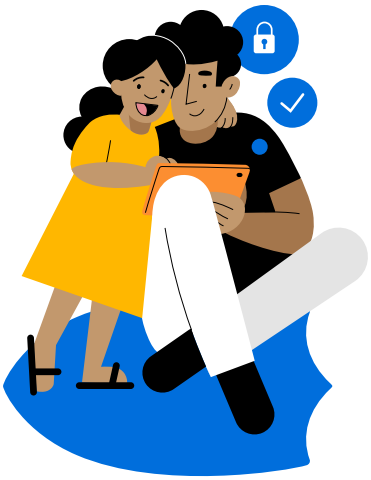


Construindo um ecossistema confiável para milhões de apps

O papel importante das proteções da App Store

Junho de 2021

2007

“Estamos tentando fazer duas coisas totalmente opostas ao mesmo tempo: fornecer uma plataforma aberta e avançada para os desenvolvedores e proteger os usuários do iPhone contra vírus, malware, ataques à privacidade etc. Não é uma tarefa fácil.”

Steve Jobs, 2007[1]

2016

“Use apenas o mercado de aplicativos oficial. Os usuários não (...) devem [baixar aplicativos] de fontes de terceiros, para diminuir o risco de instalar aplicativos maliciosos. Os usuários não devem fazer sideload de aplicativos se sua origem não for uma fonte autêntica e legítima.”

Agência da União Europeia para a Cibersegurança (ENISA), 2016[2]

2017

“As práticas recomendadas identificadas para atenuar ameaças de apps vulneráveis são relevantes para apps mal-intencionados e que invadem a privacidade. Além disso, os usuários devem evitar (e as empresas devem proibir nos seus aparelhos) o sideload de apps e o uso de lojas de apps não autorizadas.”

Relatório do Departamento de Segurança Nacional dos EUA, 2017[3]

Hoje, nossos telefones não são só telefones: eles guardam algumas das informações mais confidenciais da vida pessoal e profissional. Levamos nossos aparelhos para todo lugar e os usamos para fazer ligações e enviar mensagens às pessoas que amamos, tirar e guardar fotos dos nossos filhos, consultar itinerários quando estamos perdidos, contar os passos e enviar dinheiro para amigos. Eles estão ao nosso lado nos momentos felizes e quando acontecem emergências.

Criamos o iPhone pensando nisso. Projetamos a App Store como local para os desenvolvedores do mundo todo lançarem apps inovadores que alcançam uma comunidade global crescente e próspera de mais de um bilhão de usuários. Existem quase dois milhões de apps disponíveis para baixar na App Store, e outros milhares são adicionados toda semana. Devido à enorme dimensão da plataforma da App Store, garantir a segurança do iPhone é de extrema importância para nós desde o início. Profissionais de pesquisa em segurança concordam que o iPhone é o aparelho móvel mais seguro. Por isso, nossos usuários podem confiar nos seus aparelhos para guardar dados confidenciais. Adicionamos ao aparelho proteções integradas de ponta e criamos a App Store, um local confiável para os usuários descobrirem e baixarem apps com segurança. Na App Store, os apps vêm de desenvolvedores conhecidos que concordaram em seguir nossas diretrizes. Além disso, eles são distribuídos aos usuários sem a interferência de terceiros. Avaliamos cada app e cada atualização para verificar se atendem aos nossos altos padrões. Esse processo é aprimorado constantemente e foi criado para proteger nossos usuários. Ele ajuda a manter a App Store livre de malware, criminosos cibernéticos e fraudadores. Os apps desenvolvidos para o público infantil devem seguir diretrizes rigorosas de coleta de dados e segurança, criadas para manter as crianças seguras. Também devem ser integrados aos recursos dos controles parentais do iOS.

Acreditamos que, mais do que um fator importante, a privacidade é um direito humano fundamental. Esse princípio orienta os altos padrões de privacidade integrados aos nossos produtos: coletamos apenas os dados pessoais estritamente necessários para fornecer um produto ou serviço, deixamos o usuário no controle pedindo sua permissão antes que os apps acessem dados confidenciais e indicamos claramente quando os apps acessam alguns recursos, como microfone, câmera e a localização do usuário. Como parte do nosso compromisso contínuo com a privacidade, dois dos novos recursos — os dados de privacidade da App Store e a Transparência no Rastreamento em Apps — permitem que os usuários tenham um controle sem precedentes sobre sua privacidade, com mais transparência e informações para ajudá-los a fazer escolhas mais informadas. Graças a todas essas proteções, os usuários podem baixar qualquer app da App Store com tranquilidade. Essa tranquilidade também é vantajosa para os desenvolvedores, pois eles alcançam um público maior quando os usuários se sentem seguros para baixar seus apps.

Você sabia?

A Apple analisa todos os apps e atualizações na App Store para interceptar os que possam prejudicar os usuários. Entre eles, estão os apps que apresentam conteúdo inapropriado, invadem a privacidade dos usuários ou contêm malwares conhecidos, ou seja, softwares usados para fins mal-intencionados ou nocivos.

