, WRITE_CALL_LOG, PROCESS_OUTGOING_CALLS	Ele precisa estar registrado ativamente como gerenciador padrão de "Telefone" ou "Assistente" no dispositivo.
Grupo de permissões "SMS". Por exemplo, READ_SMS, SEND_SMS, WRITE_SMS, RECEIVE_SMS, RECEIVE_WAP_PUSH, RECEIVE_MMS	Ele precisa estar registrado ativamente como gerenciador padrão de "SMS" ou "Assistente" no dispositivo.

Apps sem o recurso de gerenciador padrão de "SMS", "Telefone" ou "Assistente" não podem declarar o uso das permissões acima no manifesto. Isso inclu[illegible] manifesto. Os apps também precisam estar ativamente registrados como [illegible]S", do "Telefone" ou do "Assistente" antes de solicitar que os usuários aceitem uma das permissões acima. Além disso, eles precisarão interromper imediatamente o uso da permissão quando não forem mais o gerenciador padrão. Os usos permitidos e exceções estão disponíveis nesta página da Central de Ajuda .

Os apps só podem usar a permissão e os dados derivados dela para fornecer a funcionalidade principal aprovada do app, que corresponde ao propósito principal dele. Isso pode incluir um conjunto de recursos principais que precisam ser documentados e promovidos com maior destaque na descrição do app. Sem os recursos principais, o app ficará "corrompido" ou não poderá ser usado. A transferência, o compartilhamento ou o uso licenciado desses dados só pode ocorrer para fornecer os recursos principais ou serviços dentro do app. Além disso, o uso dessas informações não pode ser estendido para outras finalidades (por exemplo, melhorar outros apps e serviços ou para fins de marketing e publicidade). Não é permitido usar métodos alternativos (incluindo outras permissões, APIs ou fontes de terceiros) para extrair dados atribuídos às permissões de registro de chamadas ou SMS.

Permissões de localização

A localização do dispositivo é considerada um dado pessoal e sensíveis do usuário, sujeita às políticas de Informações pessoais e sensíveis e Localização em segundo plano e aos seguintes requisitos:

- Os apps não podem acessar dados protegidos por permissões de localização (por exemplo, `ACCESS_FINE_LOCATION`, `ACCESS_COARSE_LOCATION`, `ACCESS_BACKGROUND_LOCATION`) que não sejam mais necessários para fornecer os recursos ou serviços atuais.
- Nunca solicite permissões de localização do usuário somente para fins de publicidade ou análise. Os apps que aproveitam o uso permitido desses dados para exibir publicidade precisam estar em conformidade com nossa política de Anúncios .
- Os apps precisam solicitar o escopo mínimo necessário (ou seja, localização aproximada em vez de exata e em primeiro plano em vez de segundo plano) para fornecer o recurso ou serviço atual que exige a localização. Além disso, os usuários devem esperar que o recurso ou serviço precise acessar o nível de localização solicitado. Por exemplo, podemos recusar apps que solicitam ou acessam o local em segundo plano sem uma justificativa convincente.
- A localização em segundo plano só pode ser usada para oferecer recursos úteis aos usuários e relevantes para a funcionalidade principal do app.

Os apps terão permissão para acessar a localização com o serviço em primeiro plano (quando o app só tem acesso em primeiro plano, por exemplo, "durante o uso") se o uso:

- tiver sido iniciado para dar continuidade a uma ação do usuário no app; e
- for finalizado imediatamente após o app concluir o caso de uso pretendido pelo usuário.

Os apps desenvolvidos especificamente para crianças precisam estar em conformidade com a política do Feito para Família .

Para saber mais sobre os requisitos da política, confira este artigo de ajuda .

Permissão de acesso a todos os arquivos

Os arquivos e atributos de diretório no dispositivo de um usuário são considerados dados pessoais e sensíveis dele e estão sujeitos à política de informações pessoais e sensíveis e aos seguintes requisitos:

- Os apps só podem solicitar acesso ao armazenamento dos dispositivos que seja fundamental para o funcionamento. Eles não podem fazer isso em nome de terceiros para fins não relacionados à funcionalidade principal do app para o usuário.
- Os dispositivos Android com a versão R ou mais re[illegible]o `MANAGE_EXTERNAL_STORAGE` para gerenciar o acesso no armazenamento compartilhado. Todos os apps direcionados ao R que solicitam acesso amplo ao armazenamento compartilhado ("Acesso a todos os arquivos") precisam passar por uma análise de acesso apropriada antes da publicação. Os apps que podem usar essa permissão precisam solicitar claramente que os usuários ativem a opção "Acesso a todos os arquivos" nas configurações de "Acesso especial ao app". Para saber mais sobre os requisitos do R, confira este artigo de ajuda .

Bin | 00:57:08 | Bin

Permissão de visibilidade do pacote (app)

Os inventários dos apps instalados consultados em um dispositivo são considerados dados pessoais e confidenciais, sujeitos à política de Informações pessoais e confidenciais e aos seguintes requisitos:

Os apps que têm a finalidade principal de lançar, pesquisar ou interoperar com outros apps podem ter visibilidade do escopo apropriado para outros apps instalados no dispositivo, conforme descrito abaixo:

- **Ampla visibilidade do app**: é a capacidade de um app de ter uma visibilidade extensa (ou "ampla") dos apps instalados ("pacotes") em um dispositivo.
  - Para apps segmentados pelo menos para o nível 30 da API , a visibilidade ampla para aplicativos instalados com a permissão `QUERY_ALL_PACKAGES` é restrita a casos de uso específicos em que o reconhecimento e/ou interoperabilidade com qualquer um ou todos os apps no dispositivo são necessários para que ele funcione.
    - Não será possível usar `QUERY_ALL_PACKAGES` se o app puder operar com uma declaração de visibilidade do pacote com escopo mais direcionado . Por exemplo, consultar e interagir com pacotes específicos em vez de solicitar uma visibilidade ampla.
  - O uso de métodos alternativos para aproximar o nível de visibilidade ampla associado à permissão `QUERY_ALL_PACKAGES` também está restrito à funcionalidade principal do app voltada ao usuário e à interoperabilidade com todos os apps descobertos por esse método.
  - Consulte este artigo da Central de Ajuda e veja os casos autorizados para o uso da permissão `QUERY_ALL_PACKAGES`.
- **Visibilidade limitada do app**: quando um app minimiza o acesso aos dados, ele consulta o acesso a apps específicos usando métodos mais direcionados (em vez de "amplos"). Por exemplo, consultar apps específicos que atendam à declaração do manifesto do app. É possível usar esse método para consultas nos casos em que o app tenha interoperabilidade que obedece à política ou gerenciamento desses apps.
- A visibilidade do inventário de apps instalados em um dispositivo precisa estar diretamente relacionada à finalidade ou funcionalidade principal que os usuários acessam no app.

Os dados de inventário de apps consultados naqueles distribuídos no Google Play nunca poderão ser vendidos nem compartilhados para análise ou monetização de anúncios.

API de acessibilidade

A API Accessibility não pode ser usada para:

- mudar as configurações do usuário sem a permissão dele nem impedir que ele desative ou desinstale nenhum app ou serviço, a menos que isso seja autorizado por familiares ou responsáveis com um app de controles da família ou por administradores autorizados com um software de gerenciamento empresarial;
- contornar as notificações e os controles de segurança e privacidade integrados do Android;
- mudar ou usar a interface do usuário de maneira enganosa ou que viole as políticas para desenvolvedores do Google Play.

A API Accessibility não foi projetada e não pode ser solicitada para:

- gravação de áudio de chamadas remotas;
- um app que inicia, planeja e executa ações ou dec

Bin | 00:57:08 | Bin

O uso da API Accessibility precisa ser documentado na página de detalhes do Google Play.

Diretrizes para IsAccessibilityTool

Os apps com funcionalidades principais destinadas a oferecer apoio direto às pessoas com deficiências estão qualificados para usar o **IsAccessibilityTool** e, assim, se autodesignar publicamente como um app de acessibilidade.

Os apps sem qualificação para usar o **IsAccessibilityTool** não podem incorporar a flag e precisam atender aos requisitos de consentimento e declaração em destaque conforme descrito na política de Dados do usuário já que o recurso relacionado à acessibilidade não é óbvio para o usuário.

Quando possível, os apps precisam usar APIs e permissões com escopos mais limitados em vez da API Accessibility para alcançar a funcionalidade desejada.

Consulte o artigo da Central de Ajuda API AccessibilityService para mais informações sobre o uso proibido e orientações de como usar o IsAccessibilityTool.

Permissão "solicitar pacotes de instalação"

Com a permissão `REQUEST_INSTALL_PACKAGES`, um app pode solicitar a instalação de pacotes de apps. Para usar essa permissão, a funcionalidade principal do app precisa incluir as seguintes funções:

- Envio ou recebimento de pacotes de apps; e
- Instalação de pacotes de apps iniciada pelo usuário

As funcionalidades permitidas incluem as seguintes opções:

- Pesquisa ou navegação na Web
- Serviços de comunicação compatíveis com anexos
- Compartilhamento, transferência ou gerenciamento de arquivos
- Gerenciamento de dispositivos corporativos
- Backup e restauração
- Migração do dispositivo/transferência do smartphone
- App complementar para sincronizar o smartphone com um wearable ou dispositivo de IoT, como um smartwatch ou uma smart TV

A funcionalidade principal é definida como o objetivo principal do app. Essa função e todos os recursos essenciais que a compõem precisam ser documentados e promovidos com destaque na descrição do app.

A permissão `REQUEST_INSTALL_PACKAGES` não pode ser usada para autoatualizações, modificações ou criação de pacotes de outros APKs no arquivo de recursos, a menos que seja para fins de gerenciamento de dispositivos. Todas as atualizações ou instalação de pacotes precisam obedecer à política contra Abuso de dispositivos e de rede do Google Play e serem iniciadas e conduzidas pelo usuário.

Permissões de sensor corporal

Os dados dos sensores que medem parâmetros de saúde, como frequência cardíaca, SpO_2 e temperatura da pele, são considerados pessoais ou sensíveis do usuário. Apps que solicitam acesso

estão sujeitos aos requisitos descritos na política de dados do usuário e na política de apps de saúde. Isso se aplica a pedidos para permissões android.permission.BODY_SENSORS e android.permission.BODY_SENSORS_BACKGROUND smartphones, tablets e dispositivos Wear OS.

Bin | 00:57:08 | Bin

A partir do Android 16, a permissão ampla BODY_SENSORS está sendo alterada para permissões android.permissions.health.* que são mais granulares e preservam a privacidade para tipos específicos de dados, como android.permission.health.READ_HEART_RATE, android.permission.health.READ_OXYGEN_SATURATION, android.permission.health.READ_SKIN_TEMPERATURE.

Apps destinados ao Android 16 ou versões mais recentes devem usar essas permissões específicas para APIs que precisavam de BODY_SENSORS. Confira a página Mudanças de comportamento: apps destinados ao Android 16 ou versões mais recentes para mais detalhes.

Todos os pedidos para permissões de sensor corporal, tanto as permissões legado quanto as granulares, serão analisados para garantir que o uso dos dados pessoais e sensíveis esteja de acordo com os casos aprovados que beneficiam diretamente os usuários. Os casos aprovados envolvem primeiramente recursos para acompanhamento de atividades físicas e bem-estar (como monitoramento de treinos em tempo real), monitoramento de condições médicas e de saúde ou pesquisas em saúde (com as devidas aprovações), além da melhoria de recursos em app complementar para dispositivos wearables.

Consulte o guia completo das políticas, que inclui os usos proibidos, casos de uso aceitável, requisitos detalhados, na página Permissões do Android Health: orientações e perguntas frequentes .

Permissões do Conexão Saúde no Android

O Conexão Saúde é uma plataforma Android criada para que apps de saúde e fitness armazenem e compartilhem os mesmos dados no dispositivo, em um ecossistema unificado. Ela também oferece um local único para os usuários controlarem quais aplicativos podem ler e gravar esses dados, inclusive Históricos de Saúde. Históricos de saúde podem incluir histórico médico, diagnósticos, tratamentos, medicações, exames laboratoriais e outros dados clínicos obtidos de prestadores de cuidados de saúde ou em plataformas terceirizadas compatíveis.

O app Conexão Saúde é compatível com leitura e gravação de vários tipos de dados , de passos e temperatura corporal a dados de Históricos de Saúde.

As informações acessadas com as permissões da plataforma são consideradas dados pessoais e sensíveis do usuário. Elas estão sujeitas à política de dados do usuário. Caso seu app seja qualificado como um app de saúde ou tenha funcionalidades relacionadas à saúde e acesse dados dessa natureza, como os do app Conexão Saúde, ele precisará obedecer à política de apps de saúde.

Consulte este guia para desenvolvedores Android sobre como começar a usar o app Conexão Saúde. Para solicitar acesso aos tipos de dados do app Conexão Saúde e tirar outras dúvidas, confira as Permissões do Android Health: orientações e perguntas frequentes.

Os apps distribuídos pelo Google Play precisam atender aos requisitos da política a seguir para ler e/ou gravar dados no app Conexão Saúde.

Acesso e uso adequados do Conexão Saúde

O app Conexão Saúde só pode ser usado de acordo com as políticas, termos e condições aplicáveis para casos de uso aprovados, conforme estabelecido nesta política. Portanto, apenas os apps ou serviços que atendam a um dos casos de uso aprovados podem pedir acesso às permissões.

Os casos de uso aprovados incluem: condicionamento físico e bem-estar, recompensas, coaching de condicionamento físico, bem-estar corporativo, cuidados médicos, pesquisa em saúde e jogos. Os aplicativos com acesso para esses casos de uso não podem estender seu uso a fins não divulgados ou não permitidos.

Somente aplicativos ou serviços com um ou mais recursos projetados para beneficiar a saúde e o condicionamento físico dos usuários podem pedir acesso às permissões do Conexão Saúde. Eles incluem:

Bin | 00:57:08 | Bin

- Aplicativos ou serviços que permitem aos usuários **registrar, gerar relatórios, monitorar e/ou analisar diretamente** informações sobre atividades físicas, sono, bem-estar mental, nutrição, parâmetros de saúde, descrições físicas, históricos de saúde e/ou outros dados e medições relacionados a saúde ou condicionamento físico.
- Aplicativos ou serviços que permitem aos usuários **armazenar informações sobre atividades físicas, sono, bem-estar mental, nutrição, parâmetros de saúde, descrições físicas**, **históricos de saúde** e/ou outros dados e medições relacionados a saúde ou condicionamento físico no aparelho e compartilhar com outros apps no dispositivo que atendam a esses casos de uso.
- Aplicativos ou serviços que permitem o gerenciamento de condições crônicas, tratamentos médicos ou suporte a cuidados médicos.

O acesso ao app Conexão Saúde não pode ser usado para violar esta política ou quaisquer outros termos, condições ou políticas aplicáveis da plataforma, inclusive para as seguintes finalidades:

- Não use o app Conexão Saúde para desenvolver nem integrar outro app, ambiente ou atividade em que seu uso ou falha possa levar à morte, lesões corporais, danos a indivíduos ou ambientais/patrimoniais, como a criação ou operação de instalações nucleares, controle de tráfego aéreo, sistemas de suporte à vida ou armamentos.
- Não acesse dados coletados pelo app Conexão Saúde usando aplicativos headless. Os apps precisam exibir um ícone claramente identificável na bandeja, nas configurações do app no dispositivo, nos ícones de notificação etc.
- Não use o app Conexão Saúde com aplicativos que sincronizam dados entre dispositivos ou plataformas incompatíveis.
- Não use o app Conexão Saúde para se conectar a aplicativos, serviços ou recursos direcionados exclusivamente a crianças.
- Tome medidas razoáveis e apropriadas para que todos os aplicativos ou sistemas que usam o app Conexão Saúde sejam protegidos contra acesso, uso, destruição, perda, mudança ou divulgação não autorizados ou ilegais.

Também é sua responsabilidade garantir a conformidade com requisitos regulamentares ou legais aplicáveis com base no uso pretendido do app Conexão Saúde e dos dados dessa plataforma. Por exemplo, se você é uma entidade coberta pela Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA) ou um parceiro comercial sujeito a essa lei, é obrigatório obedecer aos requisitos aplicáveis ao acessar e ao usar as informações do app Conexão Saúde. Se você é um desenvolvedor sujeito ao Regulamento geral de proteção de dados (GDPR) para usuários da União Europeia, do mesmo modo, você precisa obedecer aos requisitos do GDPR. Essas leis e regulamentações podem exigir que você firme contratos adicionais, como um Contrato de parceria comercial (BAA) ou um Contrato de tratamento de dados, com entidades relevantes envolvidas nas suas atividades de tratamento antes de compartilhar dados. Também é responsabilidade do desenvolvedor de apps determinar se as suas atividades exigem tais contratos. Os desenvolvedores precisam apresentar ao Google, mediante solicitação, evidências de conformidade ou de tais contratos.

Exceto conforme expressamente indicado na embalagem ou nas informações fornecidas pelo Google referentes a produtos ou serviços específicos, o Google não endossa o uso nem garante a precisão dos dados do app Conexão Saúde para qualquer caso ou finalidade, principalmente para uso médico, de pesquisa ou de saúde. O Google se isenta de qualquer responsabilidade associada ao uso de dados coletados no app Conexão Saúde.

Uso limitado

Ao usar o app Conexão Saúde, o acesso e uso dos dados devem obedecer a limitações específicas:

- O uso de dados deve ser limitado ao fornecimento ou melhoria do caso de uso apropriado ou dos recursos visíveis na interface do usuário do aplicativo.
- Os dados do usuário só podem ser transferidos a t[illegible] o explícito do usuário, para fins de segurança (por exemplo, inve[illegible]edecer às leis ou regulamentações aplicáveis, ou como parte de fusões/aquisições.
- O acesso humano aos dados do usuário é restrito, a menos que haja consentimento explícito do usuário, para fins de segurança, para obedecer às leis ou quando agregados para operações internas de acordo com requisitos legais.
- **Todas as outras transferências, usos ou vendas de dados do app Conexão Saúde são proibidos, incluindo o seguinte:**
  - Transferir ou vender dados do usuário para terceiros, como plataformas de publicidade, corretores de dados ou revendedores de informações.
  - Transferir, vender ou usar dados do usuário para veicular anúncios, incluindo publicidade personalizada ou baseada em interesses.
  - Transferir, vender ou usar dados do usuário para determinar classificações de crédito ou para finalidades de empréstimo.
  - Transferir, vender ou usar dados do usuário com qualquer produto ou serviço que possa se qualificar como dispositivo médico, a menos que o app do dispositivo médico obedeça a todas as regulamentações, inclusive obtendo todas as liberações ou aprovações dos órgãos regulamentares relevantes (por exemplo, a FDA nos EUA, que é equivalente à ANVISA no Brasil) para o uso pretendido dos dados do app Conexão Saúde, e o usuário tenha dado consentimento explícito para isso.
  - Transferir, vender ou usar dados do usuário para qualquer propósito ou de qualquer maneira envolvendo Informações protegidas de saúde (conforme definidas pela HIPAA), exceto se iniciado pelo usuário ou em conformidade com a regulamentação da HIPAA.

Escopo mínimo

Solicite acesso somente às permissões necessárias para implementar os recursos e serviços do seu produto. Esses pedidos devem ser específicos e se limitar aos dados necessários.

Avisos e controles transparentes e precisos

O app Conexão Saúde lida com dados de saúde e condicionamento físico, o que inclui informações pessoais e sensíveis. Os desenvolvedores precisam apresentar declarações claras e acessíveis sobre suas práticas relacionadas a dados em uma Política de Privacidade abrangente. Essas declarações precisam incluir:

- Uma representação exata da identidade do aplicativo ou serviço que solicita acesso a dados de usuários.
- Informações claras e precisas que explicam quais tipos de dados estão sendo acessados, solicitados e/ou coletados. Os dados precisam estar relacionados a um recurso ou recomendação voltados ao usuário e oferecidos pelo app.
- Uma explicação sobre como os dados serão usados e/ou compartilhados: se você solicita dados por um motivo, mas eles também serão usados para um propósito secundário, é obrigatório divulgar todos os casos de uso aos usuários.
- Documentação de ajuda explicando como usuários podem gerenciar e excluir os próprios dados do app e o que acontece com os dados quando uma conta é desativada e/ou excluída.
- Uma explicação sobre como o app lida com todos os dados pessoais e sensíveis dos usuários de forma segura, incluindo a transmissão com criptografia moderna (por exemplo, usando HTTPS).

Para mais informações sobre os requisitos dos apps que se vinculam ao Conexão Saúde, consulte este artigo da Central de Ajuda.

Serviço VPN

VpnService é uma classe de base para que os apps ampliem e criem soluções de VPN próprias. Somente os apps que usam VpnService e têm a VPN [illegible] m criar um encapsulamento seguro no nível do dispositivo para um servidor remoto. Exceções incluem apps que exigem um servidor remoto para oferecer o recurso principal, por exemplo:

Bin | 00:57:08 | Bin

- Apps de controle da família e gerenciamento empresarial
- Monitoramento de uso de apps
- Apps de segurança de dispositivos, como antivírus, gerenciamento de dispositivos móveis e firewall
- Ferramentas relacionadas à rede, como acesso remoto
- Apps de navegação na Web
- Apps de operadoras que precisam de funcionalidade VPN para oferecer serviços de telefonia ou conectividade

O VpnService não pode ser usado para:

- coletar dados pessoais e confidenciais do usuário sem consentimento e declaração em destaque;
- redirecionar ou manipular o tráfego de usuários de outros apps em um dispositivo para fins de monetização, por exemplo: redirecionar o tráfego de publicidade para um país que não seja o do usuário;

Os apps que usam o VpnService precisam:

- documentar o uso dessa classe na página "Detalhes do app";
- criptografar os dados do dispositivo para o endpoint do encapsulamento de VPN;
- obedecer a todas as Políticas do programa para desenvolvedores, incluindo as relacionadas a fraude de anúncio, permissões e malware.

Permissão de alarme exato

A nova permissão `USE_EXACT_ALARM` vai ser introduzida para dar acesso à funcionalidade de alarme exato em apps a partir do Android 13 (nível desejado da API 33).

`USE_EXACT_ALARM` é uma permissão restrita, e os apps só deverão declará-la se o recurso principal deles for compatível com a necessidade de um alarme exato. Os apps que solicitam essa permissão restrita estão sujeitos a revisão, e aqueles que não atenderem aos critérios de caso de uso aceitável não vão ser publicados no Google Play.

Casos de uso aceitáveis para a permissão de alarme exato

Seu app só deverá usar a funcionalidade `USE_EXACT_ALARM` quando o recurso principal dele voltado para o usuário exigir ações com tempo preciso, por exemplo:

- Apps de alarme ou cronômetro
- Apps de calendário que exibem notificações de eventos

Se seu caso de uso para a funcionalidade de alarme exato não estiver listado acima, avalie a possibilidade de usar `SCHEDULE_EXACT_ALARM`.

Para mais informações sobre a funcionalidade de alarme exato, consulte estas orientações para desenvolvedores.

Permissão de intent para tela cheia

Para apps destinados ao Android 14 (nível desejado da API 34) e versões mais recentes, a `USE_FULL_SCREEN_INTENT` é uma permissão de acesso especial para apps. A permissão

`USE_FULL_SCREEN_INTENT` só será concedida de modo automático se a funcionalidade principal do app se enquadrar em uma das categorias abaixo que requerem notificações de alta prioridade:

- definir um alarme
- receber ligações ou videochamadas

Bin | 00:57:08 | Bin

Os apps que solicitam essa permissão estão sujeitos a um processo de análise, e aqueles que não atenderem aos critérios descritos acima não receberão a permissão por padrão. Nesse caso, para usar a `USE_FULL_SCREEN_INTENT`, os apps precisarão solicitar a permissão do usuário.

O uso da permissão **`USE_FULL_SCREEN_INTENT`** precisa obedecer às políticas para desenvolvedores do Google Play, incluindo nossas diretrizes sobre software indesejado para dispositivos móveis, abuso de dispositivos e de rede e anúncios. As notificações de intent para tela cheia não podem interferir, interromper, danificar nem acessar o dispositivo do usuário de maneira não autorizada. Além disso, os apps não podem interferir em outros apps nem na usabilidade do dispositivo.

Saiba mais sobre a permissão `USE_FULL_SCREEN_INTENT` na nossa Central de Ajuda.

API Age Signals e dados do usuário

Esta política define as condições para o uso da API Age Signals , que dá acesso a dados pessoais e sensíveis do usuário relacionados a idade e autorização dos responsáveis.

Você só pode usar os dados acessados pela API Age Signals para cumprir obrigações legais e regulatórias aplicáveis, como oferecer experiências no seu app adequadas à faixa etária.

É estritamente proibido usar esses dados para os seguintes fins, incluindo, mas não se limitando a:

- Fins de publicidade, marketing ou personalização, incluindo a veiculação de anúncios segmentados
- Análise de dados, criação de perfis de usuários ou business intelligence
- Venda, compartilhamento ou transferência de dados para terceiros por qualquer motivo, exceto quando estritamente exigido por lei

---

Abuso de dispositivos e de rede

Não são permitidos apps que causam danos, interferências ou interrupções ou acessam de maneira não autorizada o dispositivo do usuário, assim como outros dispositivos ou computadores, servidores, redes, interfaces de programação do app (APIs, na sigla em inglês) ou serviços. Isso inclui, sem limitação, outros apps no dispositivo, qualquer serviço do Google ou uma rede de operadora de telefonia autorizada.

Os apps no Google Play precisam obedecer aos requisitos padrão de otimização do sistema Android listados nas diretrizes principais de qualidade de apps para o Google Play .

Os apps distribuídos pelo Google Play só podem ser modificados, substituídos ou atualizados pelo mecanismo de atualização do Google Play. Da mesma forma, um app só pode fazer o download de código executável (por exemplo, arquivos dex, JAR ou .so) do Google Play. Essa restrição não se aplica a códigos executados em máquinas virtuais ou intérpretes que ofereçam acesso indireto às APIs do Android (como o JavaScript em um WebView ou navegador).

