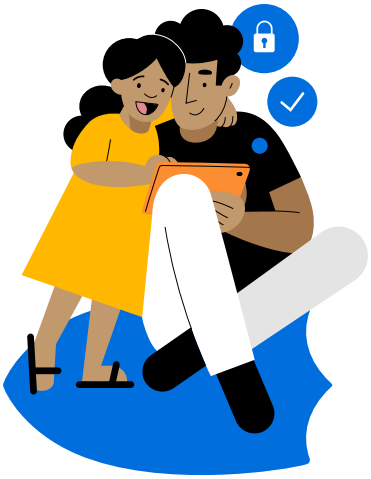


Een betrouwbaar ecosysteem voor miljoenen apps

Waarom de bescherming van de App Store zo belangrijk is

Juni 2021

2007

"We proberen twee dingen te doen die eigenlijk lijnrecht tegenover elkaar staan: ontwikkelaars een geavanceerd open platform bieden én iPhone-gebruikers beschermen tegen virussen, malware, enzovoort. Dat is niet eenvoudig."

Steve Jobs, 2007[1]

2016

"Gebruik alleen het officiële app-platform. Gebruikers downloaden best geen apps via andere kanalen. Zo minimaliseren zij het risico een kwaadaardige app te installeren. Ook horen gebruikers geen apps te sideloaden die niet van een legitieme, geverifieerde bron afkomstig zijn."

Agentschap van de Europese Unie voor cyberbeveiliging (ENISA), 2016[2]

2017

"De beste manieren die zijn vastgesteld voor het beperken van bedreigingen van kwetsbare apps zijn ook relevant voor kwaadaardige apps die het niet zo nauw nemen met de privacy. Daarnaast moeten gebruikers vermijden om apps te sideloaden en niet-goedgekeurde app-stores te gebruiken (en bedrijven moeten dit op hun devices verbieden)."

Rapport van het Amerikaanse ministerie van Binnenlandse Veiligheid, 2017[3]

De telefoon van nu is veel meer dan een telefoon. Tegenwoordig staan er allerlei gevoelige gegevens op over ons privéleven en ons werk. We hebben 'm altijd bij ons. We bellen, sms'en en appen ermee naar onze dierbaren. We nemen er foto's mee van onze kinderen. We vinden er de weg mee, tellen onze stappen en maken geld over. Onze telefoon is er op blije momenten en op momenten dat we hulp nodig hebben.

iPhone is vanuit die gedachte ontworpen. We hebben de App Store opgezet om ontwikkelaars wereldwijd een plek te bieden waar ze innovatieve apps kunnen bouwen en een bloeiende en groeiende groep van ruim een miljard gebruikers kunnen bereiken. Gebruikers kunnen bijna twee miljoen apps downloaden in de App Store, en daar komen er elke week nog eens duizend bij. Vanwege de omvang van het App Store-platform waren beveiliging en veilig gebruik van iPhone vanaf het begin van essentieel belang. Veiligheidsonderzoekers vinden iPhone het veiligste, best beveiligde mobiele device, waardoor gebruikers met een gerust hart hun gevoeligste gegevens erop kunnen zetten. We hebben de modernste beveiligingsmechanismen ingebouwd en de App Store opgezet, een betrouwbare plek waar gebruikers veilig apps kunnen ontdekken en downloaden. Alle apps in de App Store zijn gemaakt door bekende ontwikkelaars die met onze regels hebben ingestemd. Ze worden zonder tussenkomst van derden veilig onder gebruikers verspreid. We controleren elke app en elke update om te zien of ze aan onze strenge eisen voldoen. Dit proces, dat we continu verbeteren, is bedoeld om malware, cybercriminelen en oplichters uit de App Store te weren en zo onze gebruikers te beschermen. Apps voor kinderen moeten voldoen aan strenge eisen voor beveiliging en het verzamelen van gegevens. En ze moeten ook nauw geïntegreerd zijn met de features voor ouderlijk toezicht in iOS.

Privacy is voor ons méér dan alleen maar belangrijk: wij zien het als een fundamenteel mensenrecht. Op dat principe zijn de strenge privacynormen gebaseerd die we voor al onze producten hanteren: we verzamelen alleen die persoonsgegevens die strikt noodzakelijk zijn om een product of dienst te leveren. Daarbij geven we de gebruiker het roer in handen door apps om toestemming te laten vragen voordat ze toegang krijgen tot gevoelige gegevens. En we geven duidelijk aan wanneer apps bepaalde gevoelige functionaliteiten gebruiken, zoals de microfoon, de camera en de locatie van de gebruiker. Onlangs hebben we gebruikers nog meer controle over hun privacy gegeven in de vorm van twee nieuwe features: privacylabels in de App Store en transparantie bij tracking door apps. Dit zorgt voor nog meer inzicht en informatie, zodat ze weloverwogen keuzes kunnen maken. Dankzij al deze beschermingsvoorzieningen kunnen gebruikers met een gerust hart elke app in de App Store downloaden. Dit is ook goed nieuws voor ontwikkelaars, want zij bereiken zo een breed publiek dat hun apps zonder aarzelen downloadt.

Wist je dat?