Um estudo monstrou que os aparelhos em execução no sistema Android foram 15 vezes mais infectados por softwares maliciosos do que o iPhone. O principal motivo é que os apps para Android "podem ser baixados de praticamente qualquer lugar", enquanto os usuários do iPhone em geral só podem baixar apps de um local: a App Store[4].

Nossa abordagem em relação à segurança e privacidade tem sido altamente eficaz. Hoje, é raríssimo um usuário encontrar malware no iPhone[5]. Algumas pessoas sugeriram que devemos criar maneiras para os desenvolvedores distribuírem seus apps fora da App Store, por meio de sites ou lojas de apps de terceiros. Esse processo é chamado de "sideload". Permitir o sideload diminuiria a segurança da plataforma iOS e deixaria os usuários expostos a sérios riscos, não apenas nas lojas de apps de terceiros, mas também na App Store. A base de usuários do iPhone é enorme e as pessoas armazenam dados confidenciais nos telefones, como fotos, localização, saúde e informações financeiras. Por isso, permitir o sideload promoveria uma enxurrada de novos investimentos em ataques à plataforma. Agentes mal-intencionados aproveitariam a oportunidade direcionando mais recursos para criar ataques sofisticados contra os usuários do iOS. Isso ampliaria o conjunto de explorações e ataques maliciosos, também conhecido como "modelo de ameaça", do qual todos os usuários precisam se proteger. O aumento do risco de ataques de malware deixa os usuários mais vulneráveis, mesmo aqueles que só baixam apps da App Store. Além disso, até os usuários que preferem baixar apps apenas da App Store poderiam ser forçados a baixar um aplicativo de que precisam para o trabalho ou para a escola em lojas de terceiros, caso não esteja disponível na App Store. Os usuários ainda poderiam ser enganados e baixar apps de lojas de terceiros pensando ser a App Store.

Estudos mostram que as lojas de apps de terceiros para aparelhos Android, onde os apps não estão sujeitos à verificação, são muito mais arriscadas e têm uma probabilidade maior de carregar malwares em comparação com as lojas de apps oficiais[6]. Como resultado, os especialistas em segurança desaconselham que os consumidores usem as lojas de terceiros porque elas não são seguras[3,7]. Permitir o sideload abriria as portas para um mundo em que os usuários talvez se sintam obrigados a aceitar os riscos, já que alguns apps não estarão mais disponíveis na App Store. Além disso, os usuários poderiam ser enganados por fraudadores e pensar que estão baixando aplicativos da App Store quando, na verdade, não estão. Fazer sideload deixaria os usuários expostos a fraudadores, que exploram os apps para enganá-los, invadem os recursos de segurança do iPhone e violam a privacidade dos usuários. Também diminuiria a confiança dos usuários no Pedir para Comprar, um recurso de controle parental em que os pais controlam os downloads de apps e compras em apps dos filhos, e no Tempo de Uso, uma ferramenta para gerenciar quanto tempo você e seus filhos passam nos seus aparelhos. Os fraudadores teriam a oportunidade de iludir e enganar pais e filhos ao ocultar a natureza dos apps, reduzindo a eficácia dos dois recursos.

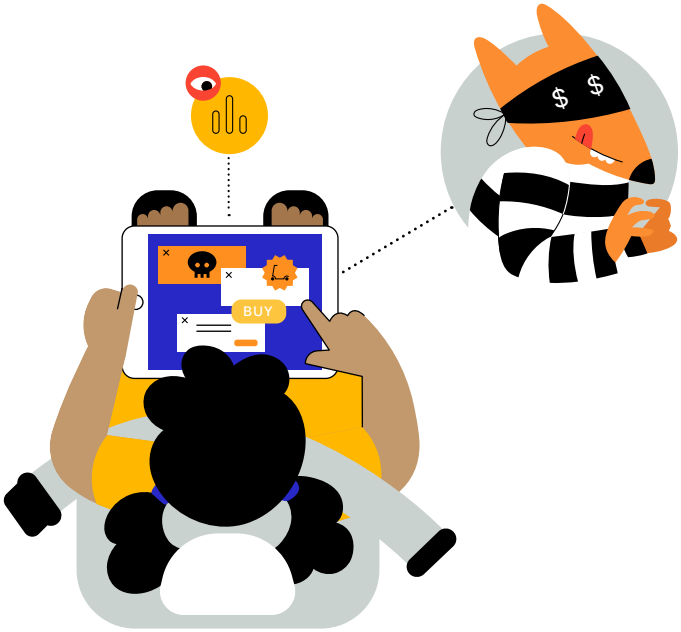
No final das contas, os usuários precisariam ficar sempre atentos a fraudes, sem saber em quem confiar, e muitos deles baixariam menos apps de menos desenvolvedores. Os próprios desenvolvedores ficariam mais vulneráveis a ameaças de agentes mal-intencionados, que poderiam oferecer ferramentas para desenvolvedores que contêm e propagam malware. Também estariam mais sujeitos à pirataria, prejudicando a capacidade de receber pagamento por seu trabalho.