Apps ou código de terceiros (por exemplo, SDKs) com linguagens interpretadas (JavaScript, Python, Lua etc.) carregadas em tempo de execução (por exemplo, não empacotadas com o app) não podem permitir possíveis violações das políticas do Google Play.

Não são permitidos códigos que introduzam ou explorem vulnerabilidades de segurança. Confira o Programa de melhoria da segurança dos aplicativos para saber mais sobre os problemas de segurança mais recentes sinalizados para os desenvolvedores.

Exemplos comuns de violação por abuso de dispositivos e de rede:

- Apps que impedem que outro app exiba anúncios ou interferem na exibição deles
- Apps para trapacear em jogos que afetam a jogabilidade de outros apps
- Apps que facilitam ou oferecem instruções de com e hardwares ou como burlar proteções de segurança
- Apps que acessam ou usam um serviço ou uma API de um modo que viola os Termos de Serviço da API ou do serviço em questão
- Apps que não estão qualificados para a lista de permissões e tentam burlar o gerenciamento de energia do sistema
- Apps que facilitam serviços de proxy para terceiros, o que só pode ser feito se essa for a finalidade principal do app
- Apps ou código de terceiros (por exemplo, SDKs) que fazem download de código executável (como arquivos dex ou código nativo) de uma fonte que não seja o Google Play
- Apps que instalam outros apps em um dispositivo sem o consentimento prévio do usuário
- Apps que facilitam a distribuição ou instalação de software malicioso ou contêm links para esse tipo de software
- Apps ou código de terceiros (por exemplo, SDKs) contendo um WebView com interface JavaScript adicionada que carrega conteúdo da Web não confiável (por exemplo, URL http://) ou URLs não verificados obtidos de fontes não confiáveis (por exemplo, URLs obtidos com intents não confiáveis)
- Apps que usam a permissão de intent para tela cheia para forçar a interação do usuário com notificações ou anúncios invasivos
- Apps que contornam as proteções do sandbox Android para derivar a atividade ou identidade do usuário de outros apps

Uso de serviço em primeiro plano

A permissão de serviço em primeiro plano garante o uso apropriado dos serviços desse tipo voltados ao usuário. Para apps destinados ao Android 14 e versões mais recentes, é necessário especificar um tipo de serviço em primeiro plano válido para cada serviço dessa categoria usado no app e declarar a permissão de serviço em primeiro plano adequada para o tipo. Por exemplo, se o caso de uso do seu app exigir geolocalização do mapa, é necessário declarar a permissão FOREGROUND_SERVICE_LOCATION no manifesto do app.

Os apps só podem declarar uma permissão de serviço em primeiro plano caso o uso:

- ofereça um recurso benéfico para o usuário e relevante para a funcionalidade principal do app;
- seja iniciado pelo usuário ou perceptível por ele (por exemplo, áudio de uma música, transmissão de mídia para outro dispositivo, notificação precisa e clara ao usuário e solicitação do usuário para enviar uma foto à nuvem);
- possa ser encerrado ou interrompido pelo usuário;
- não possa ser interrompido nem adiado pelo sistema sem gerar uma experiência negativa ao usuário ou fazer com que o recurso antecipado por ele não funcione como pretendido (por exemplo, uma chamada telefônica precisa começar imediatamente e não pode ser adiada pelo sistema);
- seja executado apenas pelo tempo necessário para concluir a tarefa.

Os seguintes casos de uso de serviços em primeiro plano estão isentos dos critérios acima:

- Tipos de serviço em primeiro plano systemExempted ou shortService
- Se os recursos do Play Asset Delivery estão sendo usados, tipo de serviço em primeiro plano "dataSync"

Saiba mais sobre o uso dos serviços em primeiro plano.

API User-initiated Data Transfer Jobs

Os apps só podem usar a API User-initiated Data Transfer Jobs se o uso for:

- iniciado pelo usuário;
- para tarefas de transferência de dados da rede;
- executado apenas pelo tempo necessário para concluir a transferência de dados.

Bin | 00:57:08 | Bin

Saiba mais sobre o uso das APIs de transferência de dados iniciada pelo usuário.

Requisitos relacionados à FLAG_SECURE

FLAG_SECURE é uma sinalização de exibição declarada no código de um app para indicar que a IU contém dados confidenciais que precisam ser limitados a uma plataforma segura durante o uso do app. Essa sinalização foi criada para impedir que os dados apareçam em capturas de tela ou sejam visualizados em telas não seguras. Os desenvolvedores declaram essa sinalização quando o conteúdo não deve ser visualizado nem transmitido fora do app ou do dispositivo dos usuários.

Por motivos de segurança e privacidade, todos os apps distribuídos no Google Play precisam respeitar a declaração FLAG_SECURE de outros apps. Os apps não devem facilitar nem criar alternativas para ignorar as configurações de FLAG_SECURE em outros apps.

Os apps qualificados como ferramenta de acessibilidade não precisam atender a esse requisito, desde que não transmitam, salvem nem armazenem em cache conteúdo protegido por FLAG_SECURE para acesso fora do dispositivo do usuário.

Apps que são executados em contêineres Android no dispositivo

Os apps executados em um contêiner Android no dispositivo oferecem ambientes que simulam todo ou partes de um SO Android. É possível que a experiência nesses ambientes não reflita o pacote completo de recursos de segurança do Android. Por isso, os desenvolvedores têm a opção de adicionar uma flag de manifesto de ambiente seguro para comunicar aos contêineres Android no dispositivo que eles não podem operar na versão simulada do sistema Android.

Sinalização de ambiente seguro no manifesto

A flag REQUIRE_SECURE_ENV pode ser declarada no manifesto do app para indicar que ele não deve ser executado em um contêiner Android no dispositivo. Para fins de segurança e privacidade, os apps que fornecem contêineres Android no dispositivo precisam respeitar os apps que declaram essa flag. Além disso:

- Revise os manifestos dos apps que eles pretendem carregar no contêiner Android no dispositivo para essa flag.
- Não carregue os apps que declararam essa flag no contêiner Android no dispositivo.
- Não opere como um proxy interceptando ou chamando APIs no dispositivo para que pareçam estar instalados no contêiner.
- Não facilite nem crie soluções alternativas para ignorar a flag, como carregar uma versão mais antiga de um app para burlar a flag REQUIRE_SECURE_ENV do atual.

Saiba mais sobre essa política na Central de Ajuda.

Comportamento enganoso

Não são permitidos apps que tentam enganar os usuários ou permitem comportamento desonesto, incluindo, mas não se limitando a, apps com um recurso impossível. Os apps precisam incluir divulgação, descrição e imagens/vídeos precisos de suas funcionalidades em todos os metadados. Os apps não podem tentar imitar a funcionalidade ou os avisos do sistema operacional ou de outros apps. As alterações nas configurações do dispositivo precisam ter o conhecimento e consentimento do usuário e ser reversíveis por ele.

Declarações enganosas

Apps que contenham informações ou declarações falsas ou enganosas, inclusive na descrição, no título, no ícone e nas capturas de tela, não são perm

Bin | 00:57:08 | Bin

Veja alguns exemplos de violações comuns:

- Apps que deturpem a funcionalidade ou que não a descrevam de forma clara e precisa:
  - Um app que alega ser um jogo de corrida na descrição e nas capturas de tela, mas na verdade é um quebra-cabeças usando a imagem de um carro
  - Um app que alega ser um antivírus, mas contém somente um manual explicando como remover vírus
- Apps que alegam ter funcionalidades impossíveis de serem implementadas (por exemplo, apps repelentes de insetos), mesmo que sejam representados como pegadinhas, dissimulações, piadas etc.
- Apps categorizados incorretamente, incluindo, mas não se limitando a, classificação ou categoria do app
- Conteúdo comprovadamente falso ou enganoso que pode interferir nos processos de votação ou nos resultados de eleições
- Apps que alegam falsamente afiliação a uma entidade governamental ou afirmam fornecer ou facilitar serviços públicos sem a devida autorização
- Apps que alegam falsamente ser o app oficial de uma entidade estabelecida. Títulos como "App oficial do Justin Bieber" não são permitidos sem os direitos ou as permissões necessárias

(1) Apps que alegam ter funções impossíveis de serem implementadas (usar o smartphone como bafômetro).

Alterações enganosas nas configurações do dispositivo

Apps que façam alterações nas configurações do dispositivo ou em recursos fora do app sem o conhecimento e consentimento do usuário não são p[illegible] os recursos do dispositivo incluem configurações do sistema e do navegador, favoritos, atalhos, ícones e widgets, além da apresentação de apps na tela inicial.

Bin | 00:57:08 | Bin

Além disso, não são permitidos:

- Apps que modifiquem as configurações ou os recursos de um dispositivo com o consentimento do usuário, mas de maneira que não possa ser revertida facilmente
- Apps ou anúncios que modifiquem as configurações ou os recursos do dispositivo, como um serviço para terceiros ou para fins de publicidade
- Apps que induzam os usuários a remover ou desativar apps de terceiros ou modificar configurações ou recursos do dispositivo
- apps que incentivem os usuários a remover ou desativar apps de terceiros ou modificar configurações ou recursos do dispositivo, a menos que sejam parte de um serviço de segurança verificável.

Permitir comportamento desonesto

Não são permitidos apps que ajudem os usuários a enganar outras pessoas ou com funcionamento enganoso de alguma forma, incluindo, entre outros, apps que gerem ou facilitem a geração de RGs, CPFs, passaportes, diplomas, cartões de crédito, contas bancárias e carteiras de motorista. É necessário apresentar informações precisas em divulgações, títulos, descrições e imagens/vídeos relacionados à função e/ou ao conteúdo do app. Além disso, o desempenho e a precisão devem atender à expectativa do usuário.

O download de recursos adicionais do app (por exemplo, recursos de jogos) só poderá ser feito se eles forem necessários para usar o app. Os recursos salvos precisam obedecer a todas as políticas do Google Play e, antes de iniciar o download, é obrigatório fazer uma solicitação ao usuário e informar claramente o tamanho do app.

A declaração do app como uma "brincadeira", "para fins de entretenimento" ou outro sinônimo não o isenta da aplicação das nossas políticas.

Veja alguns exemplos de violações comuns:

- Apps que imitam outros aplicativos ou sites para induzir os usuários a divulgar informações pessoais ou de autenticação
  - Apps que retratam ou exibem números de telefone, contatos, endereços ou informações que permitam identificar uma pessoa, sejam elas não confirmadas ou reais, de pessoas ou entidades sem o consentimento delas
- Apps com funcionalidade principal diferente com base na região geográfica, nos parâmetros do dispositivo ou em outros dados dependentes do usuário em que essas diferenças não são divulgadas em destaque para o usuário na página "Detalhes do app"
- Apps que mudam significativamente entre as versões sem alertar o usuário (por exemplo, a seção "Novidades") e atualizar a página "Detalhes do app"
- Apps que tentam modificar ou ofuscar o comportamento durante a revisão
- Apps com downloads facilitados por rede de fornecimento de conteúdo (CDN) quando não há uma solicitação ao usuário antes de começar nem é informado o tamanho do download

Mídia manipulada

Não são permitidos apps que promovam ou ajudem a criar informações falsas ou enganosas veiculadas em imagens, áudios, vídeos e/ou textos. Não são aceitos apps desenvolvidos para

promover ou perpetuar imagens, vídeos ou texto comprovadamente enganosos ou que possam causar danos relacionados a eventos sensíveis, política, questões sociais ou outros temas de interesse público.

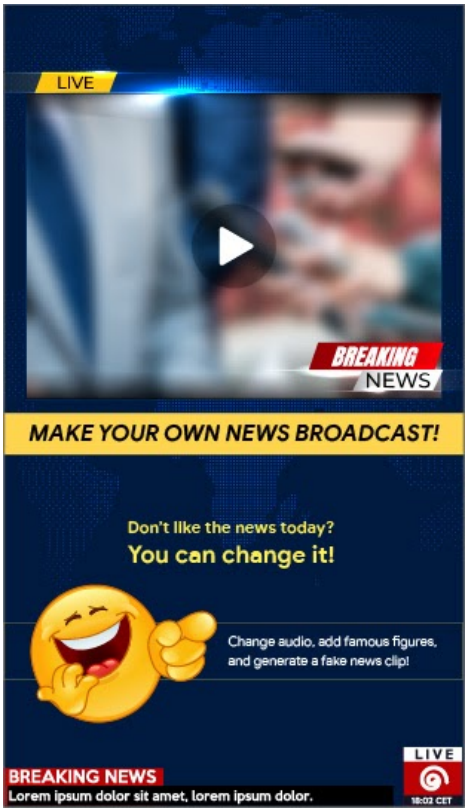
Bin | 00:57:08 | Bin

Pode haver exceções em caso de interesse público, imagens claramente artificiais, mídia manipulada com avisos ou marcas-d'água voltados ao usuário e sátiras ou paródias óbvias.

A mídia manipulada precisa obedecer às políticas para desenvolvedores do Google Play, inclusive proibindo conteúdo não permitido conforme as políticas de conteúdo restrito.

Veja alguns exemplos de violações comuns:

- Apps que usam figuras públicas ou mídia de eventos sensíveis para promover recursos de modificação de mídia na página Detalhes do app.
- Apps que alteram clipes de mídia a fim de imitar uma transmissão de notícias ao incluir nomes ou logotipos de veículos de comunicação reais sem avisos ou marcas-d'água claros.
- Apps com a única finalidade de criar mídia enganosa.



(1) Este app oferece funcionalidades para alterar clipes de mídia a fim de imitar uma transmissão de notícias e adicionar pessoas famosas ou públicas ao clipe sem uma marca-d'água.

Transparência em relação ao comportamento

A funcionalidade do app precisa ficar clara para os usuários. Ele não pode incluir recursos ocultos, inativos ou não documentados. É proibido usar técnicas para burlar as avaliações do app. Talvez seja preciso dar mais detalhes sobre o app para garantir a segurança dos usuários, a integridade do sistema e a conformidade com as políticas.

Declarações falsas

Não são permitidos apps nem contas de desenvolvedor que:

- se façam passar por outra pessoa ou organização ou que deturpem ou ocultem a propriedade ou o objetivo principal;

- se envolvam em atividades coordenadas para enganar os usuários. Isso inclui, entre outros, apps ou contas que deturpam ou ocultam o país de origem ou que direcionam conteúdo para usuários em outros países;
- se coordenem com outros apps, sites, desenvolve[illegible] ou fazer declarações falsas sobre a identidade do app ou do desenvolvedor ou outros detalhes relevantes, caso o conteúdo do app se relacione a política, questões sociais ou assuntos de interesse público.

Bin | 00:57:08 | Bin

Política de nível desejado da API do Google Play

Para proteger os usuários, o Google Play exige os seguintes níveis da API para **todos os apps**:

Novos apps e atualizações PRECISAM ser voltados para um nível da API do Android com no máximo um ano de diferença em relação à versão mais recente. Se esse requisito não for atendido, não vai ser possível enviar o app ou a atualização no Play Console.

Os apps que já estão no Google Play, mas não foram atualizados e que não forem voltados para um nível de API com no máximo dois anos de diferença em relação à versão mais recente do Android não vão estar disponíveis para novos usuários com versões mais recentes do Android no dispositivo.Quem já tiver feito a instalação no Google Play ainda vai conseguir encontrar, reinstalar e usar o app em qualquer versão do Android compatível com ele.

Para orientações técnicas sobre como atender ao requisito de nível desejado da API, consulte o guia de migração .

Para saber os prazos e as exceções, confira este artigo da Central de Ajuda .

Uso de SDKs Em Apps

Ao incluir um SDK no seu app, você é responsável por garantir que o código e as práticas de terceiros não façam o app violar as Políticas do programa para desenvolvedores do Google Play. É importante entender como os SDKs no app lidam com os dados do usuário e saber quais permissões eles usam, quais dados eles coletam e por quê.

Requisitos de SDK

Os desenvolvedores geralmente dependem de código de terceiros (por exemplo, SDKs) para integrar funcionalidades e serviços importantes aos apps. Ao incluir um SDK no seu app, é importante manter os usuários seguros e o app protegido contra vulnerabilidades. Nesta seção, demonstramos como alguns dos nossos requisitos de privacidade e segurança se aplicam ao contexto do SDK e são projetados para ajudar os desenvolvedores a integrar SDKs aos apps com segurança.

Ao incluir um SDK no seu app, você é responsável por garantir que o código e as práticas de terceiros não façam o app violar as Políticas do programa para desenvolvedores do Google Play. É importante entender como os SDKs no app lidam com os dados do usuário e saber quais permissões eles usam, quais dados eles coletam e por quê. Lembre-se de que a coleta e o manuseio de dados do usuário por um SDK precisam estar alinhados com o uso desses dados em conformidade com a política do app.

Para garantir que o uso de um SDK não viole os requisitos da política, leia e entenda as seguintes políticas na íntegra e observe os requisitos relativos a SDKs abaixo:

Política de dados do usuário

Você precisa ser transparente sobre como lida com os dados do usuário (por exemplo, dados coletados do usuário ou sobre ele, incluindo informações do dispositivo). Isso significa divulgar o acesso, a coleta, o uso, o tratamento e o compartilhamento dos dados do usuário do seu app e limitar o uso dos dados às finalidades divulgadas em conformidade com a política.

Se você inclui código de terceiros, como um SDK, no seu app, é necessário garantir que o código usado e as práticas do terceiro em relação aos dados do usuário do app obedeçam às Políticas do programa para desenvolvedores do Google Play, incl[illegible] divulgação. Por exemplo, você precisa garantir que os fornecedores [illegible] pessoais e sensíveis dos usuários do app. Esse requisito se aplica mesmo se a transferência dos dados do usuário for após o envio ao servidor ou ao incorporar código de terceiros no app.

Bin | 00:57:08 | Bin

Dados pessoais e sensíveis do usuário

- Limite o acesso, a coleta, o uso e o compartilhamento de dados pessoais e sensíveis coletados pelo app à funcionalidade do app e do serviço e às finalidades que estão em conformidade com a política e são esperadas pelo usuário.
  - Os apps que estendem o uso de dados pessoais e sensíveis do usuário para veiculação de anúncios precisam obedecer à política de anúncios do Google Play.
- Trate todos os dados pessoais ou sensíveis do usuário de maneira segura, incluindo a transmissão desses dados por criptografia moderna, como HTTPS.
- Use uma solicitação de permissões de execução sempre que disponível, antes de acessar os dados controlados por permissões do Android.

Venda de dados pessoais e sensíveis do usuário

Não venda dados pessoais e sensíveis do usuário.

- "Venda" significa a troca ou transferência de dados sensíveis e pessoais do usuário para um terceiro por compensação monetária.
  - A transferência de dados pessoais e sensíveis iniciada pelo usuário (por exemplo, quando o usuário está usando um recurso do app para transferir um arquivo a um terceiro ou quando o usuário escolhe usar um app de pesquisa de finalidade dedicada) não é considerada como venda.

Requisitos de consentimento e declaração em destaque

Quando o app acessar, coletar, usar ou compartilhar dados pessoais e sensíveis do usuário de maneira que não corresponda às expectativas do usuário do produto ou recurso em questão, é necessário obedecer à solicitação de consentimento e declaração em destaque da política de dados do usuário.

Se o app integrar código de terceiro, como um SDK, feito para coletar dados pessoais e sensíveis do usuário por padrão, você precisa, até duas semanas após receber uma solicitação do Google Play (ou, se o pedido do Google Play oferecer um prazo mais longo, dentro desse período), oferecer evidência suficiente mostrando que o app obedece à solicitação de consentimento e declaração em destaque da política, incluindo em relação ao acesso, à coleta, ao uso ou ao compartilhamento de dados por código de terceiro.

Verifique se o uso de código de terceiros (por exemplo, um SDK) não faz seu app violar a política de dados do usuário.

Consulte este artigo da Central de Ajuda para mais informações sobre à solicitação de consentimento e declaração em destaque.

Exemplos de violações causadas pelo SDK

- Um app com um SDK que coleta informações pessoais e sensíveis do usuário e não as trata como sujeitas aos requisitos da política de dados do usuário, de acesso, de tratamento de dados (incluindo a proibição de venda) e de solicitação de consentimento e declaração em destaque.
- Um app integra um SDK que coleta dados pessoais e sensíveis do usuário por padrão, violando os requisitos desta política em relação ao consentimento do usuário e à declaração em destaque.
- Um app com um SDK que declara coletar dados pessoais e sensíveis do usuário apenas para oferecer funcionalidade antifraude e antiabuso, mas também compartilha essas informações com terceiros para publicidade ou análise.
- Um app inclui um SDK que transmite informações de pacotes instalados pelos usuários sem atender às diretrizes da declaração em destaque e/ou às diretrizes da política de privacidade.
  - Consulte também a política de software indesejado para dispositivos móveis.

Requisitos adicionais para acesso a dados pessoais e sensíveis

A tabela abaixo descreve os requisitos para atividades específicas.

Atividade	Requisito
Seu app coleta ou vincula identificadores permanentes de dispositivo (por exemplo, IMEI, IMSI, Nº de série do chip etc.).	Identificadores permanentes de dispositivo não podem ser vinculados a outros dados de usuários ou identificadores [illegible] em casos de: • telefonia vinculada a uma identidade do chip (por exemplo, chamada de Wi-Fi vinculada à conta da operadora); • apps de gerenciamento de dispositivos corporativos que usam o modo proprietário do dispositivo. Esses usos precisam ser divulgados com destaque aos usuários, conforme especificado na política de dados do usuário. Consulte este recurso para identificadores únicos alternativos. Acesse a política de anúncios para ver mais diretrizes sobre o ID de publicidade do Android.
O público-alvo do seu app inclui crianças.	Seu app só pode incluir SDKs autocertificados para uso em serviços feitos para crianças. Consulte o Programa de SDKs de anúncio autocertificados para famílias para ver o texto e os requisitos completos da política.

Bin | 00:57:08 | Bin

Exemplos de violações causadas pelo SDK

- Um app usando um SDK que vincula o IMEI ao local.
- Um app com um SDK que conecta o ID de publicidade do Android (AAID) a identificadores permanentes de dispositivo para qualquer finalidade de publicidade ou análise.
  Um app usando um SDK que conecta o AAID e o endereço de e-mail para fins de análise.

Seção "Segurança dos dados"

Todos os desenvolvedores precisam ter uma seção "Segurança dos dados" clara e precisa em cada app, detalhando a coleta, o uso e o compartilhamento de dados do usuário. Isso inclui dados coletados e processados por bibliotecas ou SDKs de terceiros usados nos apps. O desenvolvedor é responsável por garantir a precisão do marcador e por manter as informações atualizadas. Quando relevante, essa seção precisa ser consistente com as divulgações feitas na Política de Privacidade do app.

Consulte este artigo da Central de Ajuda para saber como preencher a seção "Segurança dos dados".

Consulte a política de dados do usuário.

Política de permissões e APIs que acessam informações sensíveis

As solicitações de permissões e de APIs que acessam informações sensíveis precisam fazer sentido para os usuários. O app só pode solicitar permissões e APIs que acessam informações sensíveis necessárias para implementar recursos ou serviços atuais promovidos na página "Detalhes do app". Não use permissões ou APIs que acessam informações sensíveis com acesso a dados do usuário ou do dispositivo para finalidades ou recursos não revelados, não implementados ou não permitidos. Dados pessoais ou sensíveis acessados por permissões ou APIs que acessam informações sensíveis não podem ser vendidos nem compartilhados com a finalidade de facilitar uma venda.

Consulte a Política de permissões e APIs que acessam informações sensíveis.

Exemplos de violações causadas pelo SDK

- O app inclui um SDK que solicita a localização em segundo plano para uma finalidade não permitida ou não divulgada.
- O app inclui um SDK que transmite IMEI derivado da permissão read_phone_state do Android sem o consentimento do usuário.

Política de malware

Nossa política contra malware é simples: o ecossistema Android, inclusive a Google Play Store, e os dispositivos do usuário não podem apresentar comportamentos maliciosos (por exemplo, malware). Com base nesse princípio fundamental, buscamos fo[illegible]oid seguro para os usuários e os dispositivos Android deles.

Bin | 00:57:08 | Bin

Malware é qualquer código capaz de colocar um usuário, os dados dele ou um dispositivo em risco. O malware inclui aplicativos potencialmente nocivos (PHAs), binários ou modificações do framework que consistem em apps de trojans, phishing e spyware, entre outros. Além dessas, estamos continuamente atualizando e adicionando novas categorias.

Os requisitos da política também se aplicam a todo código de terceiros (por exemplo, SDKs) que você inclua no seu app.

Consulte a política de malware.

Exemplos de violações causadas pelo SDK

- Um app que inclui bibliotecas de SDK de provedores que distribuem software malicioso.
- Um app que viola o modelo de permissões do Android ou rouba credenciais (como tokens OAuth) de outros apps
- Apps que abusam de recursos para impedir que sejam desinstalados ou interrompidos
- Um app que desativa o SELinux
- Um app que inclui um SDK que viola o modelo de permissões do Android ao receber privilégios elevados com acesso aos dados do dispositivo para uma finalidade não divulgada
- Um app que inclui um SDK com código que induz os usuários a assinar ou comprar conteúdo com faturamento via operadora

Apps com escalonamento de privilégios que dão acesso root a dispositivos sem a permissão do usuário são considerados apps de acesso root.

Spyware

O spyware é um comportamento, código ou aplicativo malicioso que coleta, extrai ou compartilha dados do dispositivo ou do usuário que não têm relação com as funcionalidades que obedecem à política.

Um código ou comportamento malicioso que pode ser considerado espionagem ou extrai dados do usuário sem o devido consentimento ou aviso também é identificado como spyware.

Leia a política contra spyware na íntegra.

Confira alguns exemplos de violações de spyware causadas por SDK:

- Um app que usa um SDK que transmite dados de gravações de áudio ou chamada em algum caso não relacionado à funcionalidade do app que obedece à política
- Um app com código malicioso de terceiros (por exemplo, um SDK) que transmite dados para fora do dispositivo de maneira inesperada ao usuário e/ou sem o devido consentimento ou aviso

Política de software indesejado para dispositivos móveis

Comportamento transparente e divulgações claras

Todos os códigos precisam cumprir as promessas feitas ao usuário. Os apps precisam fornecer todas as funcionalidades informadas. Os apps não podem confundir os usuários.