Apple controleert alle apps en updates in de App Store om schadelijke software te onderscheppen. Denk aan apps met ongepaste content, of apps die lak hebben aan de privacy van de gebruiker of code bevatten die met slechte of gevaarlijke bedoelingen wordt gebruikt (malware).

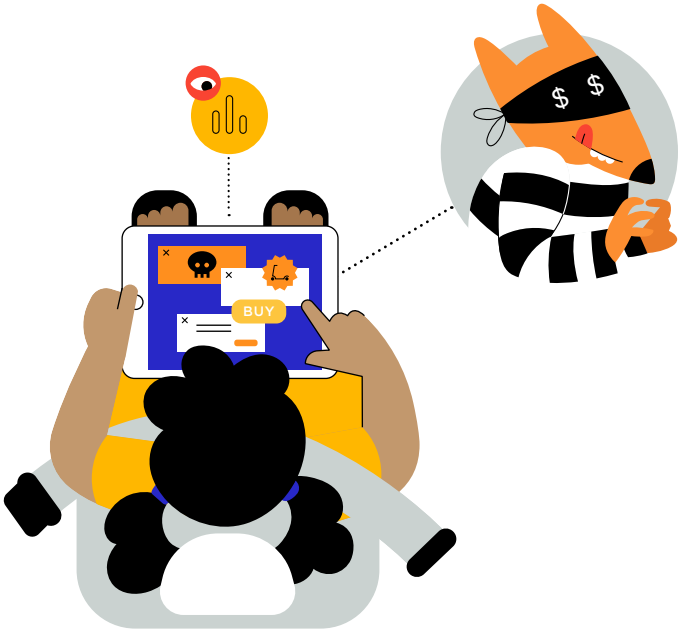
Onderzoek heeft aangetoond dat Android-devices 15 keer zoveel last hebben van malware als iPhones. De belangrijkste reden is dat Android-apps zo'n beetje overal kunnen worden gedownload, terwijl dat voor iPhone-gebruikers maar één plek is: de App Store.[4]

Deze benadering van beveiliging en privacy is bijzonder effectief gebleken. iPhone-gebruikers hebben maar heel zelden last van malware op hun toestel.[5] Nu gaan er stemmen op dat wij ontwikkelaars de gelegenheid moeten bieden om hun apps ook buiten de App Store te verspreiden, bijvoorbeeld op websites of in andere app-stores. Dit heet sideloaden. Als we sideloaden zouden toestaan, zou dit afbreuk doen aan de beveiliging van het iOS-platform, en gebruikers blootstellen aan ernstige beveiligingsrisico's. Niet alleen in die andere app-stores, maar ook in de App Store zelf. Gezien de grote doelgroep van iPhone-gebruikers en alle gevoelige gegevens op hun telefoon (foto's, locatiegegevens, informatie over gezondheid en financiën), zou het toestaan van sideloaden een nieuwe golf van aanvallen op het platform stimuleren. Kwaadwillende spelers zouden er meteen bovenop springen en nieuwe manieren bedenken om iOS-gebruikers aan te vallen. Die verzwaren dan het zogeheten bedreigingsmodel (threat model), het geheel van vormen van misbruik en aanvallen waartegen gebruikers moeten worden beschermd. Dit verhoogde risico werkt door voor alle gebruikers, zelfs voor degenen die hun apps alleen in de App Store downloaden. Bovendien kunnen gebruikers die hun apps het liefst in de App Store downloaden, zich dan genoodzaakt zien om een app voor hun werk of voor school ergens anders te downloaden als deze niet in de App Store staat. Of ze kunnen slachtoffer worden van andere app-stores die zich als de App Store voordoen.

Onderzoek toont aan dat onofficiële app-stores voor Android-devices, waar de apps niet worden gecontroleerd, veel meer risico inhouden dan een officiële app-store. De kans op malware is ook groter.[6] Beveiligingsexperts raden consumenten dan ook af om dit soort app-stores te gebruiken omdat ze niet veilig zijn.[3, 7] Als we sideloaden zouden toestaan, kunnen er situaties ontstaan waar gebruikers deze risico's voor lief moeten nemen, omdat bepaalde apps niet meer in de App Store staan. En oplichters zouden hen kunnen laten denken dat ze veilig apps in de App Store downloaden, terwijl dat niet zo is. Sideloaden vergroot de kans dat gebruikers slachtoffer worden van oplichters die met hun app de beveiliging van iPhone aanvallen en de privacy van de gebruiker schenden. Gebruikers kunnen ook minder vertrouwen op 'Vraag om te kopen', een optie waarmee ouders in de gaten kunnen houden welke apps hun kinderen downloaden en welke in-app-aankopen ze doen. Dat geldt ook voor 'Schermtijd', een feature die bijhoudt hoeveel tijd zij zelf en hun kinderen met hun device bezig zijn. Deze features zouden minder effectief worden en oplichters meer kans geven om kinderen en hun ouders om de tuin te leiden.