Ataques reais a plataformas que permitem fazer sideload

Descobriu-se que apps do Android voltados para crianças estavam envolvidos em práticas de coleta de dados que violaram a privacidade das crianças. Esses apps continuam prosperando e estão disponíveis para os usuários do Android em lojas de apps de terceiros, mesmo depois de serem removidos da Google Play Store[8].

Agentes mal-intencionados colocaram anúncios inapropriados ou obscenos em apps direcionados a crianças[9].

Vamos ver como o dia a dia de uma família que usa o iPhone seria diferente com o sideload. Vamos acompanhar o dia de John e sua filha Emma, de sete anos, enquanto eles percorrem esse mundo de incertezas.



Um jogo instalado por sideload ignora os controles parentais

Emma pergunta a John se ela pode jogar um game que é popular entre seus colegas da escola. John procura o game na App Store, mas ele só está disponível em lojas de apps de terceiros. Isso deixa John desconfortável, mas ele baixa o jogo porque Emma quer muito, e a loja de terceiros afirma que o app é apropriado para crianças. Mais tarde, no caminho para o parque, enquanto Emma se diverte com o jogo no banco de trás do carro, o app mostra a ela muitos links de sites externos e anúncios direcionados. Quando baixou o jogo, John adicionou os dados do cartão de crédito ao comprar o pacote básico para Emma, mas não reparou que os controles parentais do recurso Pedir para Comprar não funcionariam nesse app instalado por sideload. Emma compra muitas vidas adicionais e itens especiais enquanto joga, sem perceber que seu pai não aprovou essas compras. O app também tem rastreadores de terceiros integrados, que coletam, analisam e vendem os dados de Emma a corretores de dados, mesmo que o app seja comercializado para crianças.

Ataques reais a plataformas que permitem fazer sideload

Sabe-se que apps instalados por sideload no Android executam ataques de ransomware "locker". Esses apps maliciosos, se instalados, bloqueiam o acesso do usuário ao telefone ou sequestram suas fotos, a menos que concorde em pagar um resgate[10,11].

Usuários do Android foram induzidos a usar métodos inseguros para baixar versões falsas de apps como Netflix e Candy Crush. Esses apps falsos, quando têm acesso ou exploram vulnerabilidades da plataforma, podem espionar usuários do Android pelo microfone, fazer capturas de tela dos aparelhos, ver a localização, mensagens de texto e contatos, roubar credenciais de login e fazer alterações nos telefones[12,13,14]. Outros são usados para roubar dados bancários e acessar as contas dos usuários[15,16,17,18].

Um golpe recente de ransomware envolve um app para Android disfarçado de aplicativo de rastreamento de contatos com COVID-19. Se instalado, ele criptografa todas as informações pessoais, deixando um endereço de e-mail para contato caso o usuário queira resgatar seus dados[19].

Um app encontrado em lojas de aplicativos para Android de terceiros engana os usuários fingindo ser uma atualização do sistema. Depois de instalado, o app exibe uma notificação informando que está procurando uma atualização, enquanto obtém acesso e rouba os dados pessoais do usuário, como mensagens, contatos e fotos[20,21].

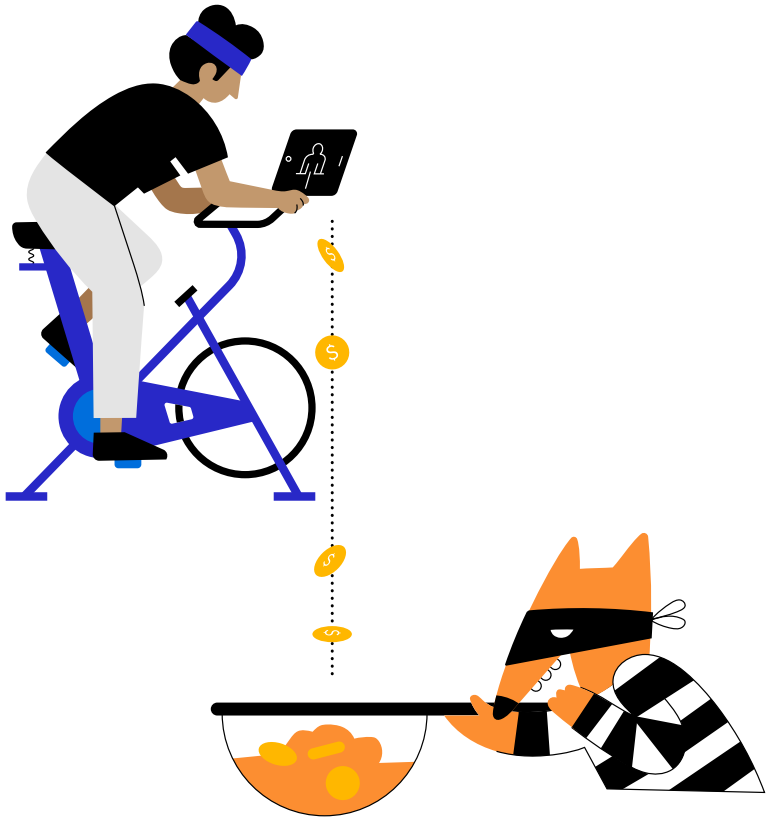
No parque, o app de filtro falso que John transferiu ameaça excluir todas as suas fotos, a menos que ele pague