Exemplos de violação:

- Fraude de anúncio
- Engenharia social

Proteção dos dados do usuário

Divulgue com clareza e transparência o acesso, o uso, a coleta e o compartilhamento de dados pessoais e sensíveis do usuário. As aplicações dos d[illegible]ar de acordo com todas as políticas relevantes sobre o assunto, quand[illegible]mar todas as precauções para proteger os dados.

Bin | 00:57:08 | Bin

Exemplos de violação:

- Coleta de dados (confira a seção sobre spyware)
- Abuso de permissões restritas

Consulte a política de software indesejado para dispositivos móveis

Política de abuso de dispositivos e de rede

Não são permitidos apps que causem danos, interferências ou interrupções ou acessem de maneira não autorizada o dispositivo do usuário, assim como outros dispositivos ou computadores, servidores, redes, interfaces de programação do aplicativo (APIs) ou serviços. Isso inclui, sem limitação, outros apps no dispositivo, qualquer serviço do Google ou uma rede de operadora de telefonia autorizada.

Apps ou código de terceiros (por exemplo, SDKs) com linguagens interpretadas (JavaScript, Python, Lua etc.) carregadas em tempo de execução (por exemplo, não empacotadas com o app) não podem permitir possíveis violações das políticas do Google Play.

Não são permitidos códigos que introduzam ou explorem vulnerabilidades de segurança. Confira o Programa de melhoria da segurança dos aplicativos para saber mais sobre os problemas de segurança mais recentes sinalizados para os desenvolvedores.

Confira a política de abuso de dispositivos e de rede.

Exemplos de violações causadas pelo SDK

- Apps que facilitam serviços de proxy para terceiros, o que só pode ser feito se essa for a finalidade principal do app.
- O app inclui um SDK que faz download de código executável, como arquivos DEX ou código nativo, de uma fonte diferente do Google Play.
- O app inclui um SDK contendo um WebView com interface JavaScript adicionada que carrega conteúdo da Web não confiável (por exemplo, URL http://) ou URLs não verificados obtidos de fontes não confiáveis (por exemplo, URLs obtidos com intents não confiáveis).
- O app inclui um SDK que tem código usado para atualizar o próprio APK.
- O app inclui um SDK que expõe os usuários a uma vulnerabilidade de segurança ao fazer o download de arquivos com uma conexão sem segurança.
- O app usa um SDK que tem código para fazer download ou instalar apps de fontes desconhecidas fora do Google Play.
- O app inclui um SDK que usa serviços em primeiro plano sem um caso de uso adequado.
- O app inclui um SDK que usa serviços em primeiro plano para um motivo que obedece às políticas, mas não declara isso no manifesto.

Política contra comportamento enganoso

Não são permitidos apps que tentam enganar os usuários ou permitem comportamento desonesto, incluindo, mas não se limitando a, apps com uma funcionalidade impossível. Os apps precisam incluir divulgação, descrição e imagens/vídeos precisos das funções em todos os metadados. Os apps não podem tentar imitar a funcionalidade ou os avisos do sistema operacional ou de outros apps. As mudanças nas configurações do dispositivo precisam ser facilmente reversíveis pelo usuário e ter o conhecimento e consentimento dele.

Confira a política contra comportamento enganoso na íntegra.

Transparência em relação ao comportamento

A funcionalidade do app precisa ficar clara para os usuários. Ele não pode incluir recursos ocultos, inativos ou não documentados. É proibido usar técni Bin | 00:57:08 | Bin do app. Talvez seja preciso dar mais detalhes sobre o app para garantir a segurança dos usuários, a integridade do sistema e a conformidade com as políticas.

Exemplo de violação causada por um SDK

- Seu app tem um SDK que usa técnicas para escapar das revisões.

Que políticas para desenvolvedores do Google Play geralmente são associadas a violações causadas por SDKs?

Para ajudar você a garantir que todos os códigos de terceiros que seu app use estejam em conformidade com as políticas do programa para desenvolvedores do Google Play, consulte as seguintes políticas na íntegra:

- Política de dados do usuário
- Permissões e APIs que acessam informações sensíveis
- Política de abuso de dispositivos e de rede
- Malware
- Software indesejado para dispositivos móveis
- Programa de SDKs de anúncio autocertificados para famílias
- Política de anúncios
- Comportamento enganoso
- Políticas do programa para desenvolvedores do Google Play

Embora essas políticas sejam as mais relevantes, é importante lembrar que um código de SDK inválido pode fazer o app violar uma política diferente não mencionada acima. Leia e fique por dentro de todas as políticas. É sua responsabilidade como desenvolvedor de apps garantir que os SDKs manipulem os dados do app sem violar as políticas.

Para saber mais, visite nossa Central de Ajuda.

Malware

Nossa política contra malware é simples: o ecossistema Android, inclusive a Google Play Store, e os dispositivos do usuário não podem apresentar comportamentos maliciosos (por exemplo, malware). Com base nesse princípio fundamental, buscamos fornecer um ecossistema Android seguro para os usuários e os dispositivos Android deles.

Malware é qualquer código capaz de colocar um usuário, os dados dele ou um dispositivo em risco. O malware inclui aplicativos potencialmente nocivos (PHAs), binários ou modificações do framework que consistem em apps de trojans, phishing e spyware, entre outros. Além dessas, estamos continuamente atualizando e adicionando novas categorias.

Os requisitos da política também se aplicam a todo código de terceiros (por exemplo, SDKs) que você inclua no seu app.

Com diferentes tipos e recursos, o malware geralmente tem um dos seguintes objetivos:

- Comprometer a integridade do dispositivo do usuário
- Controlar um dispositivo do usuário
- Ativar operações controladas remotamente para que um invasor acesse, use ou explore um dispositivo infectado
- Transmitir dados pessoais ou credenciais do dispositivo sem a divulgação e o consentimento adequados

- Enviar spam ou comandos do dispositivo infectado a outros dispositivos ou redes
- Enganar o usuário

Um app, binário ou uma modificação do framework p Bin | 00:57:08 | Bin comportamento malicioso, mesmo que essa não tenha sido a intenção. Eles podem agir de diferentes maneiras, de acordo com uma série de variáveis. Portanto, o que é nocivo para um dispositivo Android pode não provocar risco algum em outro dispositivo Android. Por exemplo, um dispositivo que executa a última versão do Android não será afetado por apps nocivos que usam APIs obsoletas para realizar comportamentos maliciosos, mas um dispositivo que use uma versão muito antiga do Android pode estar em risco. Apps, binários ou modificações do framework serão sinalizados como malware ou PHA se claramente colocarem em risco vários ou todos os dispositivos e usuários do Android.

As categorias de malware abaixo refletem nossa crença fundamental de que os usuários devem compreender como os dispositivos deles estão sendo usados e promover um ecossistema seguro que permita uma inovação robusta e uma experiência confiável do usuário.

Acesse o Google Play Protect para saber mais.

Acessos "backdoor"

É um código que permite a execução de operações indesejadas, potencialmente nocivas e controladas remotamente em um dispositivo.

Essas operações podem incluir comportamentos que fazem com que o app, binário, ou a modificação da framework se classifique em uma categoria de malware quando a execução é automática. Em geral, o termo "backdoor" descreve como uma operação potencialmente nociva pode ocorrer em um dispositivo. Portanto, ele não se enquadra exatamente em categorias como fraude de faturamento e spyware comercial. Como resultado disso, em algumas circunstâncias, determinados acessos "backdoor" podem ser considerados uma vulnerabilidade pelo Google Play Protect.

Fraude por faturamento

É um código que cobra o usuário automaticamente de forma enganosa.

As fraudes de faturamento de dispositivos móveis estão divididas entre SMS, chamada e cobrança.

Fraude de SMS
É um código que emite cobranças pelo envio de SMS premium sem o consentimento do usuário ou que tenta encobrir a atividade de SMS ao ocultar acordos de divulgação ou mensagens SMS da operadora de telefonia móvel com notificações sobre cobranças ou confirmações de assinaturas.

Alguns códigos, apesar de tecnicamente exporem o envio de SMS, também apresentam um comportamento adicional que inclui fraude de SMS. Os exemplos incluem ocultar partes de um acordo de divulgação do usuário para que não seja legível e bloquear intencionalmente as mensagens SMS da operadora de telefonia móvel informando o usuário sobre cobranças ou confirmando uma assinatura.

Fraude de chamada
É um código que emite cobranças ao realizar chamadas para números premium sem o consentimento do usuário.

Fraude de cobrança
É um código que engana o usuário para que ele assine ou compre conteúdos por meio da conta do celular.

A fraude de cobrança inclui qualquer tipo de faturamento, exceto SMS e chamadas premium. Por exemplo, o faturamento direto via operadora, o protocolo de aplicação sem fio (WAP, na sigla em inglês) e a transferência de créditos para dispositivos móveis. A fraude por WAP é um dos tipos mais comuns de fraude de cobrança. Ela pode levar os usuários a clicar em um botão ou em um WebView transparente e carregado de forma discreta. Ao realizar a ação, uma assinatura recorrente é iniciada, e

geralmente a mensagem por e-mail ou SMS é invadida para evitar que os usuários percebam a transação financeira.

Bin | 00:57:08 | Bin

Stalkerware

Código que coleta dados pessoais ou confidenciais do usuário de um dispositivo e os transmite a terceiros (outra empresa ou indivíduo) para monitoramento.

Os apps precisam incluir uma declaração em destaque adequada e receber consentimento conforme exigido pela política de dados do usuário .

Diretrizes para aplicativos de monitoramento

Os únicos apps de vigilância aceitáveis são os projetados ou comercializados exclusivamente para monitorar outro indivíduo, por exemplo, o monitoramento dos filhos pela família ou de funcionários individuais pela administração de uma empresa, desde que atendam totalmente aos requisitos descritos abaixo. Eles não podem ser usados para monitorar outras pessoas (um cônjuge, por exemplo), mesmo com conhecimento ou permissão delas e ainda que os apps exibam uma notificação contínua. Esses apps precisam usar a sinalização de metadados IsMonitoringTool no arquivo de manifesto para se designarem adequadamente como apps de monitoramento.

Os apps de monitoramento precisam atender a estes requisitos:

- Eles não podem se apresentar aos usuários como soluções de vigilância secreta ou de espionagem.
- Eles não podem usar técnicas de cloaking ou ocultar o comportamento de rastreamento nem tentar enganar os usuários sobre essa funcionalidade.
- Eles precisam apresentar aos usuários uma notificação contínua sempre que estiverem em execução e ter um ícone que os identifique facilmente.
- Os apps precisam divulgar a funcionalidade de monitoramento ou rastreamento na descrição da Google Play Store.
- Os apps e as páginas "Detalhes do app" no Google Play não podem apresentar meios de ativar nem acessar funcionalidades que violem esses termos, como links a um APK não compatível hospedado fora da plataforma.
- Os apps precisam obedecer às leis aplicáveis. Você é exclusivamente responsável por determinar a legalidade do app na localidade de destino.

Para mais informações, consulte o artigo da Central de Ajuda Uso da flag IsMonitoringTool .

Negação de serviço (DoS, na sigla em inglês)

É um código que, sem o conhecimento do usuário, executa um ataque de negação de serviço (DoS) ou faz parte de um ataque de DoS distribuído contra outros sistemas e recursos.

Por exemplo, isso pode acontecer ao enviar um volume alto de solicitações HTTP para gerar um carregamento excessivo em servidores remotos.

Componentes de downloads hostis

É um código que não é potencialmente nocivo por si só, mas que faz o download de outros PHAs.

Ele pode ser um componente de downloads hostil se:

- houver razões para acreditar que ele foi criado para espalhar PHAs e que fez download de PHAs ou contém um código que poderia fazer o download de PHAs e instalá-los; ou
- pelo menos 5% dos downloads feitos por ele são de PHAs com um limite mínimo de 500 downloads de apps observados, ou seja, 25 downloads de PHAs observados.

Os principais navegadores e apps de compartilhamento de arquivos não serão considerados componentes de downloads hostis desde que:

- não façam downloads sem a interação do usuário;
- todos os downloads de PHA sejam iniciados por usuários que deram consentimento.

Bin | 00:57:08 | Bin

Ameaça que não atinge o Android

É um código com ameaças que não atingem o Android.

Esses apps não causam danos ao usuário ou dispositivo Android, mas têm componentes potencialmente nocivos a outras plataformas.

Phishing

É um código que finge ser de uma fonte confiável, solicita credenciais de autenticação do usuário ou informações de faturamento e envia esses dados a terceiros. Esta categoria também se aplica a código que intercepta a transmissão de credenciais do usuário.

Alguns alvos comuns de phishing são credenciais bancárias, números de cartão de crédito e credenciais de contas on-line para redes sociais e jogos.

Abuso de privilégios elevados

É um código que compromete a integridade do sistema ao romper o sandbox do app, conseguindo privilégios elevados ou alterando ou desabilitando o acesso a funções centrais ligadas à segurança.

Por exemplo:

- Um app que viola o modelo de permissões do Android ou rouba credenciais (como tokens OAuth) de outros apps
- Apps que abusam de recursos para impedir que sejam desinstalados ou interrompidos
- Um app que desativa o SELinux

Apps com escalonamento de privilégios que dão acesso root a dispositivos sem a permissão do usuário são considerados apps de acesso root.

Ransomware

É um código que toma o controle parcial ou total de um dispositivo ou dados de um dispositivo e exige que o usuário faça um pagamento ou realize alguma ação para recuperá-lo.

Alguns tipos de ransomware criptografam dados no dispositivo e exigem o pagamento para descriptografá-los e/ou aproveitam os recursos de administração do dispositivo para que não possa ser removido por um usuário típico. Por exemplo:

- Bloquear um usuário do próprio dispositivo e exigir dinheiro para devolver o controle ao usuário
- Criptografar dados no dispositivo e exigir o pagamento para descriptografar os dados
- Aproveitar os recursos do Gerenciador de políticas do dispositivo e bloquear a remoção pelo usuário

O código distribuído com o dispositivo que tenha como objetivo principal o gerenciamento subsidiado do dispositivo pode ser excluído da categoria de ransomware, desde que cumpra com os requisitos de bloqueio e gerenciamento seguros e de divulgação e consentimento do usuário adequados.

Acesso root

É um código que faz root no dispositivo.

Há uma diferença entre códigos de root maliciosos e não maliciosos. Por exemplo, apps de root não maliciosos permitem que o usuário saiba antecipada [illegible] dispositivo e não executam outras ações potencialmente nocivas que se aplicam a outras categorias de PHA.

Os apps de root maliciosos não informam o usuário que farão root no dispositivo ou informam antecipadamente, mas também executam ações que se aplicam a outras categorias de PHA.

Spam

É um código que envia mensagens não solicitadas aos contatos dos usuários ou usa o dispositivo para o redirecionamento de spam de e-mail.

Spyware

O spyware é um comportamento, código ou aplicativo malicioso que coleta, extrai ou compartilha dados do dispositivo ou do usuário que não têm relação com as funcionalidades que obedecem à política.

Um código ou comportamento malicioso que pode ser considerado espionagem ou extrai dados sem o devido consentimento ou aviso também é identificado como spyware.

Confira alguns exemplos de violações de spyware:

- Gravação de áudio e de chamadas telefônicas
- Roubo de dados do app
- Um app com código malicioso de terceiros (por exemplo, um SDK) que transmite dados para fora do dispositivo de forma inesperada ao usuário e/ou sem o devido consentimento ou aviso

Todos os apps precisam obedecer a todas as Políticas do programa para desenvolvedores do Google Play, incluindo as políticas de dados de dispositivos e usuários como Software indesejado para dispositivos móveis, Dados do usuário, Permissões e APIs que acessam informações sensíveis e Requisitos de SDK.

Cavalo de Troia

É um código que parece ser benigno, como um jogo que afirma ser só um jogo, mas que realiza ações indesejáveis contra o usuário.

Essa classificação geralmente é usada em combinação com outras categorias de PHA. Um cavalo de Troia tem um componente inofensivo e um nocivo oculto. Por exemplo, um jogo que envia mensagens SMS premium do dispositivo em segundo plano e sem o conhecimento do usuário.

Observação sobre apps incomuns

Apps novos e raros poderão ser classificados como incomuns se o Google Play Protect não tiver informações suficientes para considerá-los seguros. Isso não significa que o app é necessariamente nocivo, mas sim que é preciso uma avaliação mais profunda para que seja classificado como seguro.

Observação sobre a categoria "backdoor"

A classificação na categoria de malware "backdoor" depende de como o código funciona. Uma condição necessária para que qualquer código seja classificado como de "backdoor" é que, ao ser executado automaticamente, ele permita comportamentos classificados em uma das outras categorias de malware. Por exemplo, se um app permitir o carregamento dinâmico de código, e o

código carregado dinamicamente extrai mensagens de texto, o app será classificado como malware "backdoor".

Porém, se um app permitir a execução arbitrária de c[illegible]ivos para acreditar que esse código tenha sido adicionado com o objetivo de realizar um comportamento malicioso, o app será considerado vulnerável, e não malware "backdoor". Nesse caso, será solicitado que o desenvolvedor crie um patch para corrigir o problema.

Bin | 00:57:08 | Bin

Riskware

São aplicativos que utilizam diversas técnicas de evasão para disponibilizar funcionalidades diferentes ou falsas para os usuários. Esses apps se disfarçam como jogos ou aplicativos legítimos de modo a parecerem inofensivos para as app stores e usuários, além de usarem técnicas como ofuscação, carregamento dinâmico de código ou cloaking para revelar o conteúdo potencialmente nocivo.

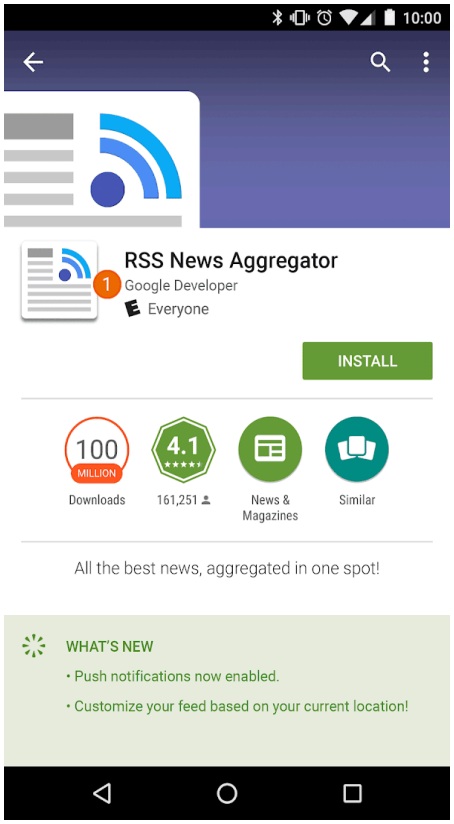
O riskware é semelhante a outras categorias de PHA, principalmente os cavalos de troia, e a principal diferença está nas técnicas usadas para ocultar as atividades mal-intencionadas.

Falsificação de identidade

Não permitimos apps que enganem os usuários ao se passarem por outra pessoa (por exemplo, outro desenvolvedor, empresa, entidade) ou outro app. Não insinue que seu app está relacionado ou autorizado por uma pessoa sem que esteja. Tenha cuidado para não usar ícones, descrições, títulos ou elementos no app que possam enganar os usuários sobre o relacionamento do app com outra pessoa ou outro app.

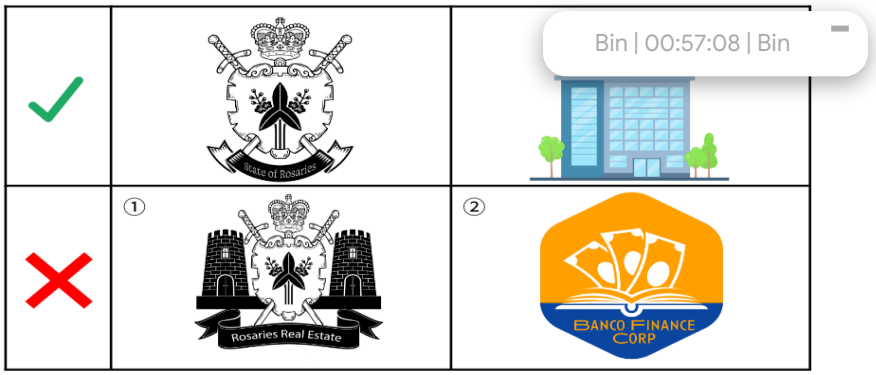
Veja alguns exemplos de violações comuns:

- Desenvolvedores que indicam falsamente uma relação com outra empresa / desenvolvedor / entidade / organização



① O nome do desenvolvedor listado para este app sugere uma relação oficial com o Google, apesar de tal relação não existir.

- Apps com ícones e títulos que sugerem falsamente um relacionamento com outra empresa / desenvolvedor / entidade / organização



① O app usa um emblema nacional e induz os usuários a acreditar que ele é afiliado ao governo.
② O app copia o logotipo de uma entidade empresarial para sugerir falsamente que é um app oficial da empresa.

- Títulos e ícones de apps que são tão semelhantes aos de produtos ou serviços atuais que podem enganar os usuários

① O app usa o logotipo de um site de criptomoeda famoso como ícone para sugerir que é o site oficial.
② O app copia o personagem e o título de um programa de TV famoso no ícone e induz os usuários a pensar que ele é afiliado ao programa.

- Apps que alegam falsamente ser o app oficial de uma entidade estabelecida (títulos como "App oficial do Justin Bieber" não são permitidos sem os direitos ou as permissões necessárias)

- Apps que violam as Diretrizes da marca Android

Para perguntas frequentes sobre a política contra falsificação de identidade, consulte este artigo da Central de Ajuda.

Software indesejado para dispositivos móveis

No Google, acreditamos que, se o foco está no usuário, todo o resto é consequência. Nos princípios de software e na política de software indesejado, apresentamos recomendações gerais para softwares que proporcionam uma ótima experiência [illegible] baseia na política de software indesejado do Google e descreve os princí[illegible] da Google Play Store. Qualquer software que viole tais princípios é potencialmente prejudicial para a experiência do usuário. Nós tomaremos as medidas para proteger esses usuários.

Bin | 00:57:08 | Bin

Conforme mencionado na política de software indesejado, descobrimos que a maioria dos softwares indesejados tem uma ou mais das mesmas características básicas:

- São enganosos, prometem um valor que não é fornecido.
- Tentam enganar os usuários para que estes os instalem ou aproveitam a instalação de outro programa.
- Não informam ao usuário todas as suas funções principais e significativas.
- Afetam o sistema do usuário de formas inesperadas.
- Coletam ou transmitem informações particulares sem o conhecimento dos usuários.
- Coletam ou transmitem informações particulares sem um tratamento seguro (por exemplo, transmissão por HTTPS).
- Agrupam-se com outro software e sua presença não é divulgada.

Em dispositivos móveis, o software é um código na forma de um app, binário, modificação de framework etc. Para evitar softwares prejudiciais ao ecossistema de software ou à experiência do usuário, tomaremos medidas em relação ao código que viola esses princípios.

A seguir, desenvolvemos a política de software indesejado para estender sua aplicabilidade a softwares para dispositivos móveis. Do mesmo modo, continuaremos refinando a política de software indesejado para dispositivos móveis para lidar com novos tipos de abuso.

Comportamento transparente e divulgações claras

Todos os códigos precisam cumprir as promessas feitas ao usuário. Os apps precisam fornecer todas as funcionalidades informadas. Os apps não podem confundir os usuários.

- Os apps precisam ser claros sobre a função e os objetivos.
- Explique de forma explícita e clara ao usuário quais alterações serão feitas pelo app no sistema. Permita que os usuários analisem e aprovem todas as opções e mudanças significativas da instalação.
- O software não pode deturpar o estado do dispositivo para o usuário, por exemplo, alegando que o sistema está em estado crítico de segurança ou infectado com vírus.
- Não use atividades inválidas criadas para aumentar o tráfego de anúncios e/ou as conversões.
- Não permitimos apps que enganem os usuários ao se passarem por outra pessoa (por exemplo, outro desenvolvedor, empresa, entidade) ou outro app. Não insinue que seu app está relacionado ou autorizado por uma pessoa sem a permissão dela.

Exemplos de violação:

- Fraude de anúncio
- Engenharia social

Proteger a privacidade e os dados do usuário

Divulgue com clareza e transparência o acesso, o uso, a coleta e o compartilhamento dos dados pessoais e sensíveis do usuário. Os usos dos dados do usuário precisam estar de acordo com todas as políticas relevantes sobre o assunto, quando aplicáveis, e é necessário tomar todas as precauções para proteger os dados.

Todos os apps precisam obedecer a todas as Políticas do programa para desenvolvedores do Google Play, incluindo as de dados de dispositivos e usuários, como Dados do usuário, Permissões e APIs que acessam informações sensíveis, Spyware e Requisitos de SDK.

- Não solicite ou induza os usuários a desativarem as proteções de segurança do dispositivo, como o Google Play Protect. Por exemplo, não ofereça mais recursos ou prêmios aos usuários em troca da desativação do Google Play Protect.

Bin | 00:57:08 | Bin

Não prejudique a experiência em dispositivos móveis

A experiência do usuário precisa ser simples, fácil de entender e se basear em escolhas claras feitas pelo usuário. Ela precisa apresentar uma proposta de valor clara para o usuário e não interromper a experiência divulgada ou esperada.

- Não exiba anúncios aos usuários de maneiras inesperadas que prejudiquem ou interfiram na usabilidade das funções do dispositivo nem os exiba fora do ambiente do app acionador sem que eles sejam facilmente dispensáveis e tenham o consentimento e a atribuição adequados.
- Os apps não podem interferir em outros apps nem na usabilidade do dispositivo.
- A desinstalação, quando aplicável, precisa ser clara.
- O software para dispositivos móveis não pode imitar solicitações do SO do dispositivo ou de outros apps. Não suprima alertas de outros apps ou do sistema operacional para o usuário, especialmente aqueles que informam sobre alterações no SO.

Exemplos de violação:

- Anúncios invasivos
- Uso não autorizado ou imitação de funcionalidade do sistema

---

Componente de download hostil

É um código que não é um software indesejado, mas faz download de outro software indesejado para dispositivos móveis (MUwS, na sigla em inglês).