Het zou erop uitdraaien dat gebruikers constant op hun hoede moeten zijn, nooit weten wie of wat ze kunnen vertrouwen en uiteindelijk minder apps van minder ontwikkelaars zouden downloaden. Op hun beurt worden ook ontwikkelaars kwetsbaarder voor bedreigingen van kwaadwillende spelers, doordat zij hun besmette tools met malware verstrekken. Hetzelfde geldt voor plagiaat, waardoor ontwikkelaars niets betaald krijgen voor hun werk.

Laten we eens kijken hoe een gezin een heel andere iPhone-ervaring zou hebben als sideloaden een optie was. We kijken een dag mee met John en zijn zevenjarige dochter Emma, die hun weg moeten vinden in een minder zekere wereld.



Een gesideloade game omzeilt ouderlijk toezicht

Emma vraagt John of ze een game mag spelen waar haar vrienden op school het over hadden. John zoekt de game in de App Store, maar de ontwikkelaar biedt deze alleen aan via andere app-stores. John is er niet gerust op, maar hij downloadt de game toch omdat Emma hem zo graag wil proberen en omdat de app-store claimt dat de game geschikt is voor kinderen. Later die dag gaan ze naar het park. Onderweg zit Emma de game op de achterbank te spelen. Ze krijgt allerlei links naar websites te zien en gerichte reclame. John had zijn creditcardgegevens ingevoerd om een starter pack te kopen. Wat hij zich niet realiseerde, was dat de optie 'Vraag om te kopen' bij deze gesideloade app niet werkt. Emma koopt al spelend dan ook vele extra's, zonder dat ze zich ervan bewust is dat haar vader die aankopen niet had goedgekeurd. De app bevat ook trackers die de gegevens van Emma verzamelen, analyseren en verkopen aan andere bedrijven, ook al was duidelijk aangegeven dat het om een app voor kinderen ging.

Waargebeurde aanvallen op platforms die sideloaden toestaan

Android-apps voor kinderen bleken gegevens te verzamelen die de privacy van kinderen schonden. Deze apps zijn weliswaar uit de Google Play Store verwijderd, maar via andere app-stores kunnen ze nog steeds Android-gebruikers benadelen.[8]

Kwaadwillende spelers hebben ongepaste of onzedelijke advertenties geplaatst in apps voor kinderen.[9]

Waargebeurde aanvallen op platforms die sideloaden toestaan

Gesideloade apps op Android-devices staan bekend om een specifiek soort ransomware-aanvallen. Gebruikers hebben dan geen toegang meer tot hun telefoon of foto's, tenzij ze geld betalen.[10, 11]

Android-gebruikers worden er op slinkse wijze toe aangezet om via onveilige methodes namaakversies van apps als Netflix of Candy Crush te downloaden. Die namaakapps kunnen bijvoorbeeld Android-gebruikers via de microfoon afluisteren, screenshots van hun device nemen, hun locatie, sms'jes en contacten inzien, hun inloggegevens stelen en instellingen veranderen.[12, 13, 14] Andere apps stelen bankgegevens en breken dan in op de bankrekening van de gebruiker.[15, 16, 17, 18]

Onlangs nog is een Android-app opgedoken die zich voordoet als een app voor contactonderzoek in verband met COVID-19. De app versleutelt alle persoonlijke gegevens en toont dan een e-mailadres waar de gebruiker een bericht heen moet sturen om weer bij de data te kunnen.[19]

In een onofficiële Android-app-store is een app aangetroffen die zich als systeemupdate voordoet. Na de installatie ziet de gebruiker de melding 'Searching for update' en intussen gaat de app met persoonlijke gegevens van de gebruiker aan de haal, zoals berichten, contacten en foto's. [20, 21]

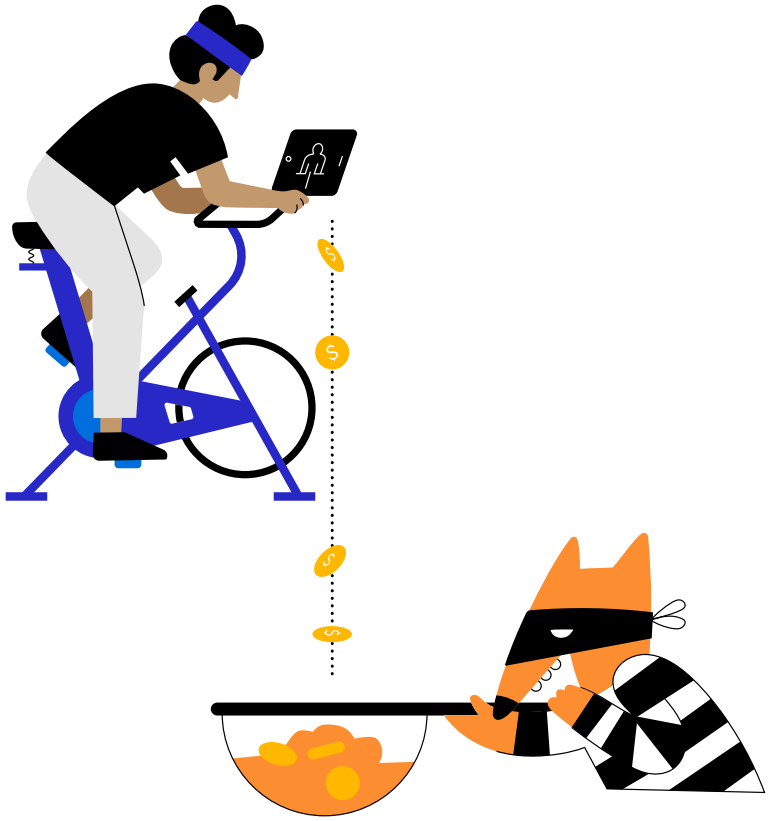
In het park moet John geld betalen, anders verwijdert de gesideloade app al zijn foto's