Quando John e Emma estão no parque, John vê o anúncio de um app de filtro para selfies de um conhecido desenvolvedor de aplicativos. Ele decide baixar para se divertir com a filha. O anúncio leva a uma página para baixar o app que se parece com a página do desenvolvedor do aplicativo na App Store. John pensa estar protegido e não percebe que, na verdade, ele está baixando uma versão falsa do app de uma loja de aplicativos de terceiros. Como John acha que o app de filtro veio de um desenvolvedor conhecido e confiável, ele concede permissão para acessar as fotos. Assim que o aplicativo começa a ser executado, ele percebe que cometeu um erro. O aparelho ameaça excluir todas as fotos do rolo da câmera, a menos que ele insira as informações do cartão de crédito e pague um resgate. Graças às proteções integradas ao iPhone, John consegue controlar quais apps têm permissão para acessar as fotos, mas, neste caso, o aplicativo fraudulento o induziu a conceder acesso às suas fotos fingindo ser um app de filtro para selfies.

Ataques reais a plataformas que permitem fazer sideload

Pesquisas mostram que apps piratas publicados em lojas de aplicativos de terceiros custam aos desenvolvedores bilhões em receita perdida por ano[22].

Apps piratas e ilegítimos são comuns no Android. Esses apps incluem jogos que permitem trapacear (por exemplo, uma versão pirata do Pokémon Go com a capacidade de simular a localização), aplicativos modificados para fornecer acesso pirateado a conteúdo ou recursos exclusivos e apps de apostas ilegais e de conteúdo adulto[23,24,25].

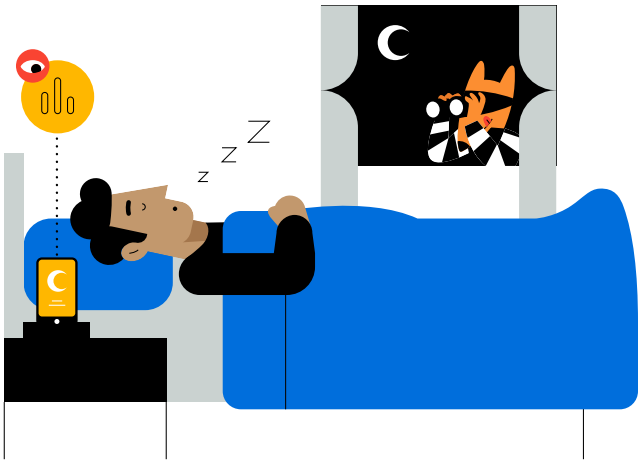


John, sem saber, baixa um app pirata de uma loja de aplicativos de terceiros

A amiga de John gostou muito de um app de fitness e decide enviar uma recomendação para que ele o experimente. Mas a indicação só funciona se ele baixar o app por meio de uma loja de aplicativos de terceiros, não pela App Store. Ele baixa o app e se inscreve com uma assinatura mensal. No entanto, o que nenhum deles percebeu foi que esse aplicativo tinha sido pirateado. Isso significa que o dinheiro que John paga todos os meses não vai para o desenvolvedor que projetou e criou o app, mas, sim, para os golpistas que roubaram o aplicativo. John acreditava estar fazendo a coisa certa – apoiando o desenvolvedor desse incrível app de fitness. Só que, na verdade, ele estava enchendo o bolso de criminosos, ajudando sem saber um esquema fraudulento que priva os desenvolvedores de seus ganhos.

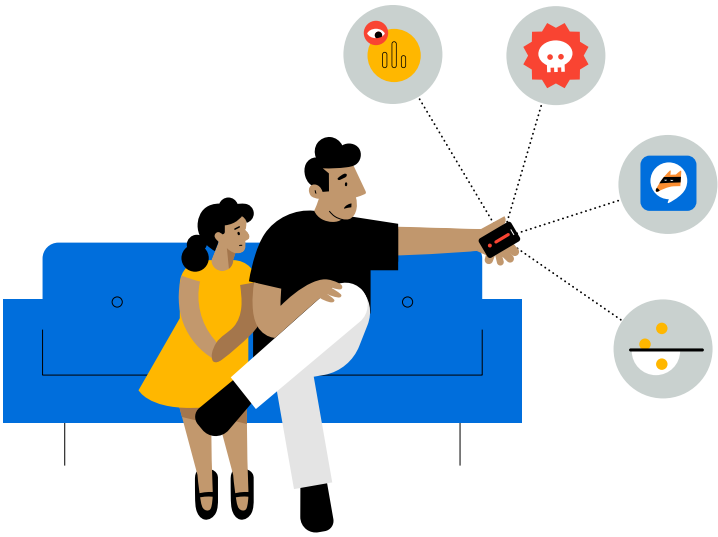
Saiba mais sobre as proteções de privacidade da Apple