Ele pode ser um componente de downloads hostil se:

- há razões para acreditar que ele foi criado para espalhar MUwS e que fez ou contém um código que poderia fazer o download de MUwS e instalá-los; ou
- pelo menos 5% dos downloads de app feitos por ele são de MUwS com um limite mínimo de 500 observados (ou seja, 25 downloads de MUwS observados).

Os principais navegadores e apps de compartilhamento de arquivos não serão considerados componentes de downloads hostis desde que:

- não façam downloads sem a interação do usuário; e
- todos os downloads de software sejam iniciados por usuários que deram consentimento.

Fraude de anúncios

A fraude de anúncios é estritamente proibida. As interações de anúncios geradas com a finalidade de fazer uma rede de publicidade acreditar que o tráfego é do interesse autêntico do usuário são fraudes de anúncios, uma forma de tráfego inválido. A fraude de anúncios pode ser realizada por desenvolvedores que implementam anúncios de maneiras não permitidas, como exibir anúncios ocultos, clicar automaticamente em anúncios, alterar ou modificar informações e se aproveitar de outras ações não humanas (indexadores, bots etc.) ou atividade humana projetada para produzir tráfego de anúncios inválidos. O tráfego inválido e a fraude de anúncios são prejudiciais para os anunciantes, os desenvolvedores e os usuários, além de gerar perda de confiança em longo prazo no ecossistema de anúncio para dispositivos móveis.

Veja alguns exemplos de violações comuns:

- Um app que renderiza anúncios que não são visíveis para o usuário

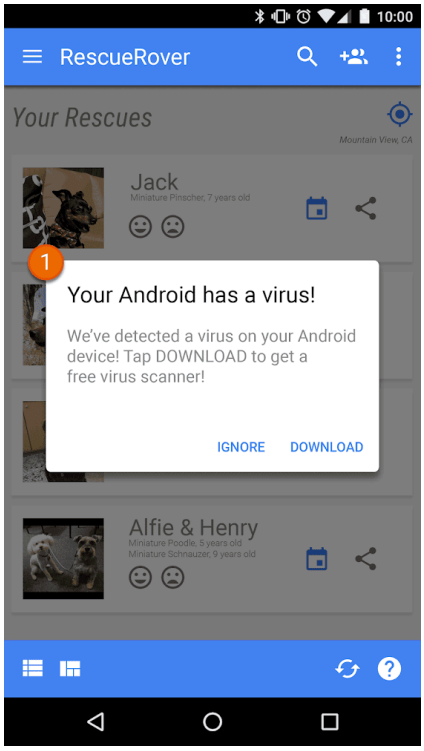
- Um app que gera cliques em anúncios automaticamente sem a intenção do usuário ou que produz tráfego de rede equivalente para fornecer créditos de cliques de maneira fraudulenta
- Um app que envia cliques falsos de atribuição de i[illegible]nentos por instalações que não se originaram na rede do rem[illegible]
- Um app que exibe anúncios pop-up quando o usuário não está na interface do app
- Declarações falsas do inventário de anúncios por um app, por exemplo, um app que comunica a redes de publicidade que está em execução em um dispositivo iOS quando, na verdade, está em um dispositivo Android; um app que declara incorretamente o nome do pacote que está sendo monetizado

Uso não autorizado ou imitação de funcionalidade do sistema

Apps ou anúncios que imitem funcionalidades do sistema ou interfiram no funcionamento delas, como notificações ou avisos, não são permitidos. As notificações no nível do sistema só podem ser usadas para os recursos integrais de um app, como quando um app de uma companhia aérea notifica os usuários sobre promoções especiais ou quando um jogo notifica os usuários sobre as próprias promoções.

Veja alguns exemplos de violações comuns:

- Apps ou anúncios exibidos por meio de uma notificação ou um alerta do sistema:



① A notificação do sistema exibida neste app está sendo usada para veicular um anúncio.

Para ver mais exemplos relacionados, consulte a política de anúncios.

Engenharia social

Não permitimos apps que finjam ser outro app com a intenção de induzir os usuários a realizar ações que pretendiam fazer no app confiável original.

Monetização e anúncios

O Google Play é compatível com diversas estratégias de monetização para beneficiar desenvolvedores e usuários. Essas estratégias incluem distribuição pa[illegible] sinaturas e modelos baseados em anúncios. Para garantir a melhor experiência do usuário, é necessário obedecer a essas políticas.

Bin | 00:57:08 | Bin

Pagamentos

1. Os desenvolvedores que cobram pelo download de apps no Google Play precisam usar o sistema de faturamento da plataforma como forma de pagamento dessas transações.
2. Os apps distribuídos no Google Play que solicitam ou aceitam pagamento pelo acesso a recursos ou serviços, incluindo funcionalidades do app, conteúdos ou produtos digitais (coletivamente, "compras no app"), precisam usar o sistema de faturamento do Google Play para essas transações, a menos que as seções 3, 8 ou 9 sejam aplicáveis.

   Exemplos de recursos ou serviços de apps que exigem o uso do sistema de faturamento do Google Play incluem, entre outros, compras no app de:

   - itens (como moedas virtuais, vidas extras, mais tempo de jogo, itens complementares, personagens e avatares);
   - serviços de assinatura (como de exercícios físicos, jogos, encontros, educação, música, vídeo, upgrades e outros conteúdos);
   - conteúdo ou funcionalidade do app (como uma versão sem anúncios de um app ou novos recursos indisponíveis na versão gratuita);
   - software e serviços em nuvem (como serviços de armazenamento de dados, software de produtividade empresarial e software de gerenciamento financeiro).

3. O sistema de faturamento do Google Play não pode ser usado quando:
   a. o pagamento é principalmente:
      - para a compra ou a locação de produtos físicos (como mantimentos, roupas, utensílios domésticos, eletrônicos);
      - para a compra de serviços físicos (como serviços de transporte, limpeza, passagem aérea, academia, entrega de comida, ingressos para eventos ao vivo);
      - uma remessa referente a uma fatura de cartão de crédito ou de serviços públicos (como serviços de cabo e telecomunicações).

   b. o pagamento está relacionado a pagamentos entre pessoas, leilões on-line e doações isentas de tributos;
   c. o pagamento é para conteúdo ou serviços que facilitam jogos de azar on-line, conforme descrito na seção Apps de jogos de azar da Política de jogos, concursos e jogos de azar com dinheiro real;
   d. o pagamento está relacionado a qualquer categoria de produto considerada inaceitável de acordo com as Políticas de conteúdo da Central de pagamentos do Google.

   Observação: em alguns mercados, oferecemos o Google Pay para apps que vendem produtos e/ou serviços físicos. Para saber mais, acesse a Página do desenvolvedor do Google Pay .

4. Exceto nas condições descritas nas seções 3, 8 e 9, os apps não podem levar usuários a formas de pagamento que não sejam o sistema de faturamento do Google Play. Essa proibição inclui, entre outras opções, direcionar os usuários a outras formas de pagamento via:
   - páginas "Detalhes do app" no Google Play;
   - promoções no app relacionadas a conteúdo comprável;
   - WebViews, botões, links, mensagens, anúncios ou outras calls-to-action no app;

- fluxos de interface do usuário no app, incluindo a criação de contas ou inscrições que levam os usuários de um app para uma forma de pagamento diferente do sistema de faturamento do Google Play como parte do processo.

Bin | 00:57:08 | Bin

5. As moedas virtuais no app só poderão ser usadas dentro do app ou jogo em que foram compradas.
6. Os desenvolvedores precisam informar os usuários de maneira clara e precisa sobre os termos e os preços do app ou sobre os recursos ou assinaturas no app oferecidos para compra. Os preços no app precisam corresponder aos preços exibidos na interface de faturamento do Google Play voltada para o usuário. Se a descrição do produto no Google Play mencionar recursos no app que exijam uma cobrança específica ou adicional, essa descrição precisará notificar claramente os usuários de que é necessário pagar para ter acesso a esses recursos.
7. Os apps e jogos que oferecem mecanismos para receber itens virtuais aleatórios de uma compra, incluindo, mas não se limitando a, "loot boxes", precisam declarar claramente as chances de receber esses itens antes e perto de efetuarem o pagamento.
8. Os desenvolvedores que atendem usuários em países/regiões qualificadas podem oferecer um sistema alternativo de faturamento no app. Para isso, os usuários devem se inscrever no programa aplicável e concordar com os termos adicionais e os requisitos do programa.

↵

9. Os desenvolvedores podem direcionar usuários em países/regiões qualificados para fora do app de acordo com os requisitos do programa. Para isso, os desenvolvedores precisam se inscrever no programa aplicável e concordar com os termos adicionais e os requisitos do programa.

Observação: para ver os cronogramas e as Perguntas frequentes sobre esta política, acesse nossa Central de Ajuda.

Anúncios

Para manter uma experiência de qualidade, consideramos o conteúdo do anúncio, o público-alvo, a experiência do usuário, o comportamento, bem como a segurança e a privacidade. Consideramos anúncios e ofertas associadas como parte do seu app. Eles também precisam obedecer a todas as outras políticas do Google Play. Além disso, temos requisitos adicionais para anúncios que geram receita em apps voltados para crianças no Google Play.

Você também pode saber mais sobre nossas políticas de promoção de apps e páginas "Detalhes do app" neste link, incluindo como lidar com práticas de promoção enganosas.

Conteúdo do anúncio

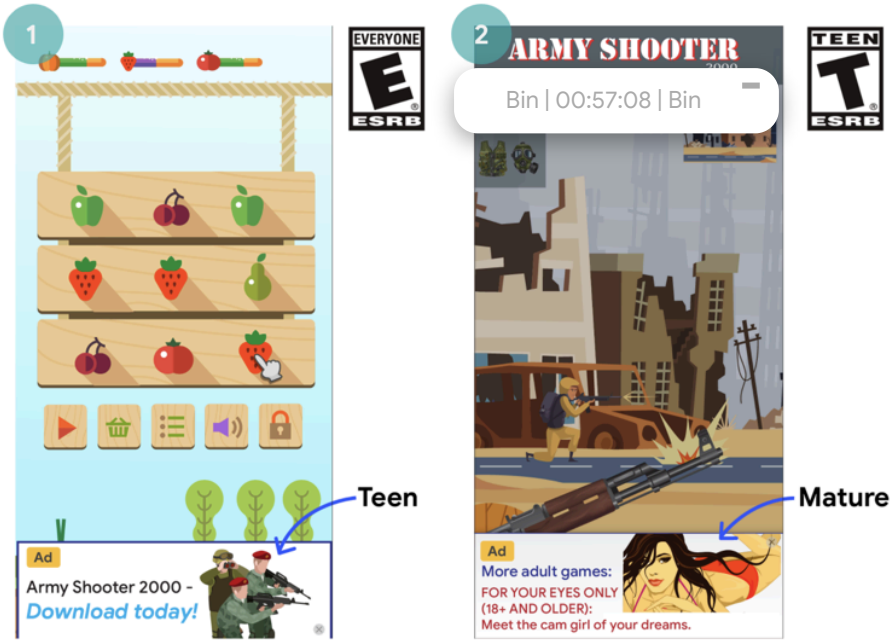
Os anúncios e ofertas associadas fazem parte do seu app e devem seguir nossas políticas de Conteúdo restrito. Apps de jogos de azar estão sujeitos a outros requisitos.

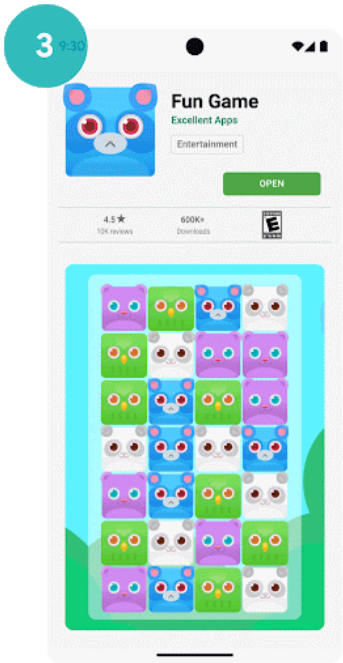
Anúncios inadequados

Mesmo que o conteúdo obedeça às nossas políticas, os anúncios e as ofertas associadas exibidos no app (por exemplo, publicidade para o download de outro app) precisam ser adequados à classificação do conteúdo .

Veja alguns exemplos de violações comuns:

- Anúncios inadequados para a classificação do conteúdo do app





① Este anúncio é inadequado (Adolescente) para a classificação do conteúdo (Todos).
② Este anúncio é inadequado (Adulto) para a classificação do conteúdo (Adolescente).
③ A oferta do anúncio (promoção do download de um app para adultos) é inadequada para a classificação do conteúdo do jogo em que o anúncio foi exibido (Todos).

Requisitos de anúncios para famílias

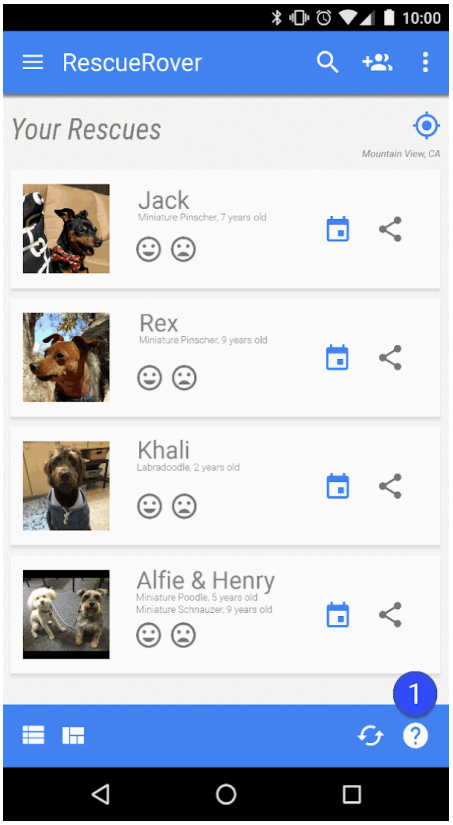
Se você gera receita com um app destinado a crianças no Google Play, é importante que ele siga os requisitos da política de anúncios e monetização para famílias.

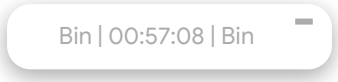
Anúncios enganosos

Os anúncios não podem simular nem imitar a interface do usuário de qualquer recurso do app, como os elementos de aviso ou de notificação de um sistema operacional. É preciso estar claro para o usuário qual app veicula cada anúncio.

Veja alguns exemplos de violações comuns:

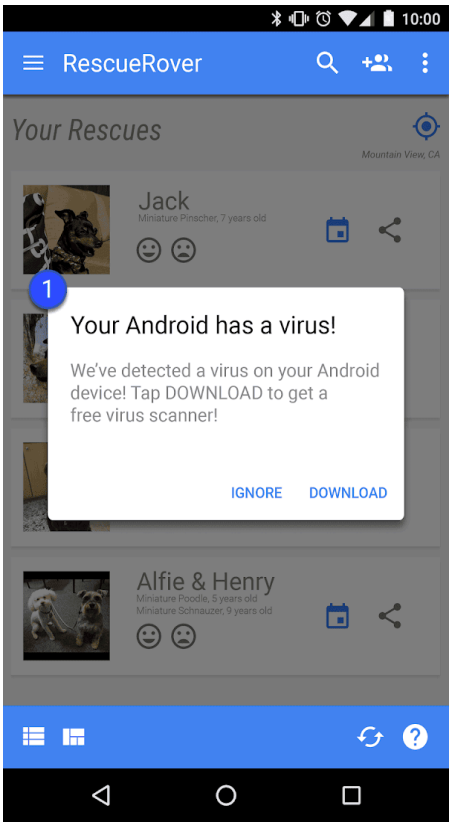
- Anúncios que imitam a interface do usuário de um app:

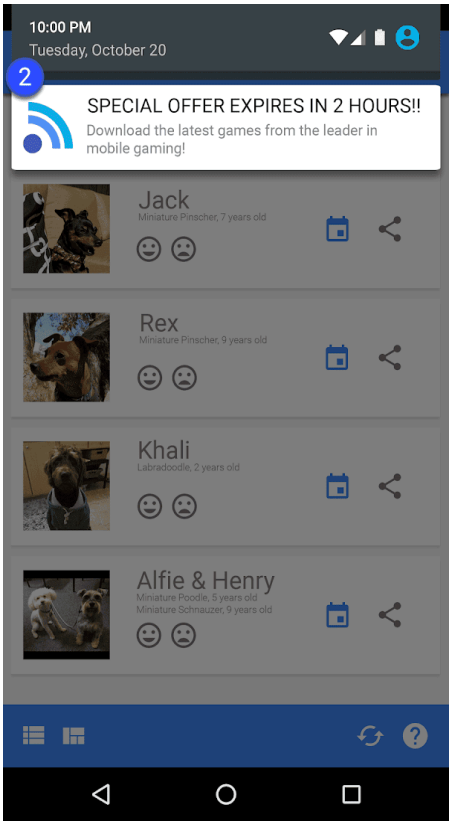


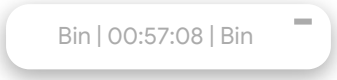


① O ícone de interrogação neste app é um anúncio que leva o usuário para uma página de destino externa.

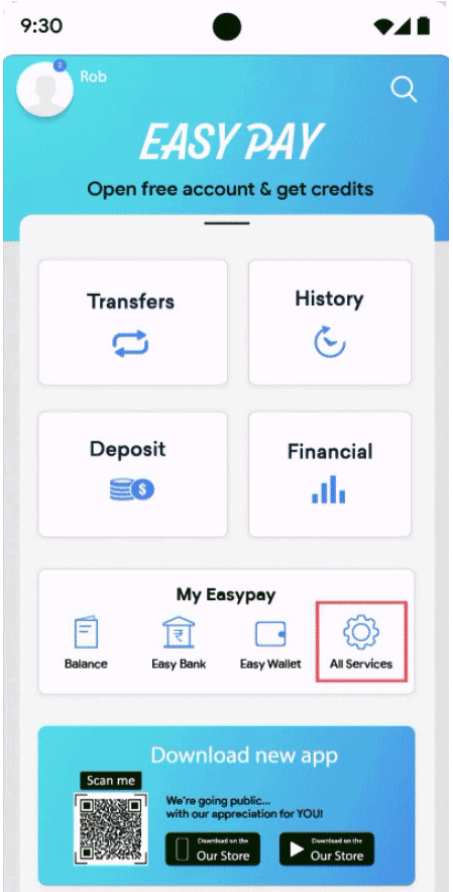
- Anúncios que imitam uma notificação do sistema:







① ② Os exemplos acima mostram anúncios que imitam várias notificações do sistema.



① O exemplo acima mostra uma seção que imita outros recursos, mas só leva os usuários a um ou mais anúncios.

Anúncios invasivos

Os anúncios invasivos são exibidos aos usuários de maneiras inesperadas e podem resultar em cliques acidentais ou prejudicar ou interferir na usabilidade das funções do dispositivo.

É proibido forçar um usuário a clicar em um anúncio [illegible] is para fins publicitários antes de usar o app por completo. Os a[illegible]s dentro do app que os veicula e não podem interferir em outros apps e anúncios ou na operação do dispositivo, incluindo portas e botões do sistema ou do dispositivo. Isso inclui sobreposições, recursos complementares e blocos de anúncios em forma de widget. Caso seu app exiba anúncios ou outra publicidade que interfira no uso normal, é necessário que eles sejam fáceis de dispensar sem qualquer prejuízo aos usuários.

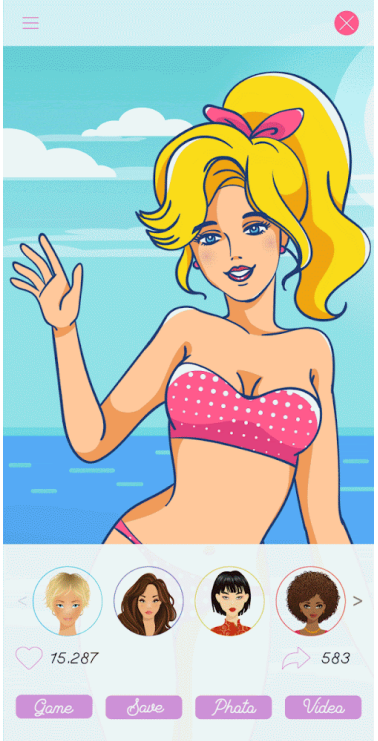
Bin | 00:57:08 | Bin

Veja alguns exemplos de violações comuns:

- Anúncios que ocupam a tela inteira ou interferem na utilização normal e não oferecem um meio claro de dispensar o anúncio:

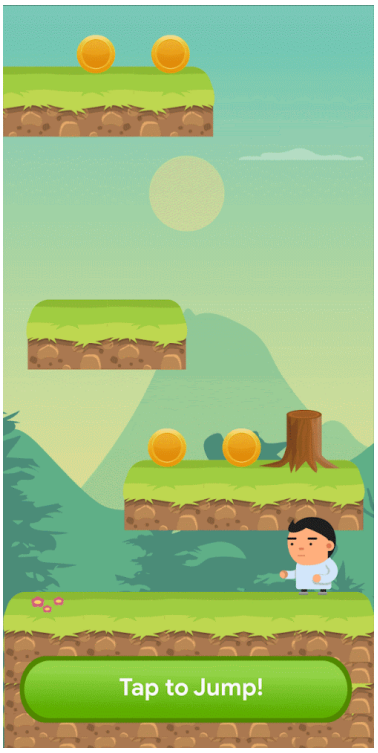
① Este anúncio não tem um botão para dispensar.

- Anúncios que forçam o usuário a clicar usando um falso botão "Dispensar" ou que aparecem repentinamente em áreas do app, mesmo que o usuário toque em outra função:



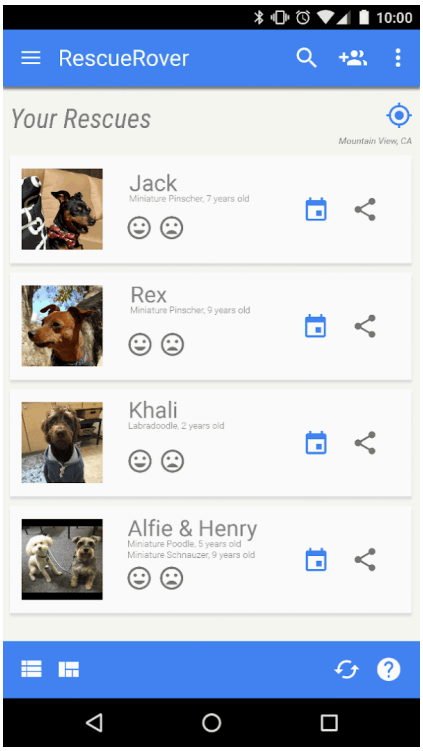
Bin | 00:57:08 | Bin

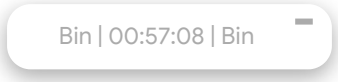
① Este anúncio usa um botão "Dispensar" falso.



② Este anúncio aparece repentinamente em áreas em que o usuário está acostumado a tocar para funções no app.

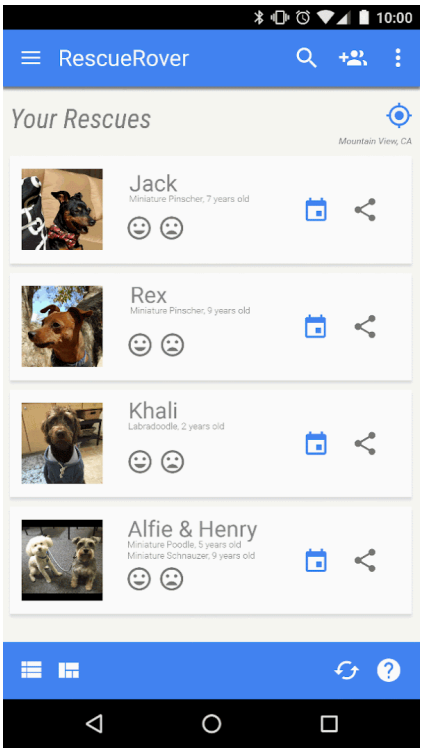
- Anúncios que são exibidos fora do app em que são veiculados:





① O usuário sai do app e vai para a tela inicial do dispositivo. De repente, um anúncio aparece nessa tela.

- Anúncios que são acionados pelo botão home ou por outros recursos projetados especificamente para sair do app:



① O usuário tenta sair do app e navegar até a tela inicial, mas, em vez disso, o fluxo esperado é interrompido por um anúncio.

Melhores experiências de anúncios

Os desenvolvedores precisam obedecer às diretrizes de anúncios a seguir para garantir experiências de alta qualidade aos usuários nos apps do Google Play. Os anúncios não podem ser exibidos das seguintes formas inesperadas para os usuários:

- Não são permitidos anúncios intersticiais em tela cheia de nenhum formato (vídeo, GIF, estáticos etc.) exibidos inesperadamente, geralmente quando o usuário optou por fazer outra coisa.
  - Não são permitidos anúncios exibidos em jogos m segmento de conteúdo.
  - Não são permitidos anúncios intersticiais em vídeo em tela cheia exibidos antes da tela de carregamento do app (tela de apresentação).
- Não são permitidos anúncios intersticiais em tela cheia de nenhum formato que não possam ser fechados após 15 segundos. Intersticiais em tela cheia com permissão ou que não interrompam as ações dos usuários (por exemplo, após a tela de pontuação de um jogo) podem durar mais de 15 segundos.

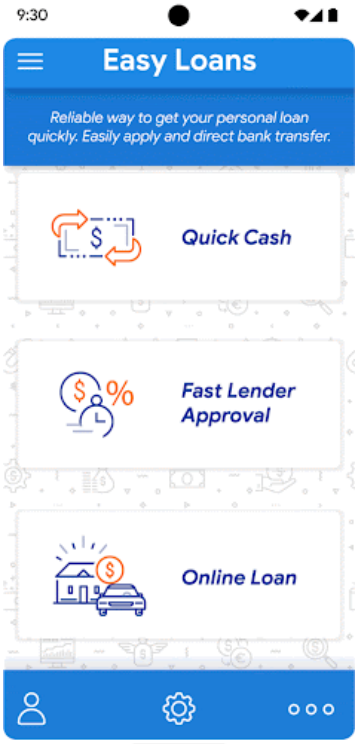
Esta política não se aplica a anúncios premiados explicitamente ativados pelos usuários, por exemplo: um anúncio que os desenvolvedores oferecem explicitamente aos usuários em troca do desbloqueio de um conteúdo ou recurso específico do jogo. Esta política também não se aplica a monetização e publicidade que não interfiram no uso normal do app ou jogo, por exemplo: conteúdo em vídeo com anúncios integrados ou anúncios de banner que não sejam em tela cheia.