Eenmaal in het park aangekomen, ziet John een advertentie voor een selfiefilterapp van een bekende ontwikkelaar die hem wel leuk lijkt voor Emma. Hij klikt op de advertentie en komt terecht op een pagina die eruitziet als de pagina van de ontwikkelaar in de App Store. John denkt dat hij veilig bezig is en beseft niet dat hij een namaakversie in een onofficiële app-store downloadt. Omdat John denkt dat deze filterapp van een bekende ontwikkelaar met een goede reputatie komt, geeft hij de app toegang tot zijn foto's. Al gauw ziet hij zijn vergissing in: de app dreigt alle foto's op zijn camerarol te verwijderen, tenzij John zijn creditcardgegevens invoert en een bepaald bedrag overmaakt. iPhone is zo beschermd dat John zelf kan beslissen welke apps toegang krijgen tot zijn foto's. Maar in dit geval was er sprake van valse voorwendselen.

Waargebeurde aanvallen op platforms die sideloaden toestaan

Onderzoek toont aan dat ontwikkelaars per jaar miljarden dollars door de neus worden geboord door namaakapps, aangeboden via onofficiële kanalen.[22]

Android-devices hebben veel last van nepapps. Denk bijvoorbeeld aan games waarin je kunt valsspelen (zoals een namaakversie van Pokémon Go waarin je locatie kan worden gesimuleerd), apps die toegang geven tot premium content of features, illegale gokapps of apps met expliciete content.[23, 24, 25]

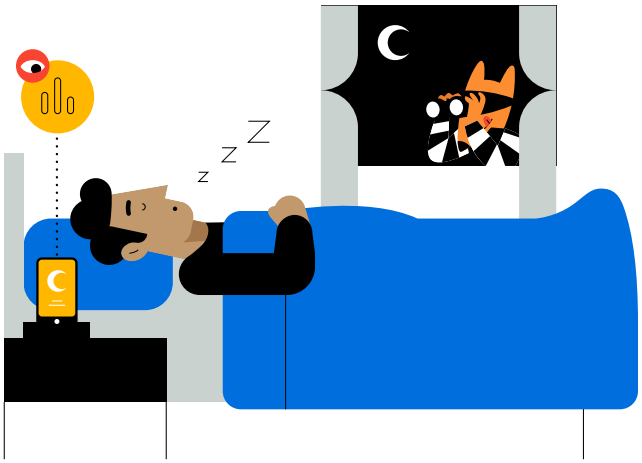


John downloadt onbewust een namaakapp in een onofficiële app-store

Een vriendin van John wil hem als lid aanmelden bij een fitness-app die zij graag gebruikt. John moet de app dan wel via een onofficieel kanaal downloaden, dus niet via de App Store. Hij downloadt de app en neemt een maandabonnement. Wat ze beiden niet weten, is dat ze een namaakapp gebruiken. Zijn maandelijkse lidmaatschapsgeld gaat niet naar de ontwikkelaar van de oorspronkelijke app, maar naar de oplichters die de app hebben gestolen. John dacht dat hij keurig de ontwikkelaar betaalde voor een geweldig product, maar in plaats daarvan spekt hij de portemonnee van een oplichter en zien de ontwikkelaars dat geld aan hun neus voorbij gaan.

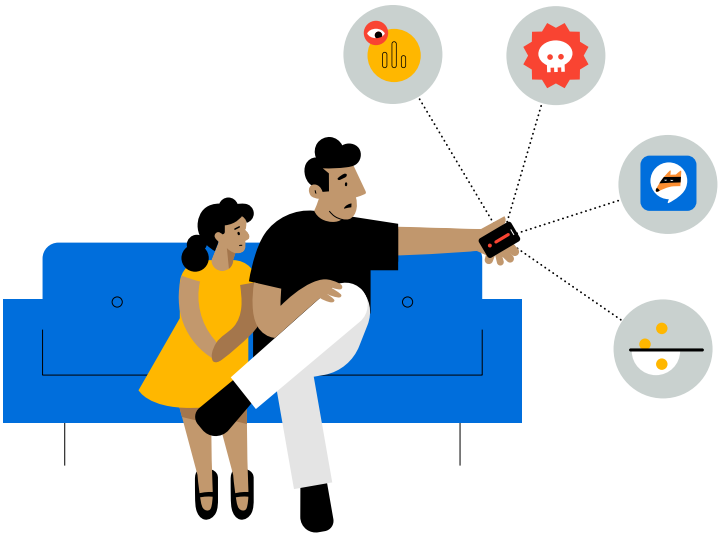
Meer informatie over de privacybescherming van Apple

Wil je meer weten over transparantie bij tracking door apps en de privacylabels in de App Store? Lees dan **A Day in the Life of Your Data** (Engelstalig) en ga naar **apple.com/benl/privacy/control** om te zien hoe je daarmee grip houdt op welke apps jouw gegevens verzamelen en gebruiken.