Para saber mais sobre como a Transparência no Rastreamento em Apps e os dados de privacidade na App Store oferecem controle e clareza sobre como os aplicativos coletam e usam seus dados, leia **Um dia na vida dos seus dados** e acesse **apple.com/br/privacy/control.**



Um app fraudulento viola a privacidade de John

John ouviu falar de um novo aplicativo de monitoramento do sono que gostaria de experimentar, mas ele não está disponível na App Store. Ele faz o download de uma loja de aplicativos de terceiros, inscreve-se usando seu endereço de e-mail e começa a usá-lo para monitorar a qualidade do sono. O app declara que mantém os dados de saúde e utilização dos usuários totalmente privados e não os vincula a dados externos nem os compartilha com terceiros. No entanto, essa afirmação é completamente falsa. Como o aplicativo foi instalado por sideload, o desenvolvedor estava livre para fazer o que quisesse. O resultado foi que o app rastreou John usando o endereço de e-mail sem pedir a permissão dele. Isso permite ao desenvolvedor vincular os dados de John a informações coletadas de outros apps e vender os dados de saúde dele a corretores de dados, sem a permissão do usuário e sem ter que se preocupar em ser interrompido.



O iPhone é usado todos os dias por mais de um bilhão de pessoas – para operações bancárias, controle dos dados de saúde e para tirar fotos da família. Uma base de usuários desse tamanho é um alvo atraente e lucrativo para criminosos cibernéticos e fraudadores. Permitir o sideload geraria uma enxurrada de novos investimentos em ataques ao iPhone, muito além da escala de ataques em outras plataformas, como o Mac. Os golpistas seriam estimulados a desenvolver ferramentas e conhecimento para atacar a segurança do iPhone. A App Store foi projetada para detectar e bloquear os ataques atuais, mas mudar o modelo de ameaça seria uma forma de contornar essas proteções. Nesse caso, os fraudadores usariam as novas ferramentas e conhecimentos para atingir lojas de terceiros, bem como a App Store, o que colocaria todos os usuários em maior risco, mesmo quem só baixa aplicativos na App Store. Os canais de distribuição adicionais introduzidos por sideload fornecem aos agentes mal-intencionados maiores oportunidades de explorar as vulnerabilidades do sistema, incentivando os invasores a desenvolver e disseminar cada vez mais malware.

Isso significa que usuários como John, que já se acostumaram com a segurança e a proteção do iPhone e da App Store, teriam que estar sempre alertas quanto aos diferentes truques de criminosos cibernéticos e fraudadores, sem nunca saber em quem ou no que confiar. Em alguns casos, John pode não ter escolha a não ser correr o risco fazendo o sideload de um aplicativo que não está disponível na App Store de uma loja de terceiros, ou ele pode ser induzido a fazer isso. Nos casos mais graves, aplicativos falsos que fingem ser algo que não são – por exemplo, alegando ser uma atualização de software da Apple ou disfarçando a página de download para se parecer com a App Store – podem tentar violar as proteções do iPhone para obter acesso a dados protegidos, como mensagens, fotos e localização. Em razão de todos esses riscos e fraudes, John teria muito mais cuidado em relação a quais apps baixar. Como resultado, ele baixaria menos aplicativos e se limitaria aos de alguns desenvolvedores confiáveis, ficando mais difícil para os novos desenvolvedores menores alcançarem os usuários com apps originais e inovadores. Ele não teria a tranquilidade de saber que os apps no iPhone são as opções mais seguras para ele e para a filha.

Você sabia?

Os usuários que estão preocupados com a própria segurança e privacidade são mais propensos a baixar menos aplicativos e a excluir apps de seus aparelhos[26,27,28]**.** Um ecossistema menos confiável, onde os usuários não se sentem seguros para baixar apps, pode fazer com que as pessoas experimentem menos novos aplicativos inovadores ou deixem de testar aplicativos de desenvolvedores novos ou menos conhecidos. Isso pode frear o crescimento da economia dos apps, prejudicando tanto usuários quanto desenvolvedores.

As camadas de segurança da Apple e o processo de análise de apps protegem John, Emma e seus aparelhos

Para proteger os usuários do iOS de aplicativos maliciosos e fornecer a melhor segurança de plataforma do mundo, adotamos uma abordagem múltipla, com diversas camadas de proteção. O iOS apresenta desafios de segurança únicos porque os usuários fazem download contínuo e frequente de novos apps nos aparelhos e porque os aparelhos com iOS precisam ser seguros o suficiente para que as crianças os usem sem supervisão. Isso significa que adotamos uma abordagem mais acentuada em relação à segurança no iPhone em comparação com o Mac, pois a população de usuários, bem como seus comportamentos e expectativas, são diferentes.