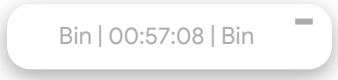
Estas diretrizes são inspiradas pelas Better Ads Experiences . Para mais informações sobre as Better Ads Experiences, consulte a Coalition for Better Ads (links em inglês).

Veja alguns exemplos de violações comuns:

- Anúncios inesperados exibidos durante o jogo ou no início de um segmento de conteúdo, por exemplo: após o usuário clicar em um botão e antes que a ação pretendida pelo clique tenha efeito. Esses anúncios são inesperados, porque os usuários esperam começar um jogo ou interagir com o conteúdo.

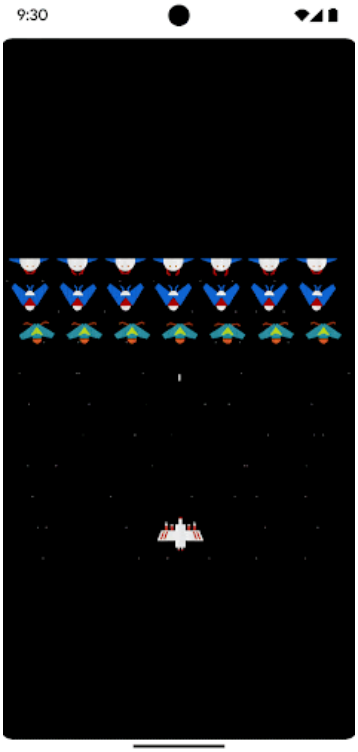
① Um anúncio estático inesperado aparece durante o jogo no início de uma fase.





② Um anúncio em vídeo inesperado aparece no início de um segmento de conteúdo.

- Um anúncio em tela cheia que aparece durante o jogo e não pode ser fechado após 15 segundos.



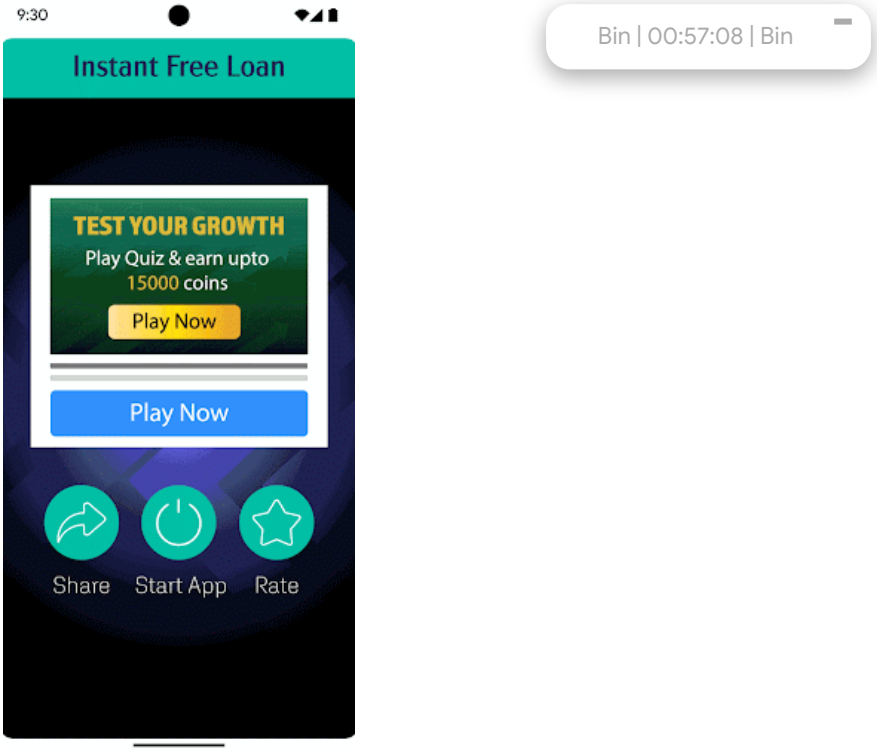
① Um anúncio intersticial aparece durante o jogo e não oferece aos usuários a opção de pular em 15 segundos.

Apps feitos para veicular anúncios

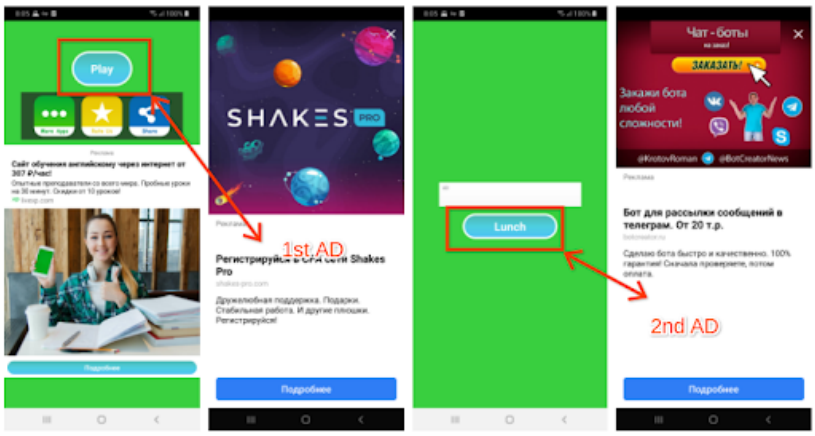
Não são permitidos apps que exibem anúncios intersticiais repetidamente para atrapalhar a interação e as tarefas no app.

Veja alguns exemplos de violações comuns:

- Apps em que um anúncio intersticial é exibido de maneira consecutiva após uma ação do usuário, incluindo, mas não se limitando a, cliques, ações de deslizar etc.



① A primeira página do app tem vários botões para interação. Quando o usuário clica em **Iniciar app** para usá-lo, um anúncio intersticial é exibido. Depois que o anúncio é fechado, o usuário volta ao app e clica em **Serviço** para usar o serviço, mas outro anúncio intersticial é exibido.



② Na primeira página, o usuário é conduzido a clicar em **Jogar**, porque é o único botão disponível para usar o app. Quando ele clica, um anúncio intersticial é exibido. Depois que o anúncio é fechado, o usuário clica em **Iniciar**, que é o único botão exibido, e outro intersticial aparece.

Monetização da tela de bloqueio

Os apps não podem apresentar anúncios ou recursos que gerem receita a partir da tela bloqueada de um dispositivo, a menos que o único objetivo do app seja oferecer o serviço de tela de bloqueio.

Fraude de anúncio

A fraude de anúncios é estritamente proibida. Para mais informações, consulte nossa Política contra fraude de anúncios.

Uso de dados de local para publicidade

Os apps que aproveitam o uso dos dados de local do dispositivo com base em permissão para exibir anúncios estão sujeitos à política de Informações pessoais e confidenciais e aos seguintes requisitos:

- O uso ou coleta de dados de local do dispositivo c Bin | 00:57:08 | Bin ins publicitários precisa estar claro para o usuário e documentado na Política de Privacidade obrigatória do app. Isso inclui links para as Políticas de Privacidade relevantes da rede de publicidade que abordem o uso desse tipo de dados.
- De acordo com os requisitos de permissões de localização, essas permissões só podem ser solicitadas para implementar recursos ou serviços atuais no app, e não apenas para uso publicitário.

Uso do ID de publicidade do Android

A versão 4.0 do Google Play Services introduziu novas APIs e um ID para ser usado por provedores de análise e publicidade. Os termos para o uso desse ID estão disponíveis abaixo.

- **Uso**. O identificador de publicidade do Android (AAID) só pode ser utilizado para publicidade e análise de usuário. O status das configurações "Desativar publicidade com base em interesses" e "Desativar a Personalização de anúncios" precisa ser verificado em cada acesso do ID.
- **Associação a informações de identificação pessoal ou outros identificadores**.
  - Uso de publicidade: o identificador de publicidade pode não estar conectado a identificadores de dispositivo permanentes (por exemplo: SSAID, endereço MAC, IMEI etc.) para qualquer finalidade publicitária. O identificador de publicidade só pode ser conectado a informações de identificação pessoal com o consentimento explícito do usuário.
  - Uso para análises: o identificador de publicidade não pode ser conectado a informações de identificação pessoal ou associado a identificadores de dispositivo permanentes (por exemplo: SSAID, endereço MAC, IMEI etc.) para finalidades de análise. Leia a política de dados do usuário para mais orientações sobre identificadores de dispositivos permanentes.
- **Respeito às seleções dos usuários**.
  - Se for redefinido, o novo identificador de publicidade não poderá ser vinculado a outro anterior nem a dados derivados desse identificador sem o consentimento explícito do usuário.
  - É preciso respeitar a configuração "Desativar publicidade com base em interesses" ou "Desativar a Personalização de anúncios" do usuário. Se um usuário tiver ativado essa configuração, o identificador de publicidade não poderá ser usado na criação de perfis de usuários para fins publicitários ou para segmentação de usuários com publicidade personalizada. As atividades permitidas incluem publicidade contextual, limite de frequência, acompanhamento de conversões, geração de relatórios, segurança e detecção de fraudes.
  - Em dispositivos mais novos, quando um usuário exclui o identificador de publicidade do Android, o identificador é removido. Qualquer tentativa de acessar o identificador receberá uma sequência de zeros. Um dispositivo sem um identificador de publicidade não pode ser conectado a dados vinculados ou derivados de um identificador de publicidade anterior.
- **Transparência aos usuários**. A coleta e o uso do identificador de publicidade e o cumprimento destes termos precisam ser divulgados aos usuários em uma notificação de privacidade adequada às normas legais. Para saber mais sobre nossos padrões de privacidade, consulte nossa política de Dados do usuário .
- **Concordância com os Termos de Uso**. O identificador de publicidade só pode ser utilizado de acordo com a Política do programa para desenvolvedores do Google Play, tanto por você quanto por qualquer parte com quem ele seja compartilhado em função dos seus negócios. Todos os apps enviados ou publicados no Google Play precisam usar o ID de publicidade (quando disponível em um dispositivo) em vez de outros identificadores de dispositivo para fins publicitários.

Para mais informações, consulte nossa política de dados do usuário.

Inscrições

Os desenvolvedores de apps não podem enganar os usuários em relação a serviços ou conteúdos de assinatura. Criar uma comunicação clara é essencial em todas as promoções no app, telas de apresentação e telas de escolha dos planos de assin[illegible] que sujeitem os usuários a experiências de compra enganosas ou ma[illegible] as ou assinaturas no app). Se você oferecer benefícios de assinatura, eles precisam ser verdadeiros e precisos, sem deturpar nenhum aspecto da assinatura.

Bin | 00:57:08 | Bin

Você precisa ser transparente sobre esse produto, o que inclui divulgar de modo claro e explícito os termos, o custo da assinatura, a frequência do ciclo de faturamento, os termos da renovação automática, a necessidade de fazer uma assinatura para usar o app (se houver) e qualquer outro dado pertinente. Os usuários não podem ter que realizar ações adicionais para acessar as informações.

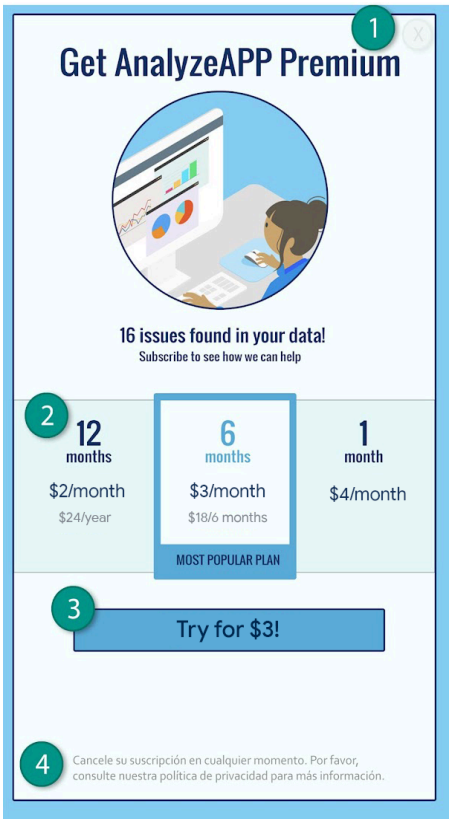
As assinaturas precisam fornecer valor contínuo ou recorrente aos usuários durante todo o período e não podem ser usadas para oferecer benefícios únicos, como SKUs de quantias de créditos ou moedas no app ou boosters de uso único para jogos. É possível oferecer incentivos ou bônus promocionais, desde que apenas complementem o valor contínuo ou recorrente oferecido durante o período da assinatura. Os produtos que não oferecem valor contínuo e recorrente precisam usar um produto no app, e não um produto de assinatura.

Benefícios pontuais não podem ser apresentados nem vendidos como assinatura. Isso inclui mudar a assinatura para uma oferta única (por exemplo, ao cancelar, descontinuar ou reduzir ao mínimo as vantagens recorrentes) depois da compra do usuário.

Veja alguns exemplos de violações comuns:

- Assinaturas mensais que serão renovadas e cobradas automaticamente todos os meses, sem nenhum tipo de aviso aos usuários
- Assinaturas anuais que mostram o custo mensal com mais destaque
- Preços e termos da assinatura que não estão completamente no idioma local
- Promoções no app que não demonstram claramente que o usuário pode acessar o conteúdo sem uma assinatura (quando disponível)
- Nomes de SKU que não indicam com precisão a natureza da assinatura, como "Teste por R$ 0" ou "Teste a assinatura Premium sem custo financeiro por 3 dias" para uma assinatura com cobrança recorrente automática.
- Várias telas no fluxo de compra que levam os usuários a clicar acidentalmente no botão de inscrição
- Assinaturas que não oferecem valor contínuo ou recorrente: por exemplo, uma oferta de mil pedras preciosas para o primeiro mês e depois a redução do benefício para uma pedra preciosa nos meses seguintes
- Exigir a inscrição do usuário em uma assinatura de renovação automática para oferecer um benefício único e cancelar a assinatura após a compra sem a solicitação do usuário

Exemplo 1:



Bin | 00:57:08 | Bin

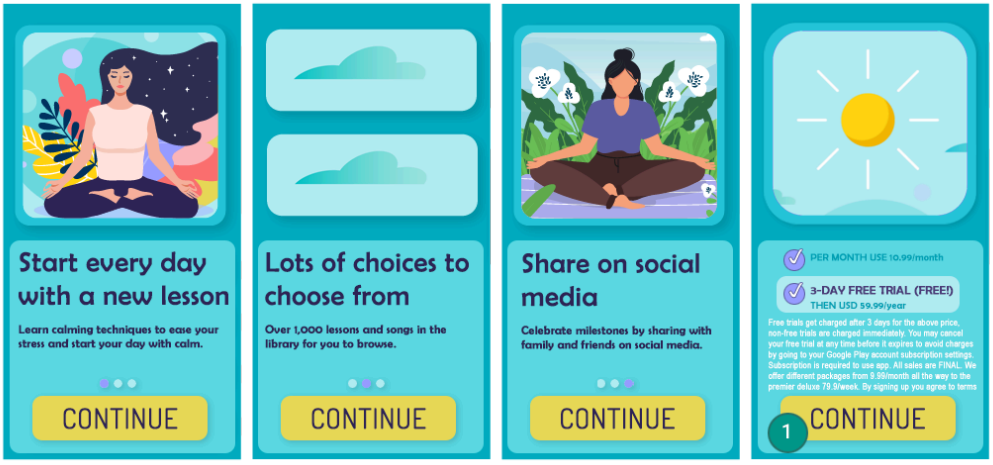
① Botão "Dispensar" ausente ou escondido, fazendo com que os usuários não entendam que podem acessar o recurso sem se inscrever no teste sem custo financeiro.

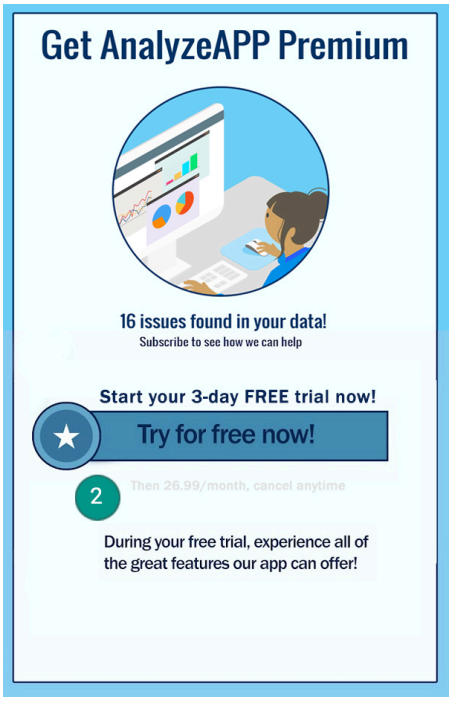
② A promoção destaca o preço como custo mensal, e não o valor total que os clientes realmente vão pagar. Os usuários podem não compreender que a cobrança será por um período de seis meses no momento da inscrição.

③ A promoção exibe somente o preço inicial, e talvez os usuários não entendam o valor que será cobrado automaticamente quando o período promocional acabar.

④ A promoção está fora de conformidade porque o idioma e a moeda não são aqueles usados no país do usuário, ao contrário dos Termos e Condições. Isso impede o usuário de entender todos os detalhes.

Exemplo 2:





Bin | 00:57:08 | Bin

① Cliques recorrentes na mesma área fazem com que o usuário clique acidentalmente no botão final de “continuar” para se inscrever.

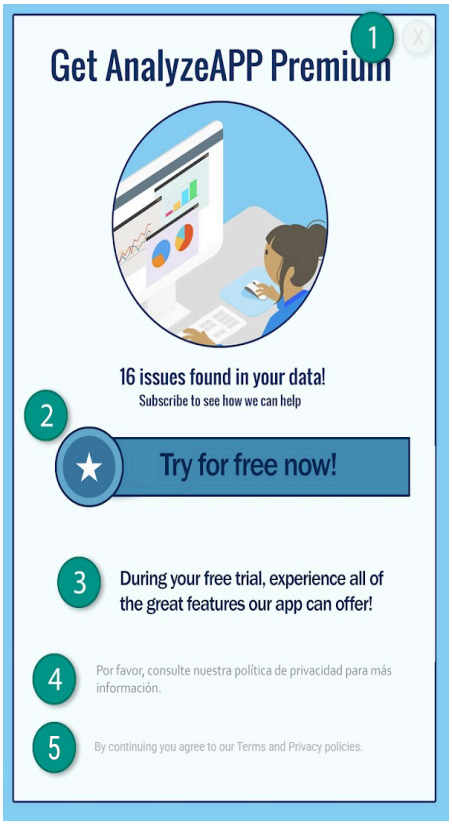
② O valor que será cobrado dos usuários ao final do período de teste é difícil de ler, de modo que os usuários podem pensar que o plano não tem custo financeiro.

Testes gratuitos e ofertas iniciais

Antes de os usuários se inscreverem na sua assinatura: é preciso indicar de maneira clara e precisa os termos do que é oferecido, incluindo a duração, o preço e a descrição dos conteúdos ou serviços acessíveis. Informe aos usuários como e quando o teste sem custo financeiro vai se tornar uma assinatura paga. Deixe claro quanto ela vai custar e como funciona o cancelamento, caso a pessoa não queira mudar para o acesso pago.

Veja alguns exemplos de violações comuns:

- Promoções que não explicam claramente a duração do teste sem custo financeiro nem do preço inicial
- Promoções que não explicam claramente que o usuário será automaticamente inscrito em uma assinatura paga ao final do período de teste
- Promoções que não demonstram claramente que o usuário pode acessar conteúdo sem um teste (quando disponível)
- Promoções com termos e preços que não foram completamente traduzidos



Bin | 00:57:08 | Bin

① Botão "Dispensar" ausente ou escondido, fazendo com que os usuários não entendam que podem acessar o recurso sem se inscrever no teste sem custo financeiro.

② A promoção enfatiza o teste sem custo financeiro, e talvez os usuários não entendam que serão cobrados automaticamente no final desse período.

③ A promoção não informa o período de teste, e talvez os usuários não compreendam por quanto tempo terão acesso sem custo financeiro ao conteúdo da assinatura.

④ A promoção apresenta violação porque os Termos e Condições foram traduzidos, mas o idioma e a moeda não. Isso impede que o usuário entenda todos os detalhes.

⑤ A promoção não explica claramente como cancelar o teste sem custo financeiro para os usuários que não querem ter uma assinatura paga após o fim do período.

Gerenciamento, cancelamento e reembolso de assinaturas

Caso você venda assinaturas nos seus apps, é necessário divulgar claramente como os usuários podem gerenciar ou cancelar assinaturas. Além disso, é preciso incluir no app um método on-line e fácil de usar para cancelamento da assinatura. Para atender a esse requisito nas configurações da conta do app (ou página equivalente), você pode incluir:

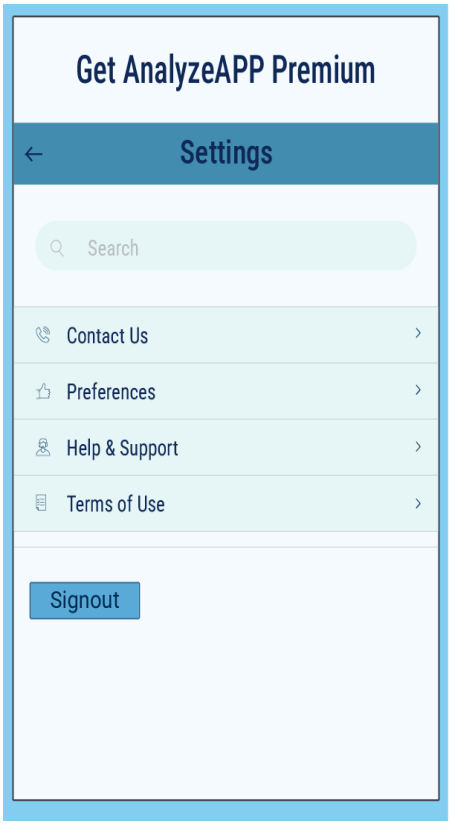
- um link para a central de assinaturas do Google Play (para assinaturas que usam o sistema de faturamento do Google Play); e/ou
- acesso direto ao processo de cancelamento.

De acordo com nossa política geral, se o usuário cancelar uma assinatura comprada pelo sistema de faturamento do Google Play, ele não vai receber um reembolso pelo período de faturamento atual. No entanto, ele vai continuar recebendo o conteúdo da assinatura até o fim do período de faturamento atual, qualquer que seja a data do cancelamento. O cancelamento vai entrar em vigor após o término do período de faturamento atual. Os usuários em alguns países podem cancelar as assinaturas imediatamente e receber reembolso proporcional, de acordo com a legislação aplicável.

O desenvolvedor (como fornecedor de conteúdo ou de acesso) pode implementar uma política de reembolso mais flexível diretamente com os usuários. É responsabilidade sua notificar os usuários de qualquer mudança nas políticas de assinatura, cance[illegible]ntir que elas obedeçam à legislação aplicável.

Bin | 00:57:08 | Bin

Veja alguns exemplos de violações comuns:



O app não tem um link para gerenciar e cancelar assinaturas na página de configurações da conta ou em alguma seção equivalente.

Programa de SDKs de anúncios autocertificados para famílias

Se você veicula anúncios no app apenas para um público-alvo infantil, conforme descrito na Política para famílias , é necessário usar apenas versões de SDK de anúncio com autocertificação de conformidade com as políticas do Google Play, o que inclui os requisitos de SDKs de anúncio autocertificados para famílias abaixo.

Se o público-alvo do seu app inclui crianças e usuários mais velhos, confira se os anúncios exibidos para crianças têm origem exclusivamente em uma dessas versões de SDKs de anúncio autocertificados (por exemplo, com uma tela neutra de informações de idade).

É sua responsabilidade garantir que todas as versões de SDKs implementadas no seu app, inclusive as versões de SDKs de anúncio autocertificados, obedeçam a todas as políticas, legislações locais e regulamentações aplicáveis. O Google não oferece declarações nem garantias quanto à precisão das informações enviadas pelos SDKs de anúncio durante o processo de autocertificação.

Os SDKs de anúncio autocertificados para famílias só são necessários se você usa SDKs de anúncio para veicular anúncios a crianças. Os casos a seguir são aceitos sem a autocertificação de SDK de anúncio com o Google Play. No entanto, você continua sendo responsável por garantir que o conteúdo dos anúncios e as práticas de coleta de dados obedeçam à política de dados do usuário e à Política para famílias do Google Play:

- Divulgação interna em que você use SDKs para fazer promoção cruzada entre apps ou outras mídias e produtos de merchandising

- Transações diretas com anunciantes em que os SDKs são usados para o gerenciamento de inventário

Requisitos de SDKs de anúncios autocertificados

Bin | 00:57:08 | Bin

- Defina e proíba conteúdos e comportamentos de anúncios questionáveis nos termos ou nas políticas do SDK de anúncios. As definições precisam obedecer às Políticas do programa para desenvolvedores do Google Play.
- Crie um método para classificar seus criativos de anúncios de acordo com grupos adequados à idade. É necessário incluir pelo menos grupos para "Todos" e "Adultos". A metodologia de classificação precisa estar de acordo com a fornecida pelo Google aos SDKs após o preenchimento do formulário de interesse abaixo.
- Ofereça aos editores a opção de pedir o tratamento para direcionamento a crianças para veiculação de anúncios, por solicitação ou por app. Esse tratamento precisa obedecer a todas as legislações e regulamentações aplicáveis de proteção infantil, como a Lei de Proteção da Privacidade On-line das Crianças (COPPA) dos EUA e o Regulamento geral de proteção de dados (GDPR) da UE (links em inglês). O Google Play exige que os SDKs de anúncios desativem anúncios personalizados, publicidade com base em interesses e remarketing como parte do tratamento para direcionamento a crianças.
- Ofereça aos editores a opção de formatos de anúncio que obedecem à Política de anúncios e monetização para famílias do Google Play e atendem aos requisitos do Programa Aprovado por Professores .
- Para os lances em tempo real de anúncios para crianças, é importante garantir que os criativos tenham sido revisados e que os indicadores de privacidade sejam propagados aos bidders.
- Envie ao Google informações suficientes (como um app de teste e as informações indicadas no formulário de interesse abaixo) para confirmar que o SDK de anúncio atende a todos os requisitos de autocertificação. Além disso, responda em tempo hábil qualquer pedido de mais informações, como o envio de novas versões para verificar a compliance do SDK de anúncio com todos os requisitos de autocertificação.
- Faça a autocertificação de que todas as novas versões obedecem às Políticas do programa para desenvolvedores do Google Play mais recentes, incluindo os requisitos da Política para famílias.