Een gesideloade app maakt inbreuk op Johns privacy

John wil een nieuwe app voor slaappatronen proberen, maar die staat niet in de App Store. Hij downloadt de app ergens anders, logt in met zijn e-mailadres en gebruikt de app om zijn slaapgedrag te volgen. De app zou de gezondheids- en gebruiksgegevens van de gebruiker strikt privé houden en deze niet aan externe gegevens koppelen of met anderen delen. Maar dat blijkt helemaal niet waar te zijn. Omdat de app is gesideload, kan de ontwikkelaar zijn gang gaan. De app volgt Johns doen en laten dan ook aan de hand van zijn e-mailadres en zonder zijn medeweten. Hierdoor kan de ontwikkelaar deze gegevens aan informatie uit andere apps koppelen en de gezondheidsgegevens van John verkopen. De ontwikkelaar heeft John nooit om toestemming gevraagd en niets of niemand houdt hem tegen.



Meer dan een miljard mensen gebruiken hun iPhone elke dag – voor internetbankieren, om hun gezondheidsgegevens te beheren en om foto's van hun gezin te nemen. Zo'n grote doelgroep is een aantrekkelijk en lucratief doelwit voor cybercriminelen en oplichters. Als we sideloaden toestaan, zou iPhone ten prooi vallen aan een nieuwe golf aanvallen op een veel grotere schaal dan op bijvoorbeeld Mac. Oplichters zouden hun kans schoon zien en investeren in nieuwe tools en kennis om de beveiliging van iPhone te doorbreken. De App Store is bedoeld om aanvallen van dit moment te detecteren en te blokkeren, maar een nieuw bedreigingsmodel zou die bescherming tenietdoen. Oplichters zouden met hun nieuwe tools en kennis zowel onofficiële kanalen als de App Store zelf bestoken, waardoor alle gebruikers meer risico's lopen, zelfs degenen die hun apps enkel in de App Store downloaden. De extra distributiekanalen die sideloaden met zich meebrengt, bieden kwaadwillende spelers meer mogelijkheden om de kwetsbaarheden van het systeem uit te buiten, waardoor meer malware wordt gemaakt en verspreid.

Dit betekent dat gebruikers als John, die de veiligheid en bescherming van iPhone en de App Store gewend was, constant op hun hoede moeten zijn voor de praktijken van cybercriminelen en oplichters, en nooit weten wie of wat ze kunnen vertrouwen. Soms zal John zich dan genoodzaakt zien om het risico te nemen en een app te sideloaden als deze niet in de App Store staat. Of hij doet dat zonder dat hij zich daarvan bewust is. In het ergste geval kunnen gesideloade apps die zich anders voordoen (bijvoorbeeld als een Apple software-update of als een downloadpagina in de App Store) de on-device beveiliging van iPhone doorbreken en toegang krijgen tot afgeschermde gegevens zoals berichten, foto's en locatiegegevens. Met al deze risico's en oplichterspraktijken zou John zich wel tweemaal bedenken voor hij een app downloadde. Uiteindelijk zou hij minder apps downloaden en zich beperken tot apps van een paar betrouwbare ontwikkelaars. Voor nieuwe, kleinere ontwikkelaars zou het dan lastiger worden om innovatieve nieuwe apps aan de man te brengen. John zou niet de geruststelling hebben dat apps op iPhone de veiligste opties zijn voor hem en zijn dochter.

Wist je dat?

Gebruikers die niet gerust zijn op hun beveiliging en privacy zijn geneigd minder apps te downloaden en vaker apps van hun device te verwijderen.[26, 27, 28] Een minder veilig ecosysteem waarin gebruikers terughoudend zijn met het downloaden van apps kan ertoe leiden dat gebruikers minder geneigd zijn om innovatieve apps of apps van nieuwe of minder bekende ontwikkelaars uit te proberen. Dat zou de groei van de app-economie remmen, een slechte zaak voor zowel gebruikers als ontwikkelaars.

De beveiligingslagen van Apple en het App Review-proces beschermen John en Emma en hun devices

Om iOS-gebruikers tegen kwaadwillende apps te beschermen en de beste platformbeveiliging ter wereld te bieden, hanteren we een meervoudige aanpak met vele beschermingslagen. iOS beveiligen is een unieke uitdaging, omdat gebruikers constant nieuwe apps op hun device downloaden én iOS-devices veilig genoeg moeten zijn voor zelfstandig gebruik door kinderen. Dit betekent dat we de beveiliging van iPhone nog serieuzer aanpakken dan die van Mac, omdat het om andere gebruikers met andere gewoonten en verwachtingen gaat.