- **Como no Mac, usamos software automatizado para verificar aplicativos em busca de malware conhecido, evitando que eles cheguem à App Store e, com isso, não consigam atingir nem prejudicar os usuários.**
- **Além disso, os desenvolvedores de apps devem enviar uma descrição do aplicativo e de seus recursos.** Uma equipe de especialistas revisa a precisão dessas informações durante o processo de análise do app, e os usuários têm acesso a elas na hora de decidir se querem ou não fazer o download de um aplicativo. Esse processo cria uma grande barreira contra os golpes mais comuns usados para espalhar malware: disfarçar o malware de app popular ou alegar que oferece recursos atraentes que não estão presentes.
- Além de verificar se os recursos do app funcionam conforme descrito e se a página da App Store do aplicativo é precisa, **esses especialistas também verificam manualmente se o app não solicita acesso desnecessário a dados confidenciais e avaliam se o conteúdo para crianças está em conformidade com as rigorosas regras de coleta de dados e segurança.**
- **Nos casos em que um aplicativo é aceito na App Store, mas posteriormente se descobre que ele viola nossas diretrizes, colaboramos com o desenvolvedor para resolver o problema logo.** Em casos perigosos, envolvendo fraude e atividades maliciosas, o aplicativo é imediatamente removido da App Store, e os usuários que fizeram o download podem ser notificados sobre o comportamento mal-intencionado do aplicativo.
- **Se um usuário tiver problemas com um aplicativo baixado da App Store, a equipe do AppleCare pode fornecer suporte e emitir reembolsos.**

O objetivo da análise de apps é garantir que os aplicativos na App Store sejam confiáveis e que as informações fornecidas na página da App Store de um aplicativo representem com precisão como o app funciona e quais dados ele acessará. Estamos sempre refinando esse processo ao atualizarmos e aprimorarmos continuamente nossas ferramentas e nossa metodologia.

Quando os usuários baixam um aplicativo pela App Store, eles podem controlar como o aplicativo funciona e quais dados ele pode acessar, usando recursos como Transparência no Rastreamento em Apps e permissões. Os pais podem controlar ainda mais o que seus filhos compram com o recurso Pedir para Comprar, quanto tempo eles passam em categorias específicas de apps com os recursos do Tempo de Uso e quais dados eles compartilham. Os usuários também podem fazer o controle centralizado de todos os pagamentos relacionados ao aplicativo, além de visualizar e cancelar assinaturas pagas por meio de Pagamentos no app. Não seria possível aplicar esses controles totalmente em apps instalados por sideload.

Além das proteções fornecidas pela equipe de App Review, desenvolvemos o hardware e o software de nossos aparelhos para fornecer uma última linha de defesa no caso de download de um aplicativo prejudicial. Por exemplo, os apps baixados no iPhone pela App Store são colocados em "sandbox", o que significa que não podem acessar arquivos armazenados por outros aplicativos nem fazer alterações no aparelho, a menos que o usuário dê sua permissão explícita.

A melhor defesa depende de uma combinação de todas as camadas: análise criteriosa de aplicativos para ajudar a evitar a instalação de apps maliciosos e proteções robustas da plataforma para limitar os danos que os aplicativos fraudulentos podem infligir. A segurança integrada ao iOS fornece aos usuários proteções sólidas que são as melhores de qualquer aparelho de consumo, mas essas proteções não são criadas para proteger contra as escolhas que um usuário pode ser induzido a fazer. A análise de apps dá força às políticas da App Store implantadas para proteger os usuários de aplicativos que podem tentar prejudicá-los ou induzi-los a conceder acesso a dados confidenciais. E, nos casos mais graves de apps maliciosos que tentam contornar as proteções no aparelho, a equipe de App Review dificulta o acesso aos aparelhos dos usuários.

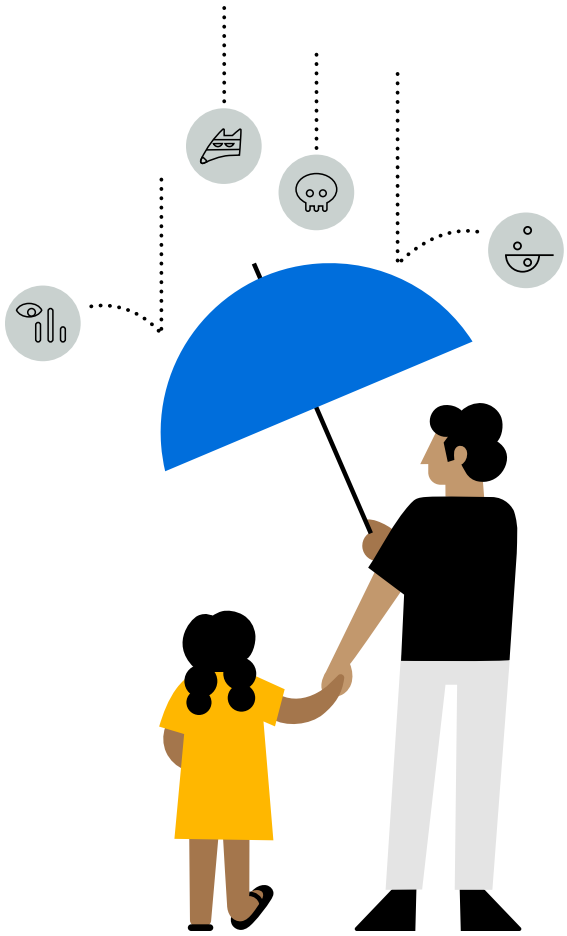
O resultado final é o consenso entre os especialistas em segurança de que o iPhone é o aparelho móvel mais seguro. As muitas camadas de segurança da Apple fornecem aos usuários um nível incomparável de proteção contra software malicioso, dando mais tranquilidade aos usuários.