Observação: os SDKs de anúncio autocertificados para famílias precisam ter suporte para veiculação de anúncios feita em conformidade com todos os regulamentos e leis relevantes em relação a crianças caso haja regras desse tipo que se apliquem aos editores.

Veja mais informações sobre como colocar marca-d'água em criativos de anúncio e oferecer um app de teste .

Veja os requisitos de mediação para plataformas de veiculação ao exibir anúncios para crianças:

- Use somente SDKs de anúncios autocertificados para famílias ou implemente as salvaguardas necessárias para garantir que todos os anúncios veiculados por mediação obedeçam a esses requisitos.
- Transmita as informações necessárias para as plataformas de mediação a fim de indicar a classificação do conteúdo do anúncio e qualquer tratamento para direcionamento a crianças aplicável.

Os desenvolvedores podem encontrar uma lista de SDKs de anúncio autocertificados para famílias e conferir quais versões específicas desses SDKs de anúncio são autocertificadas para uso em apps do programa Feito para Família neste link .

Além disso, eles podem compartilhar este formulário de interesse com os SDKs de anúncio que querem receber a autocertificação.

Página "Detalhes do app" e promoção

A promoção e a visibilidade do app têm um forte impacto na qualidade dele na Google Play Store. Evite usar spam, promoções de baixa qualidade e meios artificiais de aumentar a visibilidade do app na página "Detalhes do app" no Google Play.

Bin | 00:57:08 | Bin

Promoção de apps

Não são permitidos apps que usem ou se beneficiem, direta ou indiretamente, de práticas de promoção (como anúncios) enganosas ou prejudiciais ao ecossistema do desenvolvedor ou aos usuários. As práticas de promoção são consideradas enganosas ou prejudiciais se exibirem comportamento ou conteúdo que viole as Políticas do programa para desenvolvedores.

Veja alguns exemplos de violações comuns:

- Uso de anúncios enganosos em sites, apps ou outras propriedades, incluindo alertas ou notificações semelhantes àquelas do sistema
- Uso de anúncios sexualmente explícitos para direcionar os usuários à página "Detalhes do app" para download
- Promoção ou técnicas de instalação que causam o redirecionamento para o Google Play ou para o download do app sem uma ação informada do usuário
- Promoção não solicitada por serviços de SMS
- Texto ou imagem no título, ícone ou nome do desenvolvedor do app que indica o desempenho ou a classificação na loja, informações de preço ou promoções ou que sugere relações com programas do Google Play

É sua responsabilidade garantir que todas as redes de publicidade, afiliados ou anúncios associados com seu app estejam em conformidade com essas políticas.

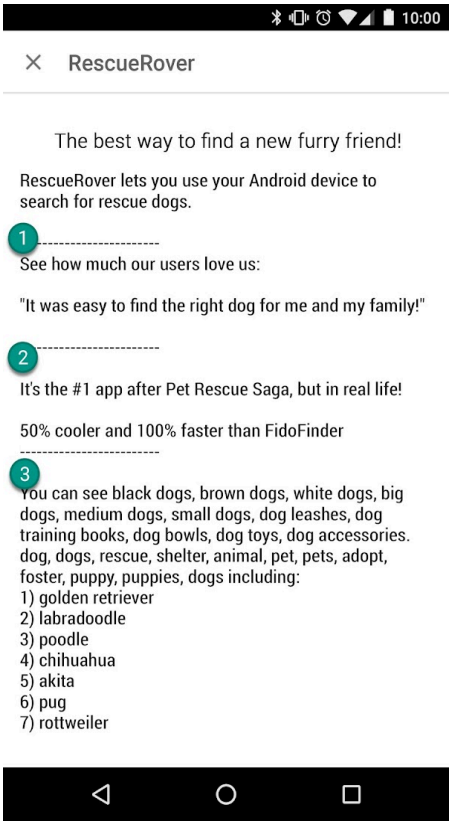
Metadados

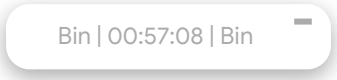
Os usuários dependem das descrições para entender a funcionalidade e a finalidade do app. Não permitimos apps com metadados enganosos, excessivos, irrelevantes, inadequados, com formatação incorreta ou sem valor descritivo, incluindo a descrição, o nome do desenvolvedor, o título, o ícone, as capturas de tela e as imagens promocionais do app. Os desenvolvedores precisam descrever claramente o app. Também não permitimos depoimentos de usuários não identificados ou anônimos na descrição do app.

O título, o ícone do app e o nome do desenvolvedor são especialmente úteis para os usuários encontrarem e saberem mais sobre seu app. Não use emojis, emoticons nem caracteres especiais repetidos nesses elementos de metadados. Evite usar TODAS AS LETRAS EM CAIXA ALTA, a menos que isso faça parte da sua marca. Não é permitido o uso de símbolos enganosos nos ícones dos apps. Por exemplo, um ponto que indique uma nova mensagem quando não há novas mensagens e símbolos de download/instalação quando o app não está relacionado ao download de conteúdo. O título do seu app precisa ter até 30 caracteres. Não use no título, no ícone ou no nome do desenvolvedor do aplicativo texto ou imagem que indiquem preços ou informações promocionais ou o desempenho e a classificação da loja, ou que sugiram relações com programas existentes do Google Play.

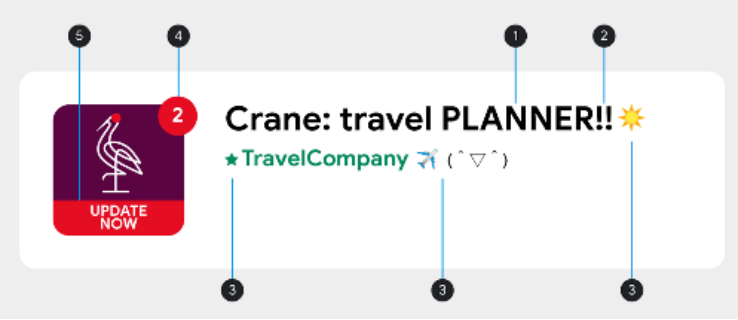
Além dos requisitos mencionados aqui, Políticas para desenvolvedores específicas ao Google Play podem exigir que você forneça outras informações de metadados.

Veja alguns exemplos de violações comuns:



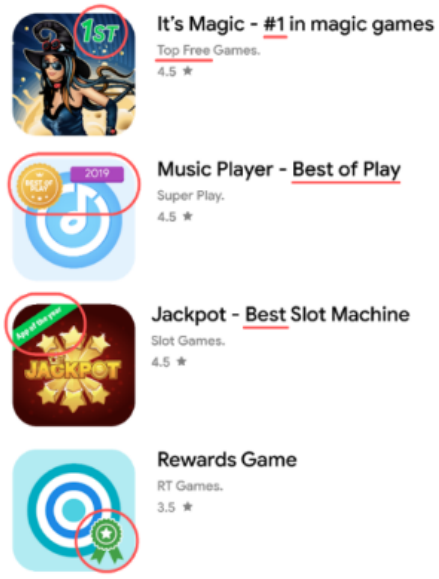


① Depoimentos de usuários anônimos ou não identificados
② Comparação de dados de apps ou marcas
③ Blocos ou listas verticais/horizontais de palavras



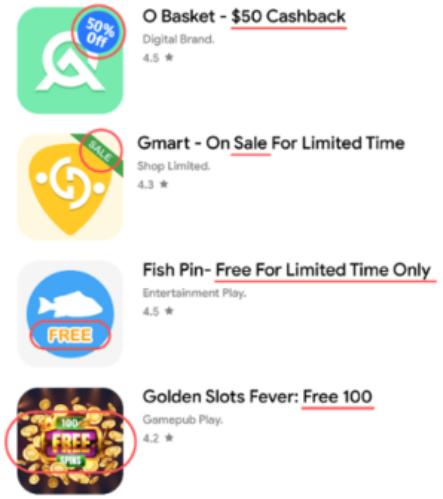
① TODAS AS LETRAS EM CAIXA ALTA, a menos que isso faça parte do nome da marca
② Sequências de caracteres especiais irrelevantes para o app
③ Emojis, emoticons (incluindo kaomojis) e caracteres especiais
④ Símbolo enganoso
⑤ Texto enganoso

- Imagens ou textos que indicam o desempenho ou a classificação na loja, como "App do ano", "Número 1", "Melhor jogo de 20XX", "Favoritos", ícones de prêmios etc.

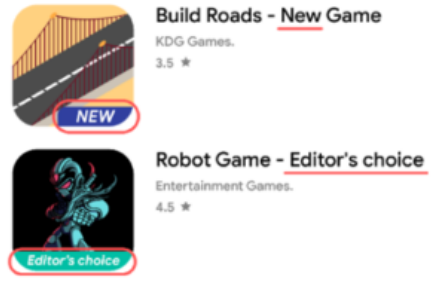


Bin | 00:57:08 | Bin

- Imagens ou textos que indicam informações promocionais ou de preço, como "10% de desconto", "R$ 50 de reembolso", "gratuito por período limitado" etc.



- Imagens ou textos que indicam programas do Google Play, como "Escolha dos editores", "Novo" etc.



Confira alguns exemplos de texto, imagens ou vídeos inadequados para a página de detalhes:

- Imagens ou vídeos com conteúdo sexualmente sugestivo. Evite imagens sugestivas que tenham seios, nádegas, órgãos genitais ou outro conteúdo ou anatomia fetichizados, seja real ou ilustração.
- É proibido usar linguagem obscena, vulgar ou outra linguagem imprópria para um público geral na página "Detalhes do app".
- Não é permitido retratar violência explícita de maneira proeminente em imagens promocionais, vídeos nem ícones do app.
- Representação do uso ilícito de drogas. Mesmo o conteúdo educacional, documental, científico ou artístico (EDSA, na sigla em inglês) precisa ser adequado para todos os públicos na página "Detalhes do app".

Confira algumas práticas recomendadas:

- Destaque o que há de melhor no seu app. Compartilhe fatos interessantes para que os usuários entendam o que ele tem de especial.
- Verifique se o título e a descrição do app mostram precisamente a funcionalidade dele.
- Evite usar palavras-chave ou referências repetitivas ou sem relação com o app.
- A descrição do app precisa ser concisa e direta. Descrições mais curtas costumam resultar em uma melhor experiência do usuário, principalmente em dispositivos com telas menores. Uma descrição excessivamente extensa, com muitos detalhes, formatação incorreta ou repetições, pode resultar na violação desta política.
- A página "Detalhes do app" precisa ser adequada para o público em geral. Evite o uso de textos, imagens ou vídeos inadequados e obedeça às diretrizes acima.

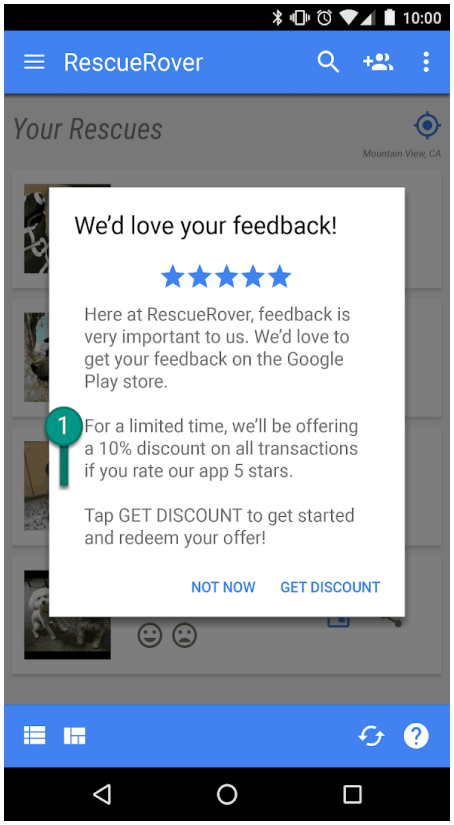
Bin | 00:57:08 | Bin

Instalações, notas e avaliações de usuários

Os desenvolvedores não podem tentar manipular a colocação dos apps no Google Play. Isso inclui, mas não se limita a, melhorar os indicadores dos produtos por meios ilegítimos, como avaliações e classificações fraudulentas ou induzidas por incentivo, ou criar apps cuja função principal é incentivar os usuários a instalar outros apps.

Veja alguns exemplos de violações comuns:

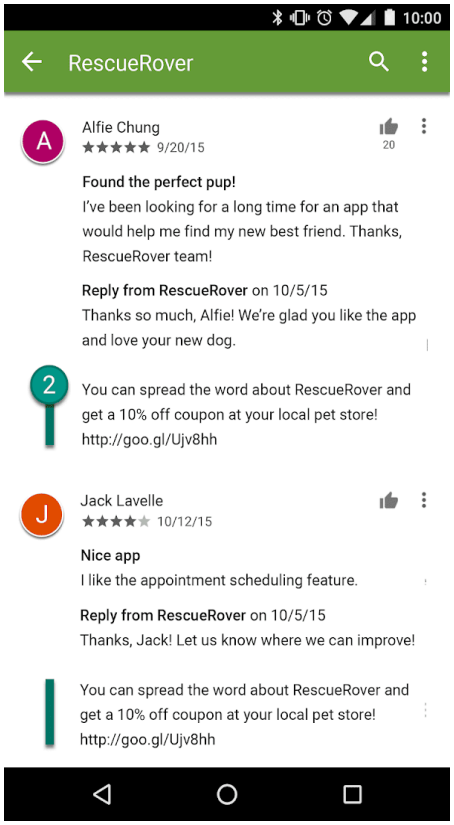
- Pedir que os usuários deem uma nota ao app e oferecer um incentivo para isso:

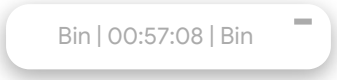


① Esta notificação oferece um desconto ao usuário em troca de uma nota alta.

- Enviar avaliações repetidamente se passando por usuários para influenciar a colocação de um app no Google Play

- Enviar ou incentivar os usuários a enviar avaliações que incluam conteúdo inadequado, como afiliados, cupons, códigos de jogos, endereços de e-mail ou links para sites ou outros apps:





② Esta avaliação incentiva os usuários a promover o app RescueRover, oferecendo um cupom.

As notas e avaliações são indicadores da qualidade do app. É importante para os usuários que essas informações sejam autênticas e relevantes. Confira algumas práticas recomendadas sobre como responder às avaliações dos usuários:

- Mantenha sua resposta focada nas questões levantadas nos comentários dos usuários e não peça uma nota melhor.
- Inclua referências a recursos úteis, como um endereço de suporte ou uma página de perguntas frequentes.

Classificações de conteúdo

As classificações de conteúdo no Google Play são realizadas pela Coalizão Internacional de Classificação Indicativa (IARC) e foram criadas para ajudar os desenvolvedores a mostrar como os apps foram categorizados de acordo com a região dos usuários. As autoridades regionais da IARC mantêm as diretrizes usadas para determinar o nível de maturidade do conteúdo em um app. Não permitimos apps sem classificação de conteúdo no Google Play. Os anúncios exibidos em um app não podem ter conteúdo muito mais maduro do que o do próprio app. Veja mais informações na política contra anúncios inadequados .

Como as classificações de conteúdo são usadas

As classificações de conteúdo são usadas para informar os consumidores, principalmente os pais, sobre conteúdo potencialmente questionável em um app. Elas também ajudam a filtrar ou bloquear seu conteúdo em determinados territórios ou para usuários específicos quando exigido por lei. Além disso, elas ajudam a determinar a qualificação do seu app para programas especiais de desenvolvedores.

Como são atribuídas as classificações de conteúdo

Para receber uma classificação do conteúdo, é necessário preencher um questionário de classificação no Play Console com perguntas sobre a natureza do conteúdo dos seus apps. De acordo com suas respostas, o app receberá uma classificação de cont[illegible] autoridades competentes. Deturpação sobre o conteúdo levam à [illegible]p. Por isso, é importante responder corretamente ao questionário.

Bin | 00:57:08 | Bin

Para evitar que seu app seja listado como "Sem classificação", preencha o questionário de classificação de conteúdo para cada novo app enviado ao Play Console e para todos aqueles que já estão ativos no Google Play. Os apps sem classificação de conteúdo serão removidos da Play Store.

Se você fizer alterações em recursos ou no conteúdo do app que afetem as respostas já fornecidas, será necessário preencher um novo questionário no Play Console.

A classificação do conteúdo atribuída ao seu app é específica para o conteúdo que ele oferece. Isso não inclui outros recursos e práticas, como contratos de usuários ou anúncios. Você é responsável por informar seus usuários sobre quaisquer considerações baseadas em idade adicionais, como práticas de privacidade específicas para idade.

Para mais informações sobre o questionário, acesse a Central de Ajuda e confira os diferentes órgãos responsáveis pela classificação em todas as regiões. Aprenda também como preencher o questionário de classificação do conteúdo.

Contestação de classificações

Se você não concordar com a classificação atribuída ao seu app, faça uma contestação diretamente para a autoridade de classificação da IARC pelo link fornecido no e-mail do seu certificado.

Notícias e revistas

Todos os apps de notícias e revistas precisam ser declarados no Google Play Console e preencher uma autodeclaração.

Os apps de notícias e revistas têm as seguintes características:

- Declaram-se como app de "notícias" ou "revista" no Google Play Console.
- Estão listados na categoria "Notícias e revistas" na Google Play Store, com a indicação "notícias" ou "revista" no título, no ícone, no nome do desenvolvedor ou na descrição do app.

Veja os requisitos para apps de notícias e relacionados para saber como enquadrar um app nessas categorias.

Além disso, os apps de notícias e revistas precisam:

- Fornecer a fonte dos artigos de notícias e revistas, incluindo, mas não se limitando ao publisher ou autor original.
- Atualizar o conteúdo com frequência (sem o formato estático).
- Oferecer aos usuários uma maneira prática e rápida de acessar as informações de contato mais recentes do app de notícias e revistas.
- Fornecer informações claras sobre as fontes de publicação do conteúdo de terceiros (por exemplo, quando fornecido por apps agregadores de notícias e revistas).
- Oferecer aos usuários uma prévia do conteúdo no app antes da compra (se precisar de assinatura).
- Não ter marketing de afiliados ou receita de publicidade como principal finalidade.

Spam, funcionalidade e experiência do usuário

Os apps devem oferecer um nível básico de conteúdo e de recursos adequados para uma experiência do usuário interessante. Os apps que apresentam falhas, exibem outros comportamentos

incompatíveis com uma experiência do usuário funcional ou servem somente para enviar spam aos usuários ou ao Google Play não são uma contribuição relevante para o catálogo.

Bin | 00:57:08 | Bin

Spam

Não são permitidos apps que enviam spam aos usuários ou ao Google Play, como os que enviam mensagens não solicitadas. Também são proibidos os apps repetitivos ou de baixa qualidade.

Spam de mensagens

Não são permitidos apps que enviem SMS, e-mails ou outras mensagens em nome do usuário sem que este possa confirmar o conteúdo e os destinatários pretendidos.

Veja um exemplo de uma violação comum:

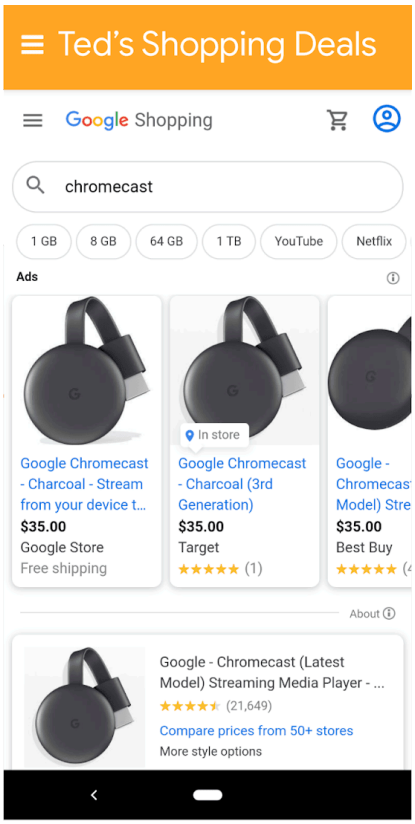
- Quando o usuário pressiona o botão "Compartilhar", o app envia mensagens em nome dele sem que ele possa confirmar o conteúdo e os destinatários:

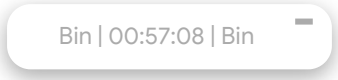
Spam de afiliados e visualizações da Web

Não são permitidos apps com a função principal de direcionar o tráfego afiliado a um site ou fornecer uma visualização da Web de um site sem a permissão do administrador ou proprietário deste.

Veja alguns exemplos de violações comuns:

- Apps com a função principal de direcionar o tráfego por referência a um site para receber crédito por inscrições ou compras do usuário no site em questão
- Apps com a função principal de exibir um WebView de um site sem permissão:





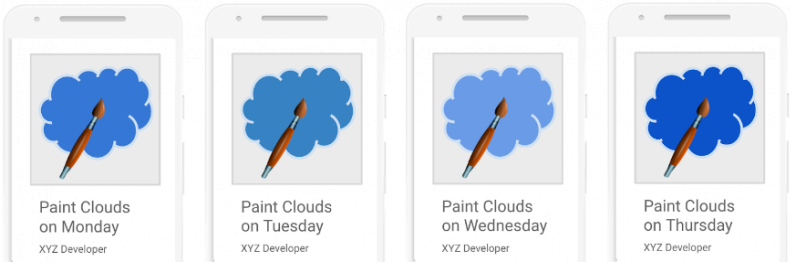
① Este app se chama "Ofertas do Ted", mas ele só fornece um WebView do Google Shopping.

Conteúdo repetitivo

Não são permitidos apps que simplesmente proporcionam a mesma experiência de outros já disponíveis no Google Play. É preciso criar conteúdos ou serviços exclusivos aos apps para oferecer valor agregado aos usuários.

Veja alguns exemplos de violações comuns:

- Não é permitido copiar conteúdo de outros apps sem adicionar valor nem conteúdo original.
- Não é permitido criar vários apps com funcionalidade, conteúdo e experiência do usuário muito semelhantes. Caso os apps tenham pouco volume de conteúdo, recomendamos que os desenvolvedores criem um único app com todo o conteúdo agregado.



Funcionalidade, conteúdo e experiência do usuário

Os apps precisam proporcionar uma experiência de usuário estável, envolvente e responsiva. Os apps que apresentam falhas, não oferecem o nível básico de utilidade adequada para dispositivos móveis, não incluem conteúdo atrativo ou exibem outro comportamento incompatível com uma experiência de usuário funcional e envolvente não são permitidos no Google Play.

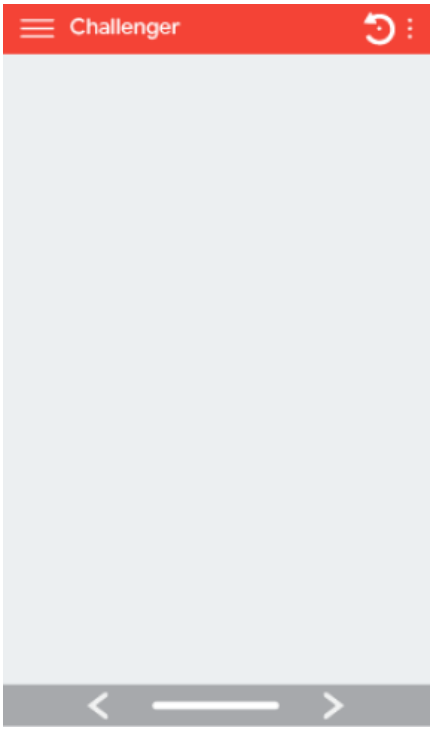
Conteúdo e funcionalidade limitados

Não são permitidos apps que só tenham conteúdo e funcionalidade limitados.

Veja um exemplo de uma violação comum:

- Apps que são estáticos sem funcionalidades específicas, como os que só mostram texto ou abrem arquivos PDF
- Apps que têm pouquíssimo conteúdo e que não oferecem uma experiência do usuário envolvente, como os que consistem apenas em um único plano de fundo
- Apps que são desenvolvidos para não fazer nada ou que não têm uma função

Bin | 00:57:08 | Bin



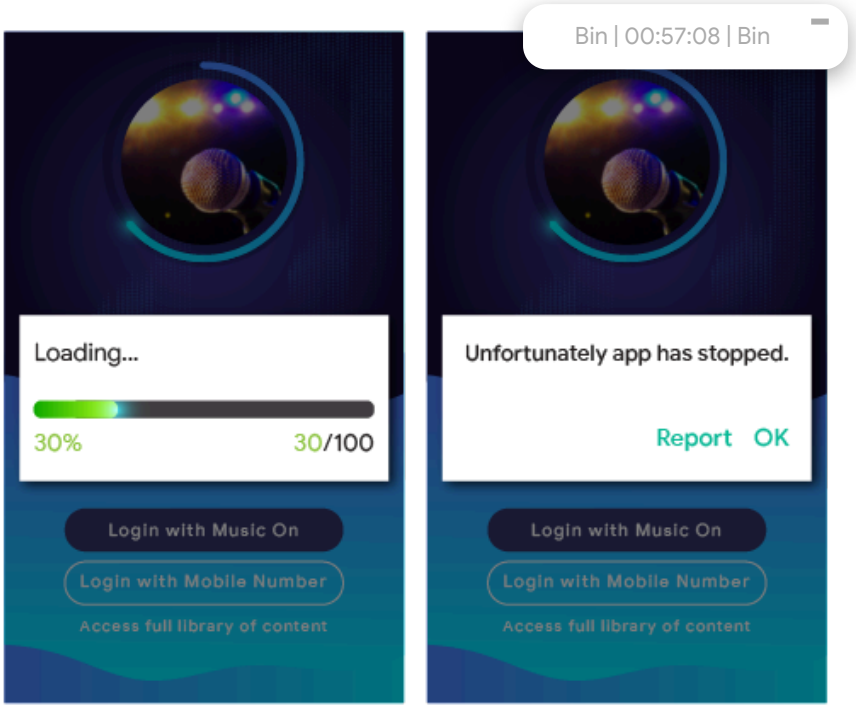
Recursos com problemas

Não permitimos apps com falhas, fechamentos forçados, travamentos ou que funcionem de maneira anormal.