- **Net als op Mac gebruiken we geautomatiseerde software om apps op bekende malware te scannen. Zo halen dat soort apps de App Store niet eens en blijven gebruikers ervan gevrijwaard.**
- **Verder moeten ontwikkelaars een beschrijving van de app en de features meeleveren.** Een team van experts kijkt tijdens het App Review-proces of deze informatie klopt. Gebruikers krijgen deze informatie te zien en kunnen op grond daarvan besluiten de app wel of niet te downloaden. Dit proces werpt een hoge barrière op tegen veelvoorkomende oplichterspraktijken bij de verspreiding van malware, zoals de malware verpakken als een populaire app of aanlokkelijke features beloven die niet worden waargemaakt.
- Naast de features van de app en de pagina in de App Store **controleren deze experts ook handmatig of de app niet onnodig om toegang tot gevoelige gegevens vraagt. Ook beoordelen zij of apps die op kinderen gericht zijn zich wel aan de strenge regels voor gegevensverzameling en veiligheid houden.**
- **Wanneer later blijkt dat een app die al tot de App Store is toegelaten toch onze regels overtreedt, lossen we het probleem snel op in overleg met de ontwikkelaar.** Als dat gevaarlijke situaties oplevert, bijvoorbeeld fraude of kwaadwillende activiteiten, wordt de app meteen uit de App Store verwijderd. Gebruikers die de app hebben gedownload, kunnen worden gewaarschuwd.
- **Als gebruikers problemen ervaren met een app die in de App Store is gedownload, kunnen zij bij Apple Care terecht voor hulp en restitutie.**

Het App Review-proces moet ervoor zorgen dat apps in de App Store betrouwbaar zijn en dat de informatie op de app-pagina in de App Store waarheidsgetrouw aangeeft hoe de app werkt en welke gegevens de app wil inzien. We stellen dit proces voortdurend bij: we updaten en perfectioneren onze tools en manier van werken constant.

Zodra gebruikers een app in de App Store hebben gedownload, kunnen ze zelf bepalen hoe die app functioneert en tot welke gegevens die app toegang heeft. Daar zijn features als transparantie bij tracking door apps en bevoegdheden voor bedoeld. Bovendien kunnen ouders bepalen wat hun kinderen kunnen kopen ('Vraag om te kopen'), hoeveel tijd zij in bepaalde categorieën apps spenderen ('Schermtijd') en welke gegevens zij delen. Gebruikers kunnen bovendien alle appgerelateerde betalingen centraal regelen en abonnementen die via in-app-betalingen worden voldaan, inzien en opzeggen. In gesideloade apps kunnen deze instellingen niet onverkort worden afgedwongen.

Naast de bescherming van het App Review-proces zijn de hardware en software van onze devices zo ontworpen dat zij een laatste verdedigingslinie vormen, mocht iemand toch een schadelijke app op een device downloaden. Downloads van apps in de App Store op een iPhone worden in een zogeheten sandbox uitgevoerd. Dit houdt in dat ze geen toegang hebben tot bestanden van andere apps en niets op het device kunnen veranderen tenzij de gebruiker daar nadrukkelijk toestemming voor geeft.

De beste verdediging berust op het geheel van alle lagen: een grondige App Review om de installatie van kwaadwillende apps te voorkomen en een sterke bescherming van het platform om de schade door zulke apps in te perken. Dankzij de ingebouwde iOS-beveiliging profiteren gebruikers van de beste beschermingsvoorzieningen op een consumentendevice, maar die zijn er niet op berekend om gebruikers te beschermen tegen keuzes die zij maken wanneer ze worden misleid. Het App Review-proces is de concrete manier waarop de App Store gebruikers beschermt tegen apps die schade kunnen berokkenen of die onder valse voorwendselen toegang tot gevoelige gegevens vragen. En wanneer kwaadwillende apps de on-device beschermingsvoorzieningen proberen te omzeilen, maakt de App Review het die apps moeilijker om überhaupt op het device van gebruikers terecht te komen.

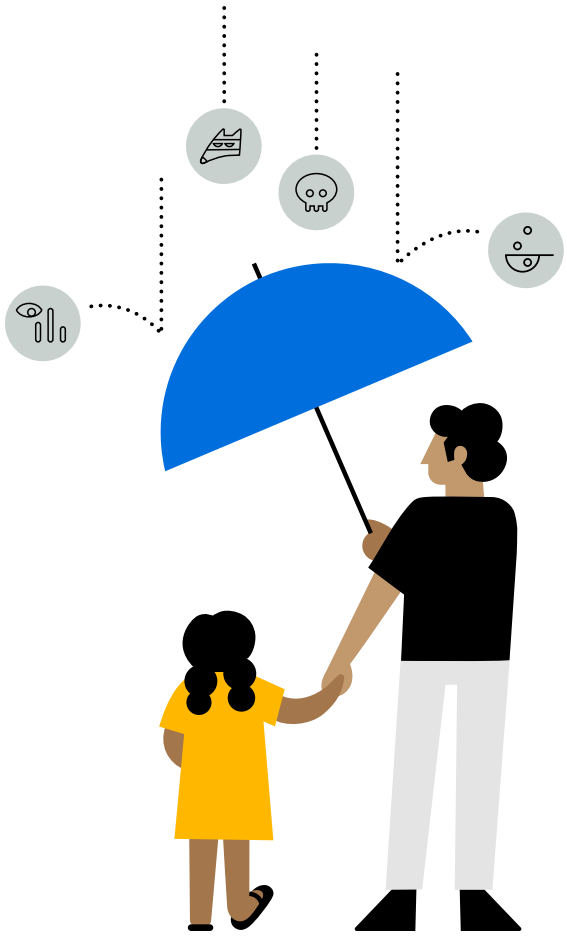
Alles bij elkaar komt het erop neer dat beveiligingsexperts iPhone het veiligste, best beveiligde mobiele device vinden. Dankzij de vele beveiligingslagen die een ongekende bescherming bieden tegen kwaadwillende software, kunnen gebruikers met een gerust hart hun gang gaan.