App Review

Por meio do processo de análise de apps, trabalhamos para garantir que o conteúdo venha de fontes aprovadas e não inclua componentes nocivos conhecidos. Também verificamos se os apps não tentam induzir o usuário a fazer compras indesejadas ou dar acesso a dados pessoais. Avaliamos desenvolvedores e usuários e expulsamos quem não segue as regras. Embora os processos de análise de apps não impeçam a distribuição de todos os apps de baixa qualidade existentes, continuamos inovando e aprimorando a tecnologia, as práticas e os procedimentos.

Proteções da Apple para apps em 2020

- **Cem mil novos apps e atualizações são analisados por semana**, em média, por uma equipe com mais de 500 especialistas exclusivos que avaliam apps em diferentes idiomas.
- **Rejeição ou remoção de aproximadamente um milhão de apps novos com problemas e uma quantidade semelhante de atualizações:**
  - Mais de 150.000 por serem spam ou imitação, ou por enganar usuários
  - Mais de 215.000 por violarem as diretrizes de privacidade
  - Mais de 48.000 por incluir recursos ocultos ou não documentados
  - Cerca de 95.000 por violações relacionadas a fraude, principalmente por incluir propaganda enganosa para cometer crimes ou ações proibidas
- **A Apple impediu mais de US$ 1,5 bilhão em transações potencialmente fraudulentas.**
- **A Apple expulsou 470.000 equipes do Apple Developer Program por motivos relacionados a fraudes.** Além disso, rejeitou quase 205.000 tentativas de registro de desenvolvedor por suspeita de fraude.
- **A Apple desativou 244 milhões de contas de clientes por causa de atividade fraudulenta e abusiva, incluindo avaliações falsas.** Também rejeitou 424 milhões de tentativas de criação de conta por causa de padrões fraudulentos e abusivos.



Graças à equipe de App Review, John pode ficar tranquilo ao baixar os apps

Os recursos de segurança e privacidade da App Store garantem tranquilidade a John na hora de baixar apps para ele próprio e para a filha. John sabe que a Apple verifica todos os apps na App Store em busca de malware conhecido e que, comparado com outros aparelhos, é extremamente raro que usuários encontrem software malicioso no iPhone.

Saiba mais sobre as proteções da Apple

Para saber como a Apple protege sua segurança e privacidade na App Store, acesse **apple.com/br/app-store.**

Para saber como a Apple protege seus dados de localização, leia o documento sobre os **Serviços de Localização.**

Para saber mais sobre controles parentais no iOS, acesse **apple.com/br/families.**

Perguntas frequentes

O que é sideload?

"Sideload" é o processo de baixar e instalar em um aparelho móvel apps de outra fonte que não a App Store oficial, como um site ou uma loja de apps de terceiros. Para proteger a segurança e privacidade dos usuários, desde a concepção criamos o iPhone para não permitir que usuários comuns façam sideload.

O que é modelo de ameaça?

Modelo de ameaça é um conjunto de ataques e vulnerabilidades contra o qual os usuários precisam ser protegidos. Aparelhos, usuários e ambientes diferentes têm modelos de ameaça distintos, e é preciso planejar a segurança com isso em mente. A App Store é um componente fundamental da proteção contra o modelo de ameaça do iPhone. É um lugar de confiança para usuários baixarem com segurança apps analisados pela Apple, de desenvolvedores conhecidos que precisam obedecer às diretrizes da Apple.

Permitir sideload de sites e lojas de apps de terceiros no iPhone seria uma ameaça a usuários que só fazem download na App Store?

Sim. Ao oferecer outros canais de distribuição, mudar o modelo de ameaça e ampliar o conjunto de ataques possíveis, o sideload no iPhone colocaria todos os usuários em risco, inclusive aqueles que, em um esforço consciente para se proteger, só baixam apps pela App Store. Permitir essa prática estimularia uma enxurrada de novos investimentos em ataques ao iPhone, incentivando pessoas mal-intencionadas a produzir ferramentas e conhecimentos para enfraquecer a segurança do aparelho em um nível nunca visto. Depois de ganhar experiência criando ataques cada vez mais sofisticados, essas pessoas visariam lojas de terceiros e a App Store, colocando todos os usuários em enorme risco. Além disso, até os usuários que preferem baixar apps apenas da App Store poderiam ser forçados a baixar um aplicativo de que precisam para o trabalho ou para a escola em lojas de terceiros, caso não esteja disponível na App Store. Os usuários ainda poderiam ser enganados e levados a baixar apps de lojas de terceiros pensando ser a App Store.