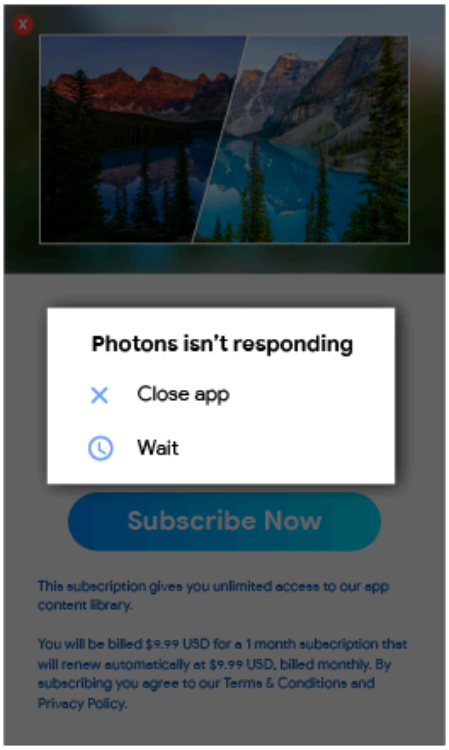
Veja alguns exemplos de violações comuns:

- Apps que não instalam

- Apps que instalam, mas não carregam



- Apps que carregam, mas não são responsivos



Outros programas

Além do cumprimento das Políticas de conteúdo estabelecidas nesta Central de políticas, os apps que foram projetados para outras experiências do Android e distribuídos pelo Google Play também estão

sujeitos aos requisitos da política específica ao programa. Leia a lista abaixo para verificar se essas políticas se aplicam ao seu app.

Bin | 00:57:08 | Bin

Instant Apps Android

Nosso objetivo com o Instant Apps Android é criar experiências do usuário que sejam agradáveis e descomplicadas e que, ao mesmo tempo, atendam aos mais altos padrões de privacidade e segurança. Nossas políticas foram criadas para fundamentar esse objetivo.

Os desenvolvedores que optem por distribuir Instant Apps Android pelo Google Play precisam aderir às políticas a seguir e a todas as outras políticas do programa para desenvolvedores do Google Play.

Identidade

No caso dos apps instantâneos que incluem o recurso de login, os desenvolvedores precisam integrar o Smart Lock para senhas .

Suporte a links

É obrigatório que os desenvolvedores de Instant Apps Android ofereçam suporte adequado a links para outros apps. Se apps instantâneos ou instalados tiverem links que podem direcionar a um app instantâneo, o desenvolvedor desses apps precisará direcionar os usuários para o app instantâneo em questão, em vez de capturar os links em um WebView , por exemplo.

Especificações técnicas

É obrigatório que os desenvolvedores cumpram com as especificações e os requisitos técnicos do Instant Apps Android fornecidos pelo Google, incluindo as respectivas atualizações periódicas e aqueles listados na nossa documentação pública .

Oferta de instalação do app

O app instantâneo poderá oferecer ao usuário o app instalável, mas esta não pode ser a finalidade principal dele. Ao oferecer uma instalação, os desenvolvedores precisam:

- usar o ícone "Instalar app" do Material Design (em inglês) e o rótulo "Instalar" para o botão de instalação;
- incluir até dois ou três avisos de instalação implícitos no app instantâneo;
- evitar o uso de banners ou outras técnicas semelhantes a anúncios ao mostrar solicitações de instalação aos usuários.

Veja mais detalhes sobre apps instantâneos e diretrizes adicionais de UX nas práticas recomendadas para a experiência do usuário .

Alteração do estado do dispositivo

Os apps instantâneos não podem fazer alterações no dispositivo do usuário que permanecem após a sessão do app em questão. Por exemplo, os apps instantâneos não podem alterar o plano de fundo do usuário ou criar um widget de tela inicial.

Visibilidade do app

Os desenvolvedores precisam garantir que os apps instantâneos fiquem visíveis ao usuário de modo que ele sempre saiba quando o app está em execução no dispositivo.

Identificadores de dispositivo

Os apps instantâneos não têm permissão de acesso a identificadores de dispositivo que (1) permanecem no dispositivo após o app instantâneo ser interrompido e (2) não podem ser redefinidos pelo usuário. Alguns exemplos são:

Bin | 00:57:08 | Bin

- Série da versão
- Endereços mac de qualquer chip de rede
- IMEI e IMSI

Se obtidos por meio da permissão de tempo de execução, os apps instantâneos poderão acessar o número de telefone. O desenvolvedor não pode tentar reconhecer o usuário usando esses identificadores nem de qualquer outra maneira.

Tráfego de rede

O tráfego de rede dentro do app instantâneo precisa ser criptografado com um protocolo TLS como HTTPS.

Política de emoji do Android

Nossa política de emojis foi desenvolvida para promover uma experiência do usuário consistente e inclusiva. Para isso, todos os apps precisam ser compatíveis com a versão mais recente do Unicode Emoji ao serem executados no Android 12 ou mais recente.

Os apps que usam o Android Emoji padrão sem implementações personalizadas já usam a versão mais recente do Unicode Emoji ao serem executados no Android 12 ou mais recente.

Os apps com implementações personalizadas de emoji, incluindo aqueles fornecidos por bibliotecas de terceiros, precisam ser totalmente compatíveis com a versão mais recente do Unicode ao serem executados no Android 12 ou mais recente em até quatro meses após o lançamento do novo Unicode Emoji.

Consulte este guia para saber como ser compatível com emojis modernos.

Famílias

O Google Play oferece uma plataforma completa para que os desenvolvedores possam exibir conteúdo de alta qualidade com classificação indicativa adequada a toda a família. Antes de enviar um app ao programa Feito para Família ou publicar conteúdo voltado para crianças na Google Play Store, você é responsável por garantir que ele seja adequado a esse público e obedeça a toda a legislação relevante.

Saiba mais sobre o processo relacionado ao conteúdo para famílias e confira a lista de verificação interativa na Formação para criar apps de sucesso.

Políticas para famílias do Google Play

A tecnologia é cada vez mais usada como ferramenta para melhorar a vida das famílias, e a procura dos responsáveis por conteúdo seguro e de alta qualidade para compartilhar com as crianças só aumenta. Você pode desenvolver apps específicos para crianças ou seu app pode atrair a atenção delas. O Google Play quer ajudar a fazer com que seu app seja seguro para todos os usuários, inclusive as famílias.

A palavra "crianças" pode ter diferentes significados dependendo do local e do contexto. É importante que você consulte uma assessoria jurídica para determinar a que obrigações e/ou restrições de idade o app está sujeito. Você é quem mais sabe como seu conteúdo funciona. Por isso, contamos com sua colaboração em fazer com que os apps do Google Play sejam seguros para todas as famílias.

Se o app obedece às Políticas para famílias do Google Play, você pode solicitar a avaliação dele para o Programa Aprovado por Professores, mas não garantimos a inclusão dos apps na iniciativa.

Bin | 00:57:08 | Bin

Requisitos do Play Console

Público-alvo e conteúdo

Na seção Público-alvo e conteúdo do Google Play Console, você precisa indicar o público-alvo a que se destina o app antes de publicá-lo, selecionando uma opção na lista de faixas etárias fornecidas. Independentemente do que você identificar no Google Play Console, se você optar por incluir no app imagens e termos que possam ser considerados voltados para crianças, talvez isso afete a avaliação do Google Play em relação ao público-alvo declarado. O Google Play reserva-se o direito de fazer a própria análise das informações do app fornecidas por você para determinar se o público-alvo divulgado está correto.

Só selecione mais de uma faixa etária para o público-alvo se o app tiver sido desenvolvido para e for apropriado aos usuários nas faixas etárias selecionadas. Por exemplo, apps para bebês, crianças pequenas ou em idade pré-escolar precisam ter somente a faixa etária "Até 5 anos" selecionada como público-alvo. Se o app for destinado a uma série escolar específica, escolha a faixa etária que melhor representa esse nível de ensino. Selecione apenas faixas etárias que incluam adultos e crianças, caso você realmente tenha projetado seu app para todas as idades.

Atualizações da seção "Público-alvo e conteúdo"

É possível atualizar a qualquer momento as informações do app na seção "Público-alvo e conteúdo" no Google Play Console. É necessário atualizar o app para que essas informações sejam refletidas na Google Play Store. No entanto, todas as mudanças feitas nessa seção do Google Play Console poderão ser avaliadas quanto à conformidade com as políticas antes mesmo do envio da atualização do app.

Recomendamos fortemente que você informe aos usuários existentes do seu app sobre alterações no público-alvo ou se passar a permitir anúncios ou compras no aplicativo. Para fazer isso, use a seção "Novidades" na página "Detalhes do app" ou as notificações no app.

Declarações falsas no Play Console

Fazer declarações falsas no Play Console, inclusive na seção "Público-alvo e conteúdo", pode resultar na remoção ou suspensão do app. Por isso, é importante fornecer informações precisas.

Requisitos da Política para famílias

Se crianças forem um dos públicos-alvo do app, será preciso cumprir os seguintes requisitos. A não conformidade com eles poderá resultar na remoção ou suspensão do app.

1. **Conteúdo do app**: o conteúdo disponível no app precisa ser adequado para crianças. Caso o app tenha conteúdo que não seja globalmente adequado, mas que seja considerado adequado para usuário menor de idade em uma determinada região, ele talvez seja disponibilizado nessa região (regiões limitadas), mas vai permanecer indisponível em outras.
2. **Funcionalidade do app**: seu app não pode apenas oferecer uma visualização da Web de um site nem ter o objetivo principal de direcionar tráfego para um site sem permissão do proprietário ou administrador.
3. **Respostas no Play Console**: você precisa responder com precisão às perguntas sobre seu app no Play Console e atualizar as respostas para que reflitam corretamente qualquer mudança aplicada a ele. Isso inclui, mas não se limita a, apresentar com precisão as informações necessárias sobre o app nas seções "Público-alvo e conteúdo" e "Segurança dos dados" e no questionário de classificação de conteúdo da Coalizão Internacional de Classificação Indicativa (IARC).
4. **Práticas relacionadas a dados**: você precisa divulgar a coleta de todas as informações pessoais e sensíveis de crianças, inclusive por APIs e SDKs chamados ou usados no seu app. As informações sensíveis de crianças incluem, mas não se limitam a, informações de autenticação, dados do sensor

da câmera e do microfone, dados do dispositivo, ID do Android e dados de uso de publicidade. Também é preciso que o app siga estas práticas relacionadas a dados:

- Os apps que segmentam somente crianças não [illegible] dor de publicidade do Android (AAID), os números de série do chip [illegible] AC, o SSID, o IMEI e/ou o IMSI.
  - Os apps que segmentam somente crianças não podem solicitar a permissão AD_ID ao segmentar o nível 33 da API do Android ou versões mais recentes.
- Os apps segmentados para públicos-alvo que incluam crianças e adultos não podem transmitir o AAID, os números de série do chip e do hardware, o BSSID, o MAC, o SSID, o IMEI e/ou o IMSI de crianças ou usuários com idade desconhecida.
- O número de telefone do dispositivo não pode ser solicitado ao TelephonyManager da API do Android.
- Os apps segmentados apenas para crianças não podem solicitar a permissão de localização nem coletar, usar e transmitir o local exato.
- Os apps precisam usar o Gerenciador de dispositivos complementar (CDM, na sigla em inglês) ao pedir para usar o Bluetooth, a menos que o app segmente apenas versões de sistema operacional (SO) não compatíveis com o CDM.

5. **APIs e SDKs**: você precisa garantir a implementação correta de qualquer API e SDK no app.
   - Os apps que só segmentam crianças não podem conter APIs nem SDKs que não sejam aprovados para uso em serviços primariamente direcionados para crianças.
     - Por exemplo, um serviço de API que usa a tecnologia OAuth para autenticação e autorização e indica nos Termos de Serviço que não é aprovado para uso em serviços feitos para crianças.
   - Os apps que segmentam simultaneamente crianças e públicos-alvo mais velhos não podem implementar APIs nem SDKs que não sejam aprovados para uso em serviços direcionados a crianças, a menos que sejam usados por trás de uma tela neutra de informações de idade ou implementados de uma maneira que não resulte na coleta de dados de crianças. Apps que são direcionados simultaneamente a crianças e públicos mais velhos não podem exigir que os usuários acessem o conteúdo do app usando APIs ou SDKs que não sejam aprovados para uso em serviços feitos para crianças.

6. **Realidade aumentada (RA)**: se o app usar realidade aumentada, será necessário incluir um aviso de segurança imediatamente após a abertura da seção de RA. O aviso precisa ter as seguintes informações:
   - Uma mensagem apropriada sobre a importância da supervisão da família.
   - Um lembrete alertando sobre os perigos físicos no mundo real (por exemplo, sobre o ambiente ao redor dos usuários).
   - O app não pode exigir o uso de dispositivos não recomendados para crianças (por exemplo, Daydream e Oculus).

7. **Recursos e aplicativos sociais**: se o app permitir que os usuários compartilhem ou troquem informações, vai ser necessário divulgar esses recursos com precisão no questionário de classificação do conteúdo no Play Console.
   - Aplicativos sociais: têm como foco principal permitir que os usuários compartilhem conteúdo em formato livre ou se comuniquem com grandes grupos de pessoas. Todos os aplicativos sociais que incluem crianças no público-alvo precisam exibir um lembrete no próprio app sobre segurança on-line e sobre os riscos reais das interações na Internet antes de permitir que usuários dessa faixa etária troquem mídia ou informações em formato livre. Além disso, é preciso exigir a ação de um adulto antes de permitir que crianças troquem informações pessoais.
   - Recursos sociais: incluem qualquer funcionalidade adicional do app que permita aos usuários compartilhar conteúdo em formato livre ou se comunicar com grandes grupos de pessoas. Todos os apps que incluem crianças no público-alvo e têm recursos sociais precisam exibir um lembrete no próprio app sobre segurança on-line e sobre os riscos reais das interações na Internet antes de permitir que usuários dessa faixa etária troquem mídia ou informações em formato livre. Além

disso, é preciso oferecer um método para que os adultos gerenciem os recursos sociais de crianças, incluindo ativar/desativar esses recursos ou selecionar diferentes níveis de funcionalidade, entre outros. Também é necessá[illegible]to antes de ativar recursos que permitem que crianças troquem i[illegible]

Bin | 00:57:08 | Bin

- A "ação de um adulto" é um mecanismo para verificar a idade do usuário sem incentivar as crianças a falsificar essa informação para ter acesso a áreas do app projetadas para adultos. Por exemplo: PIN do adulto, senha, data de nascimento, verificação de e-mail, ID por foto, cartão de crédito ou documento oficial.
- Aplicativos sociais em que o foco principal é conversar com pessoas desconhecidas não podem ter crianças como público-alvo. Por exemplo: apps do tipo "chat roulette", apps de encontros, salas de chat abertas com foco em crianças etc.

8. **Compliance legal**: você precisa garantir que o app, inclusive as APIs ou os SDKs chamados ou usados por ele, obedeçam à Lei de Proteção da Privacidade On-line das Crianças (COPPA) dos EUA, ao Regulamento geral de proteção de dados (GDPR) da UE e a qualquer outra legislação ou regulamento aplicável.

Veja alguns exemplos de violações comuns:

- Apps que promovem jogos para crianças na página "Detalhes do app", mas têm conteúdo que só é apropriado para adultos
- Apps que implementam APIs com Termos de Serviço que proíbem o uso em apps feitos para crianças
- Apps que exaltam o uso de bebidas alcoólicas, tabaco ou substâncias controladas
- Apps que incluem jogos de azar reais ou simulados
- Apps que incluem violência, sangue ou conteúdo chocante não apropriado para crianças
- Apps que fornecem serviços de relacionamento pessoal ou aconselhamento sexual e amoroso
- Apps que têm links para sites com conteúdo que viola as Políticas do programa para desenvolvedores do Google Play
- Apps que exibem anúncios destinados a adultos (por exemplo, conteúdo violento, sexual ou de jogos de azar) para crianças

Anúncios e monetização

Se você gera receita com um app destinado a crianças no Google Play, é importante que ele siga os seguintes requisitos da política de anúncios e monetização para famílias.

As políticas abaixo se aplicam a todo tipo de monetização e publicidade, incluindo anúncios, promoções cruzadas (para seus aplicativos e os de terceiros), ofertas de compras no app ou qualquer outro conteúdo comercial (como inserção paga de produto). Toda monetização e publicidade nesses apps precisa obedecer às legislações e regulamentações aplicáveis, inclusive a todas as diretrizes do setor ou de autorregulamentação relevantes.

O Google Play reserva-se o direito de recusar, remover ou suspender apps devido a táticas comerciais excessivamente agressivas.

Requisitos dos anúncios

Se o app exibe anúncios para crianças ou usuários de idade desconhecida, é preciso:

- usar somente SDKs de anúncios com autocertificação de cumprimento das Políticas do Google Play para famílias para exibir anúncios a essas pessoas;
- garantir que os anúncios exibidos para esses usuários não envolvam publicidade com base em interesses (direcionada a usuários específicos com determinadas características de acordo com o comportamento de navegação on-line) nem remarketing (publicidade que segmenta usuários específicos com base em interações anteriores com um app ou site);
- garantir que os anúncios exibidos a esses usuários apresentem conteúdo apropriado para crianças;

- garantir que os anúncios exibidos a esses usuários sigam os requisitos de formato do anúncio para famílias; e
- garantir o cumprimento de todos os padrões do se aplicáveis com relação à publicidade para crianças.

Bin | 00:57:08 | Bin

Requisitos de formato dos anúncios

A monetização e a publicidade no app não podem ter conteúdo enganoso nem ser projetadas de maneira que leve a cliques acidentais de usuários menores de idade.

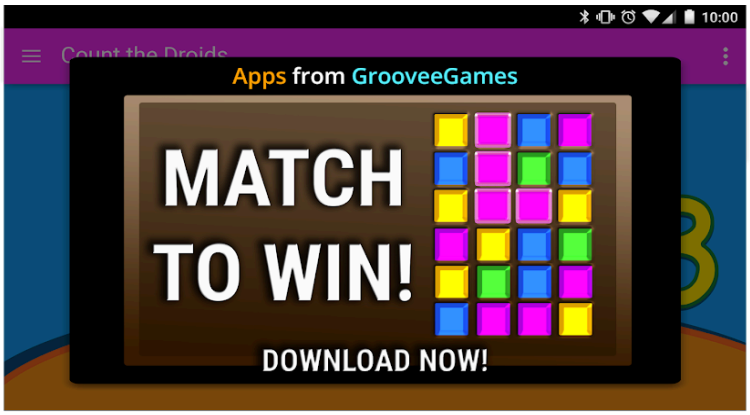
Se as crianças são o único público-alvo do app, os itens abaixo são proibidos. Caso o público-alvo inclua crianças e adultos, esses elementos não são permitidos ao veicular anúncios para menores ou usuários com idade desconhecida:

- Publicidade e monetização invasivas, como as que ocupam a tela inteira ou interferem no uso normal e não oferecem uma maneira clara de dispensar o anúncio (por exemplo, paredes de anúncios)
- Publicidade e monetização que interferem no uso normal do app ou jogo e não podem ser fechadas depois de 5 segundos, inclusive no caso de anúncios premiados e com permissão
- Exceção permitida: monetização e publicidade que duram mais de 5 segundos, mas não interferem no uso normal do app ou jogo (por exemplo, conteúdo de vídeo com anúncios integrados)
- Publicidade e monetização intersticiais exibidas imediatamente após a inicialização do app
- Vários posições de anúncio em uma página, por exemplo: mostrar mais de um banner ou anúncio em vídeo ou usar anúncios de banner que exibem diversas ofertas em um canal
- Monetização e publicidade que não podem ser facilmente diferenciadas do conteúdo do app, como offerwalls e outras experiências de anúncios imersivos
- Uso de táticas chocantes ou que envolvem manipulação emocional para incentivar a visualização de anúncios ou as compras no app
- Anúncios enganosos que forçam o usuário a clicar usando um botão "Dispensar" para acionar outro anúncio ou que aparecem repentinamente em áreas do app onde o usuário geralmente toca para outra função
- Falta de distinção entre o uso de moedas virtuais no jogo e dinheiro real para fazer compras no app

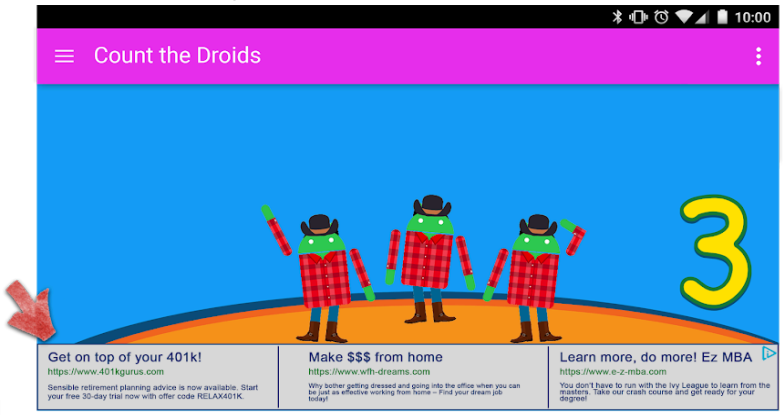
Veja alguns exemplos de violações comuns:

- Monetização e publicidade que se afastam do dedo do usuário quando ele tenta fechar
- Monetização e publicidade que não fornecem ao usuário uma maneira de fechar a oferta após 5 (cinco) segundos, conforme descrito no exemplo abaixo:

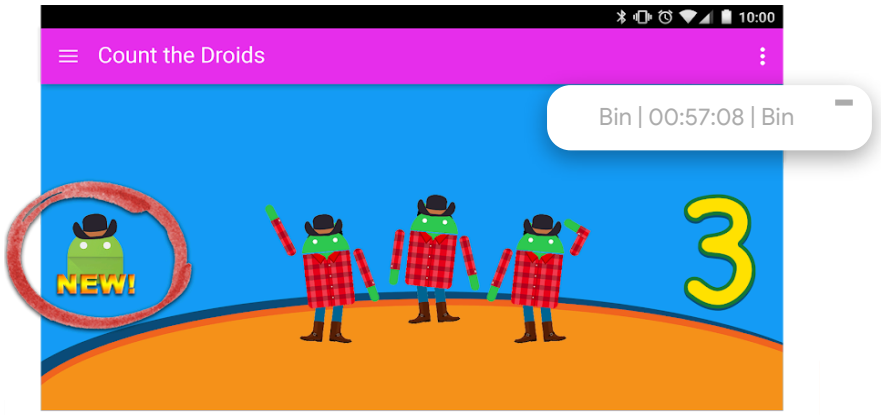
- Monetização e publicidade que ocupam a maior parte da tela do dispositivo sem fornecer ao usuário uma maneira clara de dispensá-lo, conforme descrito no exemplo abaixo:



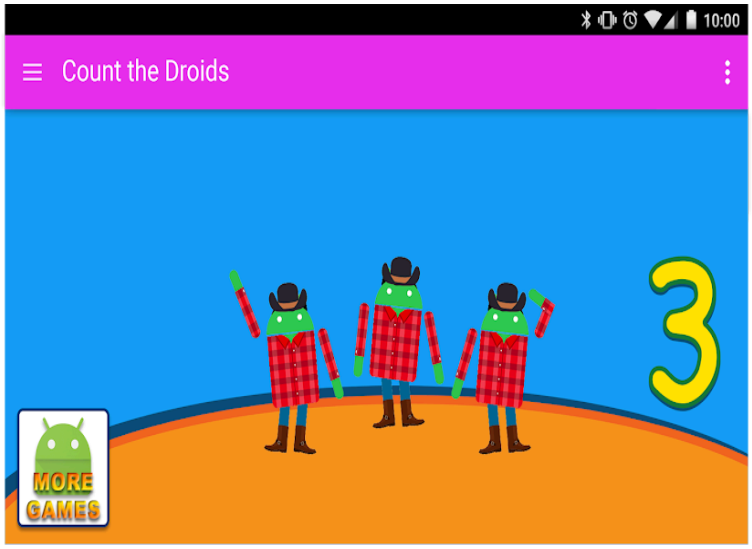
- Anúncios de banner que mostram várias ofertas, conforme mostrado no exemplo abaixo:



- Monetização e publicidade que podem ser confundidas com o conteúdo do app, conforme mostrado no exemplo abaixo:



- Botões, anúncios ou outra monetização que promovem outras páginas "Detalhes do app" do Google Play, mas que podem ser confundidos com o conteúdo do app, conforme mostrado no exemplo abaixo:



Veja alguns exemplos de conteúdo impróprio de anúncios que não podem ser exibidos para crianças.

- **Conteúdo de mídia impróprio:** são anúncios de programas de TV, filmes, álbuns de música ou qualquer outro meio de comunicação que não sejam apropriados para crianças.
- **Videogames e software para download impróprios:** são anúncios de videogames e software para download que não sejam apropriados para crianças.
- **Substâncias controladas ou prejudiciais:** são anúncios de bebidas alcoólicas, tabaco, substâncias controladas ou prejudiciais.
- **Jogos de azar:** são anúncios de simulações de jogos de azar, competições ou promoções de sorteios, mesmo com participação gratuita.
- **Conteúdo adulto e sexualmente sugestivo:** são anúncios com conteúdo sexual e para maiores.
- **Namoro ou relacionamentos:** são anúncios de sites de namoro ou de relacionamento para adultos.
- **Conteúdo violento**: são anúncios com conteúdo violento e imagens inadequadas para crianças.