App Review

Door het App Review-proces zorgen we ervoor dat alle apps van een geverifieerde bron komen en dat ze vrij zijn van bekende kwaadwillende componenten. Ook controleren we of apps de gebruiker niet onder valse voorwendselen proberen over te halen om ongewenste aankopen te doen of toegang tot persoonlijke gegevens vragen. We screenen ontwikkelaars en gebruikers, en degenen die zich schuldig maken aan wangedrag worden uit de App Store geweerd. Hoewel het App Review-proces niet de verspreiding van alle slechte apps kan voorkomen, blijven we steeds innoveren en de gebruikte technologieën, methodes en processen verder verbeteren.

De app-bescherming van Apple in actie in 2020

- **Wekelijks werden gemiddeld 100.000 nieuwe apps en updates beoordeeld** door een team van ruim 500 experts, die apps in verschillende talen onder de loep namen.
- **Bijna 1 miljoen problematische nieuwe apps en ongeveer net zoveel updates werden om de volgende redenen afgewezen of verwijderd:**
  - Meer dan 150.000 apps waren spam, namaakapps of misleidend
  - Meer dan 215.000 apps hielden zich niet aan de privacyregels
  - Meer dan 48.000 apps bevatten verborgen of niet-gedocumenteerde features
  - Ongeveer 95.000 apps maakten zich schuldig aan frauduleuze overtredingen, voornamelijk functionaliteit van het type ‘bait & switch’ om criminele of andere verboden acties uit te voeren
- **Apple voorkwam meer dan 1,5 miljard dollar aan potentieel frauduleuze transacties.**
- **Apple heeft 470.000 teams uit het Apple Developer Program gezet om fraudegerelateerde redenen.** Om soortgelijke redenen zijn ook bijna 205.000 aanmeldingen van ontwikkelaars afgewezen.
- **Apple heeft 244 miljoen accounts van gebruikers gedeactiveerd vanwege frauduleuze activiteiten en misbruik, onder meer neprecensies.** Om soortgelijke redenen zijn ook 424 miljoen pogingen tot het aanmaken van een nieuwe account gestopt.



Dankzij App Review kan John met een gerust hart apps downloaden

Dankzij de beveiligings- en privacyfeatures in de App Store kan John met een gerust hart apps downloaden voor zichzelf en voor zijn dochter. Hij weet immers dat Apple alle apps in de App Store op bekende malware screent en dat iPhone-bezitters, in tegenstelling tot bezitters van andere devices, zelden last hebben van kwaadwillende software.

Meer informatie over de beschermings-voorzieningen van Apple

Meer informatie over de beveiligings- en privacyfeatures in de App Store is te vinden op **apple.com/benl/app-store.**

Meer informatie over de bescherming van locatiegegevens is te vinden in de **whitepaper over Locatievoorzieningen (Engelstalig).**

Meer informatie over ouderlijk toezicht in iOS is te vinden op **apple.com/benl/families.**

Veelgestelde vragen

Wat is sideloaden?

Sideloaden is het downloaden en installeren van apps op een mobiel device via een andere bron dan de officiële App Store, zoals een website of een onofficiële app-store. Om gebruikers en hun privacy te beschermen is iPhone zo ontworpen dat sideloaden voor gewone gebruikers niet is toegestaan.

Wat is een bedreigingsmodel?

Een bedreigingsmodel (of een threat model) is het geheel van aanvallen en kwetsbaarheden waartegen gebruikers moeten worden beschermd. Per device, groep gebruikers en omgeving wordt een ander bedreigingsmodel toegepast en de beveiliging is daarop afgestemd. De App Store vormt een cruciale schakel in de bescherming tegen het bedreigingsmodel voor iPhone. Op deze betrouwbare plek kunnen gebruikers veilig apps downloaden die door Apple zijn gecontroleerd en die afkomstig zijn van bekende ontwikkelaars die zich aan de regels van Apple moeten houden.

Stel dat het sideloaden van apps op iPhone via websites en onofficiële app-stores wordt toegestaan. Is dat een gevaar voor gebruikers die hun apps alleen via de App Store downloaden?