Como é o processo de análise de apps da Apple?

Usamos uma combinação de tecnologia sofisticada e especialistas na análise criteriosa de cada app e cada atualização para avaliar se estão em conformidade com as rígidas diretrizes da App Store para privacidade e segurança. Recorremos aos especialistas quando a análise automática não é suficiente para detectar problemas específicos, como violações de privacidade ou apps infantis que não obedecem às nossas rigorosas diretrizes. Com o objetivo de proteger os usuários e proporcionar uma experiência superior na App Store, as diretrizes mudaram ao longo do tempo para responder a novas ameaças e desafios. Em média, 100.000 novos apps e atualizações são analisados semanalmente por uma equipe com mais de 500 especialistas exclusivos em todo o mundo.

O que é analisado?

Todos os apps e atualizações enviados para a App Store estão sujeitos ao processo de análise de apps.

Que controles parentais estão disponíveis nos aparelhos Apple?

Criamos recursos que permitem aos pais controlar como as crianças usam os aparelhos. O Tempo de Uso ajuda a entender melhor as horas que as crianças passam em apps, sites e aparelhos. Esse recurso também permite definir quanto tempo por dia elas podem passar em categorias de apps e sites. Além disso, os pais podem usar o Pedir para Comprar para aprovar ou recusar no próprio aparelho compras e downloads de apps que os filhos fazem. O Pedir para Comprar tem um tempo-limite de 15 minutos para impedir compras posteriores.

O que são os dados de privacidade e a Transparência no Rastreamento em Apps na App Store?

São recursos novos que oferecem aos usuários mais controle sobre os próprios dados e privacidade. A Transparência no Rastreamento em Apps exige que os apps peçam a permissão dos usuários antes de rastrear os dados entre apps ou sites de outras empresas. Com os dados de privacidade na App Store, exigimos que todo app mostre aos usuários um resumo simples das práticas de privacidade do desenvolvedor, apresentando informações importantes sobre como um app usa os dados.

Fontes

1. Jobs, Steve, "Third Party Applications on the iPhone", 17 de outubro de 2007, acessado via tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, "Vulnerabilities - Separating Reality from Hype", *Agência Europeia para a Segurança das Redes e da Informação*, 24 de agosto de 2016.

3. Griffin, Robert Jr., "Study on Mobile Device Security", *Departamento de Segurança Nacional dos EUA*, abril de 2017.

4. Nokia, "Threat Intelligence Report 2020", *Nokia*, 2020.

5. Johnson, Dave, "Can iPhones get viruses? Here's what you need to know", *Business Insider*, 4 de março de 2019.

6. Symantec, "Internet Security Threat Report, Volume 23", abril de 2018.

7. Golovin, Igor, "Malware in Minecraft mods: story continues", *Kaspersky*, 9 de junho de 2021.

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations", *Tech Crunch*, 23 de outubro de 2020.

9. Henry, Josh, "Malicious Apps: For Play or Prey?", *United States Cybersecurity Magazine*, 2021.

10. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it", *Avira*, 13 de agosto de 2020.

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices", *ThreatPost*, 24 de junho de 2020.

12. Owaida, Amer, "Trojan para Android se faz passar pelo app Clubhouse", *WeLiveSecurity by ESET*, 18 de março de 2021.

13. Desai, Shivang, "SpyNote RAT posing as Netflix app", *Zscaler*, 23 de janeiro de 2017.

14. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove", *The Washington Post*, 6 de novembro de 2015.

15. Palmer, Danny, "This Android trojan malware is using fake apps to infect smartphones, steal bank details", *ZDNet*, 1º de junho de 2021.

16. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks", *ThreatPost*, 21 de abril de 2020.

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on", *WeLiveSecurity* by ESET, 11 de dezembro de 2018.

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World", *Cybereason*, 1º de julho de 2020.

19. Stefanko, Lukas, "Ransomware se faz passar por app de rastreamento da COVID-19 e ESET cria decifrador", *WeLiveSecurity by ESET*, 24 de junho de 2020.

20. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'", *Zimperium*, 26 de março de 2021.

21. Aamir, Humza, "Beware of this newly discovered Android spyware that pretends to be a system update", *TechSpot*, 29 de março de 2021.

22. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy", *Forbes*, 2 de fevereiro de 2018.

23. Koetsier, John, "App Developers Losing $3-4 Billion Annually Thanks To 14 Billion Pirated Apps", *Forbes*, 24 de julho de 2017.

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit", *TorrentFreak*, 8 de janeiro de 2021.

25. Campaign for a Commercial-Free Childhood, "Apps which Google rates as safe for kids violate their privacy and expose them to other harms", 12 de dezembro de 2019.

26. J.P. Morgan, "2020 E-commerce Payments Trends Report: Japan", *J.P. Morgan*, 2020.

27. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019", 2019.

28. Gikas, Mike, "How to Protect Your Privacy on Your Smartphone", *Consumer Reports*, 1º de fevereiro de 2017.