SDKs de anúncio

Se você veicula anúncios no app, e o público-alvo dele só inclui crianças, use apenas os SDKs de anúncio autocertificados para famílias . Se o público-alvo do app inclui crianças e maiores, implemente medidas de triagem etária, como uma tela neutra de informações de idade . Além disso, os anúncios exibidos para crianças precisam vir exclusivamente de versões desses SDKs.

Saiba mais sobre esses requisitos na política do Programa de SDKs de anúncio autocertificados para famílias e consulte neste artigo a lista atual de versões desses SDKs.

Se você usar a AdMob, consulte a Central de Ajuda Bin | 00:57:08 | Bin talhes sobre os produtos dela.

É sua responsabilidade garantir que o app atenda a todos os requisitos relacionados a anúncios, compras no app e conteúdo comercial. Fale com os provedores dos seus SDKs de anúncio para saber mais sobre as políticas de conteúdo e práticas de publicidade deles.

Política de SDKs de anúncio autocertificados para famílias

O Google Play tem o compromisso de criar uma experiência segura para crianças e famílias. Uma parte importante disso é fazer com que as crianças só vejam anúncios apropriados para a idade, e que os dados delas sejam processados de maneira adequada. Para alcançar esse objetivo, exigimos que os SDKs de anúncio e as plataformas de mediação autocertifiquem que são apropriados para crianças e obedecem às Políticas do programa para desenvolvedores do Google Play e às Políticas para famílias do Google Play, o que inclui os requisitos do Programa de SDKs de anúncio autocertificados para famílias.

O Programa de SDKs de anúncio autocertificados para famílias do Google Play é uma maneira importante para os desenvolvedores identificarem quais desses SDKs de anúncio ou plataformas de mediação confirmaram que são adequados ao uso em apps feitos especialmente para crianças.

Fazer declarações falsas no SDK, incluindo no seu formulário de interesse, talvez resulte na remoção ou suspensão do SDK do Programa de SDKs de anúncio autocertificados para famílias. Por isso, é importante enviar informações precisas.

Requisitos da política

Caso seu SDK ou plataforma de mediação veicule apps que façam parte do programa para Famílias do Google Play, é preciso obedecer a todas as políticas para desenvolvedores do Google Play, inclusive os requisitos a seguir. O não cumprimento de qualquer requisito da política pode resultar na remoção ou suspensão do Programa de SDKs de anúncio autocertificados para famílias.

É sua responsabilidade garantir que o SDK ou a plataforma de mediação esteja em conformidade. Portanto, confira as Políticas do programa para desenvolvedores do Google Play, as Políticas para famílias do Google Play e os requisitos do Programa de SDKs de anúncio autocertificados para famílias.

1. **Conteúdo do anúncio**: anúncios disponíveis para crianças precisam ter conteúdo adequado a esse público-alvo.
   - É necessário (i) definir conteúdo e comportamentos de anúncios questionáveis e (ii) proibir esses elementos nos termos ou nas políticas. As definições precisam obedecer às Políticas do programa para desenvolvedores do Google Play.
   - Além disso, você precisa criar um método para classificar seus criativos de anúncios de acordo com grupos adequados à idade. É necessário incluir pelo menos grupos para "Todos" e "Adultos". A metodologia de classificação precisa estar de acordo com a oferecida pelo Google aos SDKs após o preenchimento do formulário de interesse.
   - É preciso garantir que, quando forem usados lances em tempo real para veicular anúncios a crianças, os criativos tenham sido revisados e obedeçam aos requisitos acima.
   - Além disso, é preciso ter um mecanismo para identificar visualmente os criativos provenientes do seu inventário, como incluir uma marca d'água no criativo do anúncio com um logotipo visual da empresa ou outra funcionalidade semelhante.
2. **Formato do anúncio**: é preciso garantir que todos os anúncios exibidos para usuários menores de idade sigam os requisitos de formato do anúncio para famílias, além de permitir que os

desenvolvedores selecionem formatos de anúncio que obedeçam à Política para famílias do Google Play.

- A publicidade não pode ter conteúdo enganoso [illegible] a que leve a cliques acidentais de crianças. É proibido usar anúncios [illegible] uário a clicar usando um botão "Dispensar" para acionar outro anúncio ou que aparecem repentinamente em áreas do app onde o usuário geralmente toca para outra função.
- Não é permitida a publicidade disruptiva, inclusive anúncios que ocupam a tela inteira ou interferem no uso normal e não incluem um meio claro de fechamento (por exemplo, paredes de anúncios).
- Se a publicidade interferir no uso normal do app ou jogo, inclusive anúncios premiados ou com permissão, o usuário precisa ter a opção de fechar o anúncio após 5 segundos.
- Não é permitido posicionar vários anúncios em uma página. Por exemplo, não são permitidos anúncios de banner que mostram várias ofertas em uma posição ou exibir mais de um banner ou anúncio em vídeo.
- A publicidade precisa ser claramente diferenciada do conteúdo do app. É proibido usar Offerwalls e experiências de anúncios imersivos que não sejam claramente identificáveis como publicidade por usuários menores de idade.
- Os anúncios não devem usar táticas chocantes ou que envolvem a manipulação emocional para incentivar a visualização.

3. **IBA/remarketing**: é necessário garantir que os anúncios exibidos para usuários menores de idade não envolvam publicidade com base em interesses (direcionada a usuários individuais que tenham determinadas características com base no comportamento de navegação on-line) nem remarketing (direcionada a usuários individuais com base na interação anterior com um app ou site).
4. **Práticas relacionadas a dados**: você, provedor de SDK, precisa ser transparente na forma como lida com os dados do usuário (por exemplo, dados coletados do usuário ou sobre ele, incluindo informações do dispositivo). É necessário divulgar como os SDKs acessam, coletam, usam e compartilham dados, bem como limitar o uso dessas informações às finalidades divulgadas. Além dessas exigências do Google Play, é preciso seguir os requisitos prescritos pelas legislações de privacidade e proteção de dados aplicáveis. Você precisa divulgar a coleta de todas as informações pessoais e sensíveis de crianças, incluindo, mas não se limitando a, informações de autenticação, dados do sensor da câmera e do microfone, dados do dispositivo, ID do Android e dados de uso de publicidade.
   - É preciso permitir que os editores tenham a opção de pedir o tratamento para direcionamento a crianças para veiculação de anúncios, por solicitação ou por app. Esse tratamento precisa obedecer a todas as legislações e regulamentações aplicáveis de proteção infantil, como a Lei de Proteção da Privacidade On-line das Crianças (COPPA) dos EUA e o Regulamento geral de proteção de dados (GDPR) da UE (links em inglês).
     - O Google Play exige que os SDKs do setor desativem anúncios personalizados, publicidade com base em interesses e remarketing como parte do tratamento para direcionamento a crianças.
   - Você precisa garantir que, quando forem usados lances em tempo real para veicular anúncios a crianças, os indicadores de privacidade sejam propagados para os bidders.
   - Não é permitido transmitir o AAID, número de série do chip, número de série, BSSID, MAC, SSID, IMEI e/ou IMSI de crianças ou usuários com idade desconhecida.
5. No caso de **plataformas de mediação**, é preciso obedecer aos requisitos abaixo ao veicular anúncios para crianças:
   - Use somente SDKs de anúncios autocertificados para famílias ou implemente as salvaguardas necessárias para garantir que todos os anúncios veiculados por mediação obedeçam a esses requisitos.
   - Transmita as informações necessárias para as plataformas de mediação a fim de indicar a classificação do conteúdo do anúncio e qualquer tratamento para direcionamento a crianças

aplicável.

6. **Autocertificação e compliance**: você precisa enviar ao Google informações suficientes, como as indicadas no formulário de interesse , para conf e anúncio obedece a todos os requisitos de autocertificação, incluindo, mas não se limitando a:
   - Incluir uma versão em inglês dos Termos de Serviço, da Política de Privacidade e do guia de integração do editor do SDK ou da plataforma de mediação
   - Enviar um app de teste com a versão compatível mais recente do SDK de anúncio. O app de teste precisa ser um APK Android completo e executável que use todos os recursos do SDK. Requisitos para apps de teste:
     - Ser enviado como um APK Android completo e executável em um formato de smartphone
     - Usar a versão mais recente do SDK ou uma a ser lançada em breve que esteja em conformidade com as políticas do Google Play
     - Usar todos os recursos do SDK, incluindo chamadas para buscar e exibir anúncios
     - Ter acesso total a todos os inventários de anúncios ativos/exibidos na rede por criativos solicitados pelo app de teste
     - Não ser restrito por geolocalização
     - Se seu inventário for destinado a um público-alvo misto, o app de teste vai precisar diferenciar solicitações de criativos de todo o inventário e aquele adequado para crianças ou todas as idades.
     - Ele não pode ser restrito a anúncios específicos no inventário, a menos que seja controlado pela tela neutra de informações de idade.
7. Você precisa responder em tempo hábil a solicitações de informações subsequentes e ter uma autocertificação de que todos os lançamentos de novas versões estejam em conformidade com as Políticas do programa para desenvolvedores do Google Play mais recentes, inclusive os requisitos da Política para famílias.
8. **Conformidade legal**: os SDKs de anúncio autocertificados para famílias precisam ser compatíveis com a veiculação de anúncios feita em conformidade com todos os estatutos e regulamentos relacionados a crianças e aplicáveis aos editores.
   - Você precisa garantir que o SDK ou a plataforma de mediação obedeça à Lei de Proteção da Privacidade On-line das Crianças (COPPA) dos EUA , ao Regulamento geral de proteção de dados (GDPR) da UE (links em inglês) e a qualquer outra legislação ou regulamento aplicável.

     Observação: a palavra "crianças" pode ter diferentes significados dependendo do local e do contexto. É importante que você consulte uma assessoria jurídica para determinar a que obrigações e/ou restrições de idade o app está sujeito. Você é quem mais sabe como seu conteúdo funciona. Por isso, contamos com sua colaboração em fazer com que os apps do Google Play sejam seguros para todas as famílias.

Consulte a página Programa de SDKs de anúncio autocertificados para famílias para conferir mais detalhes sobre os requisitos do programa.

Restrição

É sempre melhor evitar uma violação da política do que solucioná-la. No entanto, quando uma ocorre, temos o compromisso de explicar aos desenvolvedores como os apps deles podem voltar a estar em conformidade com nossas políticas. Entre em contato com nossa equipe se você identificar alguma violação ou tiver dúvidas sobre como solucioná-la .

Cobertura da política

Nossas políticas aplicam-se a qualquer conteúdo que o app do desenvolvedor exibe ou a que se vincula, incluindo quaisquer anúncios exibidos aos usuários e quaisquer conteúdos gerados por

usuários que o app hospeda ou a que se vincula. Da mesma forma, essas políticas se aplicam a qualquer conteúdo da conta de desenvolvedor que for exibido publicamente no Google Play, incluindo o nome do desenvolvedor e a página de destino do si

Bin | 00:57:08 | Bin

Não permitimos apps que possibilitam a instalação de outros apps nos dispositivos. Apps que fornecem acesso a outros apps, jogos ou software sem instalação, incluindo experiências e recursos fornecidos por terceiros, precisam garantir que todo o conteúdo fornecido esteja em conformidade com as políticas do Google Play. Além disso, esse material estará sujeito a análises adicionais de acordo com as políticas.

Os termos definidos usados nessas políticas têm o mesmo significado que aqueles utilizados no Contrato de distribuição do desenvolvedor (DDA). Além de estar em conformidade com essas políticas e a DDA, o conteúdo do app precisa ser classificado de acordo com nossas Diretrizes de classificação do conteúdo.

Não permitimos apps ou conteúdo que prejudicam a confiança do usuário no ecossistema do Google Play. Ao avaliar a inclusão ou remoção de apps do Google Play, consideramos diversos fatores, incluindo, mas não se limitando a um padrão de comportamento prejudicial ou alto risco de abuso. Identificamos o risco de abuso usando vários itens, como reclamações específicas sobre apps e desenvolvedores, relatórios de notícias, histórico de violações, feedback de usuários e o uso de marcas, personagens e outros recursos conhecidos.

Como funciona o Google Play Protect

O Google Play Protect verifica os apps quando você os instala. Ele também faz verificações periódicas no dispositivo. Se encontrar um app potencialmente nocivo, ele poderá realizar as seguintes ações:

- Enviar uma notificação para você. Para remover o app, toque na notificação e depois em "Desinstalar".
- Desativar o app até que ele seja desinstalado.
- Remover o app automaticamente. Na maioria dos casos, se um app nocivo for detectado, você receberá uma notificação informando que ele foi removido.

Como funciona a proteção contra malware

Para proteger você contra softwares e URLs maliciosos de terceiros, além de outros problemas de segurança, o Google pode receber informações sobre:

- conexões de rede do seu dispositivo;
- URLs potencialmente nocivos;
- sistema operacional e apps instalados no dispositivo por meio do Google Play ou de outras fontes.

Você pode receber um alerta do Google sobre um app ou URL potencialmente perigoso. O app ou URL poderá ser removido ou ter a instalação bloqueada pelo Google se for reconhecido como prejudicial para dispositivos, dados ou usuários.

É possível desativar certas proteções nas configurações do dispositivo. No entanto, talvez o Google continue recebendo informações sobre os apps instalados por meio do Google Play. Além disso, os apps instalados no seu dispositivo de outras fontes poderão ser verificados em busca de problemas de segurança sem o envio de informações ao Google.

Como funcionam os alertas de privacidade

O Google Play Protect enviará um alerta caso um app seja removido da Google Play Store por permitir o acesso às suas informações pessoais para que você possa desinstalá-lo.

Processo de restrição

Ao analisar conteúdo ou contas para determinar se eles são ilegais ou violam nossas políticas, tomamos decisões considerando várias informações, incluindo: metadados do app (por exemplo, título e descrição), experiência no app, informações da co[illegible] violações da política) e código de terceiros em apps, além de outr[illegible] anismos de denúncia (quando aplicável) e avaliações próprias. Ao usar código de terceiros (por exemplo, SDKs) no seu app, você é responsável por garantir que todo esse código usado no app, assim como as práticas dos terceiros em relação ao seu app, obedeçam a todas as Políticas do programa para desenvolvedores do Google Play.

Bin | 00:57:08 | Bin

Caso o app ou a conta de desenvolvedor viole uma das nossas políticas, vamos tomar as medidas cabíveis conforme descrito abaixo. Além disso, vamos apresentar informações relevantes sobre a medida a ser tomada por e-mail, junto com instruções sobre como contestar caso você acredite que nossa ação tenha sido um engano.

Talvez a remoção ou as notificações administrativas não contemplem todas as violações de políticas presentes no app ou no catálogo de apps em geral. Os desenvolvedores são responsáveis pela resolução de todos os problemas relativos às políticas e por garantir, com a devida diligência, que o restante do app ou da conta também esteja em total conformidade com as políticas. Não resolver violações da política na conta e em todos os seus apps pode resultar em ações adicionais de fiscalização.

Violações recorrentes ou graves dessas políticas (como malware, fraude e apps que podem causar danos ao usuário ou ao dispositivo) ou do Contrato de distribuição do desenvolvedor (DDA, na sigla em inglês) vão resultar no encerramento de contas de desenvolvedor do Google Play individuais ou relacionadas.

Ações de restrição

Cada aplicação da política pode afetar os apps de uma maneira diferente. Usamos uma combinação de avaliação automática e humana para analisar os apps e o conteúdo deles, com o objetivo de detectar e avaliar conteúdo que viole nossas políticas e seja prejudicial aos usuários e ao ecossistema do Google Play em geral. O uso de modelos automáticos permite detectar mais violações e avaliar possíveis problemas com mais rapidez, o que nos ajuda a manter o Google Play seguro para todos. O conteúdo que viola as políticas é removido pelos nossos modelos automáticos ou, quando é necessária uma avaliação mais detalhada, é sinalizado para análise adicional por operadores e analistas treinados, que conduzem avaliações de conteúdo. Isso ocorre, por exemplo, quando é necessário compreender o contexto do conteúdo. Os resultados dessas análises manuais são usados na criação de dados de treinamento para a melhoria dos nossos modelos de aprendizado de máquina.

Na seção a seguir, há uma descrição de várias ações que a plataforma pode realizar e o impacto delas em um app ou na conta de desenvolvedor do Google Play.

Salvo indicação em contrário em um aviso de restrição, essas ações afetam todas as regiões. Por exemplo, se o app for suspenso, ele vai ficar indisponível em todas as regiões. Além disso, salvo indicação em contrário, essas ações vão permanecer em vigor, a menos que você envie uma contestação e ela seja aceita.

Rejeição

- Um app novo ou uma atualização enviados para revisão não serão disponibilizados no Google Play.
- Se uma atualização de um app for rejeitada, a última versão publicada permanecerá disponível no Google Play.
- Isso não afeta o acesso às instalações do usuário, às estatísticas e às notas do app rejeitado.
- Também não afeta a situação da conta de desenvolvedor do Google Play.

Observação: não tente reenviar um app rejeitado até corrigir todas as violações da política.

Remoção

- O app e as versões anteriores dele vão ser removidos do Google Play e não vão estar mais disponíveis para download.
- Como o app é removido, os usuários não vão poder conferir a página "Detalhes do app". Essas informações vão ser restauradas depois que você enviar uma atualização do app removido em conformidade com a política.
- Talvez os usuários não consigam fazer compras no aplicativo nem utilizar recursos de faturamento em apps até que uma versão em conformidade com a política seja aprovada pelo Google Play.
- As remoções não afetam imediatamente a situação da sua conta de desenvolvedor do Google Play, mas várias remoções podem resultar em suspensão.

Observação: não tente publicar novamente um app removido até corrigir todas as violações da política.

Suspensão

- O app e as versões anteriores dele vão ser removidos do Google Play e não vão estar mais disponíveis para download.
- A suspensão pode ocorrer como resultado de violações graves ou repetidas das políticas, bem como por várias rejeições ou remoções do app.
- Como o app está suspenso, os usuários não vão ter acesso à página "Detalhes do app".
- Não é mais possível usar o APK nem o pacote do app suspenso.
- Os usuários não vão poder fazer compras no app nem usar os recursos do Faturamento do Google Play nele.
- As suspensões contam como avisos que afetam a situação regular da conta de desenvolvedor do Google Play. Quando há vários avisos, isso pode levar ao encerramento de contas de desenvolvedor do Google Play individuais e relacionadas.

Visibilidade limitada

- A detecção do app no Google Play é restrita. O app vai permanecer disponível no Google Play e poderá ser acessado por usuários com um link direto para a página "Detalhes do app".
- Colocar o app em um estado de visibilidade limitada não afeta a situação da sua conta de desenvolvedor do Google Play.
- Colocar o app em um estado de visibilidade limitada não afeta a capacidade dos usuários de conferir a página "Detalhes do app" atual.

Regiões limitadas

- O download do app no Google Play só está disponível em certas regiões.
- Os usuários de outras regiões não encontrarão o app na Play Store.
- As pessoas que instalaram o app anteriormente poderão continuar a usá-lo nos dispositivos, mas não receberão mais atualizações.
- A limitação de região não afeta a situação da sua conta de desenvolvedor do Google Play.

Estado de conta restrita

- Quando a conta de desenvolvedor está em estado restrito, todos os apps no catálogo são removidos do Google Play e não é possível publicar apps novos nem republicar os atuais. Você ainda vai ter acesso ao Play Console.
- Como todos os apps são removidos, os usuários não vão poder conferir a página "Detalhes do app" nem o Perfil do desenvolvedor.
- Os usuários atuais não vão poder fazer compras no app nem usar recursos de faturamento dos seus apps.

- Você ainda pode usar o Play Console para enviar mais dados ao Google Play e corrigir as informações da sua conta.
- Você vai poder republicar seus apps depois de cor lítica.

Bin | 00:57:08 | Bin

Encerramento da conta

- Quando a conta de desenvolvedor é encerrada, todos os apps no catálogo são removidos do Google Play e não é possível publicar novos apps. Isso também significa que todas as contas de desenvolvedor do Google Play associadas também são suspensas permanentemente.
- Várias suspensões ou suspensões por violações graves da política também podem resultar no encerramento da conta do Play Console.
- Como os apps na conta encerrada são removidos, os usuários não vão poder conferir a página "Detalhes do app" e o Perfil do desenvolvedor.
- Os usuários atuais não vão poder fazer compras no app nem usar recursos de faturamento dos seus apps.

Observação: todas as novas contas que você tentar abrir também vão ser encerradas (sem reembolso da taxa de registro do desenvolvedor). Portanto, não tente se inscrever em uma nova conta do Play Console quando uma das suas outras contas for encerrada.

Contas inativas

Contas inativas são contas de desenvolvedor que não estão ativas ou foram abandonadas. Essas contas não estão em situação regular conforme exigido pelo Contrato de distribuição do desenvolvedor .

As contas de desenvolvedor do Google Play são destinadas a desenvolvedores ativos que publicam e mantêm apps ativamente. Para evitar abusos, fechamos as contas inativas que não são usadas ou não apresentam atividade significativa (por exemplo, de publicação e atualização de apps, acesso a estatísticas ou gerenciamento de páginas "Detalhes do app", entre outras) regularmente.

Em caso de encerramento por inatividade, sua conta deixará de existir. Você não terá mais acesso aos relatórios, estatísticas, insights nem outras informações no Play Console, exceto se a conta inativa for restabelecida. A taxa de registro não é reembolsável e será perdida. Antes de encerrarmos sua conta inativa, avisaremos você usando as informações de contato fornecidas para essa conta.

O encerramento de uma conta inativa não impede você de criar uma nova conta no futuro, caso decida publicar no Google Play.

Gerenciamento e denúncia de violações da política

Contestar uma ação de restrição

Em caso de erro e se o app não violar as políticas do programa do Google Play e o Contrato de distribuição do desenvolvedor, todos os apps vão ser restabelecidos. Se você tiver analisado as políticas com atenção e acreditar que a ação pode ter sido um engano, siga as instruções fornecidas na notificação por e-mail de restrição ou clique aqui para contestar nossa decisão.

Recursos adicionais

Se você precisar de mais informações sobre uma ação de restrição ou uma nota/comentário de um usuário, consulte alguns dos recursos abaixo ou entre em contato por meio da Central de Ajuda do Google Play. No entanto, não podemos oferecer orientação jurídica ao desenvolvedor. Se você precisar de orientação jurídica, consulte um advogado.

- Verificação de apps

- Como denunciar uma violação de política
- Entrar em contato com o Google Play sobre o encerramento de uma conta ou a remoção de um app
- Avisos cordiais
- Denunciar comentários e apps impróprios
- Meu app foi removido do Google Play
- Para compreender os encerramentos das contas de desenvolvedor do Google Play

Bin | 00:57:08 | Bin

Requisitos do Play Console

Para garantir a segurança e proteção do nosso ecossistema de apps, o Google Play exige que todos os desenvolvedores atendam aos requisitos do Play Console, incluindo perfis vinculados à sua conta de desenvolvedor do Play Console. As informações verificadas serão exibidas no Google Play para ajudar a conquistar a confiança dos usuários. Saiba mais sobre as informações que aparecem no Google Play.

O Google Play oferece dois tipos de conta de desenvolvedor: pessoal e de organização. Selecionar o tipo certo de conta de desenvolvedor e concluir as verificações necessárias é fundamental para uma boa experiência de integração. Saiba mais sobre como escolher um tipo de conta de desenvolvedor.

Ao criar a conta do Play Console, os desenvolvedores precisam se inscrever como uma Organização caso forneçam os seguintes serviços:

- Produtos e serviços financeiros, incluindo, mas não se limitando a, serviços bancários, empréstimos, negociação de ações, fundos de investimento, corretoras de criptomoedas e carteiras de software de criptomoedas. Saiba mais sobre a política de serviços financeiros.
- Apps de saúde, como apps de medicina e apps de pesquisa em seres humanos. Saiba mais sobre as categorias de apps de saúde.
- Apps aprovados para uso da classe VpnService . Saiba mais sobre a política de serviço de VPN.
- Apps governamentais, incluindo apps desenvolvidos por um órgão governamental ou em nome dele.

Depois de selecionar um tipo de conta, faça o seguinte:

- Envie informações precisas da sua conta de desenvolvedor, incluindo os seguintes detalhes:
  - Nome civil e endereço
  - Número D-U-N-S , caso se registre como uma organização
  - Endereço de e-mail e número de telefone para contato
  - Endereço de e-mail e número de telefone do desenvolvedor exibidos no Google Play, quando aplicável
  - Formas de pagamento, quando aplicável
  - Perfil para pagamentos do Google vinculado à sua conta de desenvolvedor
- Para os desenvolvedores que se registram como uma organização, as informações da conta de desenvolvedor precisam estar atualizadas e condizer com os detalhes armazenados no perfil da Dun & Bradstreet.

Antes de enviar seu app, faça o seguinte:

- Envie com precisão todas as informações e metadados do app.
- Faça upload da Política de Privacidade do seu app e preencha os requisitos da seção "Segurança dos dados".
- Envie uma conta de demonstração ativa, além de informações de login e todos os outros recursos necessários para que o Google Play revise o app (especificamente, credenciais de login, QR code etc.)

Como sempre, garanta que o app ofereça uma experiência de usuário estável, envolvente e responsiva e verifique se todos os elementos dele, incluindo redes de publicidade, serviços de análise e SDKs de terceiros, estão em conformidade com as Políticas do programa para desenvolvedores do Google Play.

Caso o público-alvo do app inclua crianças, também é preciso estar em conformidade com a Política para famílias.

É sua responsabilidade ler o Contrato de distribuição Políticas do programa para desenvolvedores para garantir que o app esteja em total conformidade.

Bin | 00:57:08 | Bin

Developer Distribution Agreement

Precisa de mais ajuda?

Siga as próximas etapas:

Postar na Comunidade de Ajuda

Receba respostas dos membros da comunidade

Fale conosco

Conte mais sobre o problema para podermos ajudar você