Ja. Sideloaden brengt extra distributiekanalen, een ander bedreigingsmodel en veel meer potentiële aanvallen met zich mee. Dat is een gevaar voor alle gebruikers, ook voor degenen die bewust voor extra bescherming kiezen en hun apps alleen via de App Store downloaden. iPhone zou ten prooi vallen aan een nieuwe golf aanvallen en kwaadwillende spelers zouden hun kans schoon zien en op grote schaal investeren in nieuwe tools en kennis om de beveiliging van iPhone te doorbreken. Als kwaadwillende spelers nog gewiekstere aanvallen kunnen uitvoeren, kunnen ze zowel onofficiële kanalen als de App Store zelf bestoken, met alle gevolgen van dien voor alle gebruikers. Bovendien kunnen gebruikers die hun apps het liefst in de App Store downloaden zich dan genoodzaakt zien om een app voor hun werk of voor school ergens anders te downloaden als deze niet in de App Store staat. Of ze kunnen slachtoffer worden van andere app-stores die zich als de App Store voordoen.

Wat houdt het App Review-proces van Apple in?

We zetten geavanceerde technologie in combinatie met menselijke expertise in om van elke app en elke update zorgvuldig te controleren of ze zich aan de strenge privacy-, beveiligings- en veiligheidsregels van de App Store houden. Die menselijke expertise komt om de hoek kijken wanneer de geautomatiseerde controle ontoereikend is om specifieke problemen te signaleren, zoals privacyschendingen of apps voor kinderen die zich niet aan onze strenge regels houden. We hebben die regels in de loop der tijd aangepast in verband met nieuwe bedreigingen en uitdagingen. Zo willen we onze gebruikers optimaal beschermen en hun het allerbeste van de App Store bieden. Wekelijks worden gemiddeld 100.000 nieuwe apps en updates beoordeeld door een team van ruim 500 experts over de hele wereld.

Wat wordt er precies gecontroleerd bij de App Review?

Alle apps en updates die bij de App Store worden ingediend, worden aan ons App Review-proces onderworpen.

Welke voorzieningen voor ouderlijk toezicht zijn er beschikbaar op Apple devices?

We bieden speciale features voor ouders die grip willen houden op de manier waarop hun kinderen hun device gebruiken. ‘Schermtijd’ geeft ouders een beter beeld van de tijd die hun kinderen besteden aan apps, het bezoeken van websites en het gebruik van hun device in het algemeen. Met ‘Schermtijd’ kunnen ouders ook limieten instellen voor de tijd die hun kinderen dagelijks aan bepaalde apps en websites mogen besteden. Verder kunnen ouders met ‘Vraag om te kopen’ vanaf hun eigen device de aankopen en downloads van hun kinderen goedkeuren of afwijzen. ‘Vraag om te kopen’ heeft een time-out van 15 minuten om te voorkomen dat kinderen alsnog zonder toestemming iets kopen.

Wat houden transparantie bij tracking door apps en de privacylabels in de App Store in?

Dit zijn nieuwe features waarmee gebruikers meer grip hebben op hun gegevens en privacy. Transparantie bij tracking door apps houdt in dat apps de gebruiker om toestemming moeten vragen voordat zij hun gegevens in apps of op websites van andere bedrijven mogen volgen. De privacylabels in de App Store houden in dat elke app in de App Store gebruikers een overzichtelijke samenvatting van het privacybeleid van de ontwikkelaar geeft. Zo weten gebruikers precies hoe een app met hun gegevens omspringt.

Bronnen

1. Jobs, Steve, 'Third Party Applications on the iPhone', 17 oktober 2007, bekeken op tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, 'Vulnerabilities - Separating Reality from Hype', *Agentschap van de Europese Unie voor cyberbeveiliging*, 24 augustus 2016.

3. Griffin, Robert Jr., 'Study on Mobile Device Security', *Amerikaans ministerie van Binnenlandse Veiligheid*, april 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 maart 2019.

6. Symantec, 'Internet Security Threat Report, Volume 23', april 2018.

7. Golovin, Igor, 'Malware in Minecraft mods: story continues', *Kaspersky*, 9 juni 2021.

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

11. Seals, Tara, 'Emerging Ransomware Targets Photos, Videos on Android Devices', *ThreatPost*, 24 juni 2020.

12. Owaida, Amer, 'Beware Android trojan posing as Clubhouse app', *WeLiveSecurity* van ESET, 18 maart 2021.

13. Desai, Shivang, 'SpyNote RAT posing as Netflix app', *Zscaler*, 23 januari 2017.

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

15. Palmer, Danny, 'This Android trojan malware is using fake apps to infect smartphones, steal bank details', *ZDNet*, 1 juni 2021.

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

17. Stefanko, Lukas, 'Android Trojan steals money from PayPal accounts even with 2FA on', *WeLiveSecurity* van ESET, 11 december 2018.

18. Cybereason Nocturnus Team, 'FakeSpy Masquerades as Postal Service Apps Around the World', *Cybereason*, 1 juli 2020.

19. Stefanko, Lukas, 'New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor', *WeLiveSecurity* van ESET, 24 juni 2020.

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

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

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

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

24. Maxwell, Andy, 'Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit', *TorrentFreak*, 8 januari 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 december 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', *Deloitte*, 2019.

28. Gikas, Mike, 'How to Protect Your Privacy on Your Smartphone', *Consumer Reports*, 1 februari 2017.