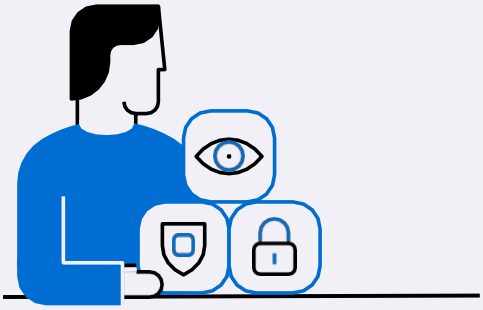


Voldoen aan de Wet digitale markten

De inspanningen van Apple om de veiligheid en privacy van gebruikers te beschermen in de Europese Unie

Maart2024

Inhoud

Apple wil gebruikers beschermen

Bij Apple is het onze hoogste prioriteit om geweldige producten te maken die het leven van onze gebruikers over de hele wereld verrijken. We maken producten die we zelf willen gebruiken en waarvan we willen dat onze familie en vrienden ze net zo mooi vinden als wij. We zijn er voortdurend op gericht om onze gebruikers een hoogwaardige en veilige ervaring te bieden door de naadloze integratie van hardware, software en services. En we weten dat een belangrijke reden waarom klanten voor Apple en iPhone kiezen, is dat ze geloven dat we die visie waarmaken.[1]

Toen Apple in 2007 de iPhone introduceerde, werd het tijdperk van mobiel computergebruik ingeluid. En het inspireerde tot nieuwe producten, waaronder bijna twee miljoen apps van externe ontwikkelaars die onmisbaar zijn geworden in het dagelijks leven van mensen, waardoor een geheel nieuwe app-economie is ontstaan die verantwoordelijk is voor miljoenen banen en wereldwijd triljoenen euro's aan handel mogelijk maakt.[2]

Helaas leven we ook in een wereld waarin aanvallen op de beveiliging en privacy steeds geavanceerdere bedreigingen vormen voor iedereen. Kwaadwillenden maken kwaadwillende apps die je gegevens kunnen veranderen, gijzelen voor losgeld of lekken naar het hele web. Ze kunnen bedrieglijke of frauduleuze activiteiten ontplooien, proberen je te bespioneren zonder dat je het weet of de functionaliteit van je apparaat zelf in gevaar brengen. Ze kunnen schijnwebsites bouwen die ontworpen zijn om je gevoelige gegevens te ontfutselen, je te overtuigen om gevaarlijke software te downloaden of zelfs je webbrowser aan te vallen. Ze kunnen phishingmails versturen om je over te halen je wachtwoorden te geven. Cybercriminelen kunnen ook proberen om uw gegevens te stelen door toegang te krijgen tot uw apparaat zonder uw medeweten of toestemming, door gebruik te maken van Bluetooth-accessoires en open netwerkverbindingen of door gewoon fysiek

toegang te krijgen tot uw apparaat.
je apparaat. Andere kwaadwillenden kunnen zelfs proberen om je informatie en berichten te hacken terwijl ze digitaal van en naar je apparaat worden verzonden. Deze kwaadwillenden vormen een bedreiging voor iedereen, waar ze ook wonen, en dat zal zo blijven.

We hebben iPhone gemaakt om gebruikers tegen dit soort risico's te beschermen, door hardware, software en diensten te combineren die zijn ontworpen om samen te werken voor maximale beveiliging en een transparante gebruikerservaring in dienst van het uiteindelijke doel: persoonlijke informatie veilig houden. Dit is een belangrijke reden waarom apps van derden zo succesvol zijn op iPhone: omdat gebruikers ondanks al deze bekende en altijd aanwezige risico's vertrouwen hebben in de toewijding van Apple om hen te beschermen. **Dit zijn enkele van de belangrijkste standaarden van Apple:**

BEVEILIGING

Gebruikers vertrouwen hun iPhones hun meest gevoelige gegevens toe. We hebben toonaangevende beveiligingsmaatregelen genomen om te voorkomen dat iemand anders dan de gebruiker toegang heeft tot de gegevens op hun iPhone.
gegevens op hun iPhone. En wij vinden het belangrijk dat gebruikers een vertrouwde plek hebben waar ze veilig software kunnen downloaden en ontdekken, zonder malware, cybercriminelen en oplichters.

PRIVACY

Bij Apple vinden we dat privacy een fundamenteel mensenrecht is en we ontwerpen onze producten en diensten met innovatieve technologieën en technieken om de privacy van onze gebruikers te beschermen. Gebruikers mogen niet worden blootgesteld aan software of websites die hun gegevens verzamelen, gebruiken of delen zonder hun uitdrukkelijke toestemming. We ontwikkelen onze producten en diensten om gebruikers controle te geven over hun gegevens en hen te beschermen tegen het verzamelen, gebruiken of delen van hun informatie zonder hun toestemming, en om ervoor te zorgen dat gebruikers weten welke gegevens van hen worden gedeeld en hoe deze worden gebruikt, en dat ze hier controle over kunnen uitoefenen.

VEILIGHEID

Gebruikers mogen niet worden blootgesteld aan fysieke schade via iOS, ook niet via apps die schade bepleiten of veroorzaken.

Deze waarden zijn fundamenteel voor wie we zijn, voor wat iPhone-gebruikers van ons verwachten en voor de integriteit van ons platform.

We zijn dankbaar dat gebruikers in meer dan 175 landen en regio's over de hele wereld de iPhone hebben omarmd, en Apple doet er alles aan om deze kernwaarden overal te handhaven. Dat betekent dat we een manier moeten vinden

om de veiligheid, privacy en bescherming van gebruikers te waarborgen en tegelijkertijd de wet na te leven in elk land waar we zakendoen.

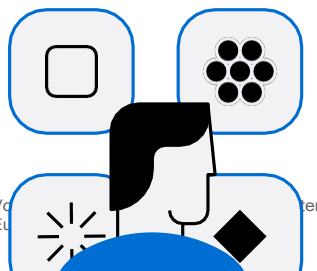
Vanaf dit jaar vereist de nieuwe Digital Markets Act (DMA) van de Europese Unie van ons een nieuwe aanpak in ons werk om onze EU-gebruikers van dienst te zijn.

Om aan de DMA te voldoen, hebben we nieuwe opties voor ontwikkelaars en gebruikers gecreëerd en **meer dan 600 nieuwe API's en tools voor ontwikkelaars** gebouwd **om deze veranderingen mogelijk te maken**. De nieuwe opties omvatten het mogelijk maken van **sideloading**, zodat EU-gebruikers apps kunnen downloaden via andere app marketplaces dan de App Store, het mogelijk maken van **alternatieve manieren om betalingen te verwerken** in de App Store, en **vele andere veranderingen**.[3] Hiervoor moesten we de unieke succesvolle aanpak die we hebben gebruikt om de veiligheid en privacy van gebruikers te beschermen, veranderen.

Sinds we de iPhone in 2007 op de markt brachten, hebben we onze gebruikers overal ter wereld op dezelfde manier beschermd, met veel uitgebreide en toonaangevende beveiligingen tegen talloze bedreigingsvectoren. In de App Store wilden we vanaf het begin in 2008 een veilige en vertrouwde plek creëren waar gebruikers apps kunnen vinden en ontwikkelaars een veilige en ondersteunende manier bieden om apps te ontwikkelen, te testen en wereldwijd onder gebruikers te verspreiden. In de loop der jaren hebben we ontwikkelaars meer mogelijkheden geboden met meer dan 40 SDK's (Software Development Kits), 250.000 API's (Application Programming Interfaces) en vele andere geavanceerde tools.

Door te eisen dat alle apps op iPhone worden gedistribueerd via één vertrouwde bron, de App Store, konden we ons doel om gebruikers te beschermen effectiever bereiken dan welk ander platform dan ook. Hoewel onze inspanningen om gebruikers te beschermen en ontwikkelaars nooit volledig zijn, heeft iOS nog nooit een wijdverspreide malware-aanval op gebruikers toegelaten, wat uitzonderlijk is voor een 17 jaar oud, modern computerplatform.

De nieuwe opties die we introduceren om te voldoen aan de DMA betekenen noodzakelijkerwijs dat we gebruikers niet op dezelfde manier kunnen beschermen. Om gebruikers het veiligste, meest privacybeschermende en veiligste platform te blijven bieden - in lijn met wat gebruikers van Apple verwachten, hebben we nieuwe beveiligingen ontworpen en geïmplementeerd om hen te beschermen en te informeren. Hoewel de door de DMA vereiste wijzigingen onvermijdelijk zullen leiden tot een kloof tussen de bescherming waarop Apple gebruikers buiten de EU kunnen vertrouwen en de bescherming die gebruikers in de EU voortaan genieten, werken we er onvermoeibaar aan om ervoor te zorgen dat iPhone de veiligste telefoon blijft die in de EU verkrijgbaar is, door de risico's die deze noodzakelijke wijzigingen met zich meebrengen te beperken - ook al kunnen we die risico's niet helemaal uitsluiten.



Dit document geeft een overzicht van de belangrijkste stappen die we nemen op drie belangrijke fronten - gebruikersbeveiliging, privacy en veiligheid - om de veranderingen aan te pakken die de DMA vereist voor app-distributie en -betalingen, en wat we verwachten dat deze veranderingen zullen opleveren voor ontwikkelaars en gebruikers in de EU.

Apple's waarborgen voor de distributie van apps en alternatieve betalingen zijn erop gericht om de veiligheid en privacy van gebruikers te beschermen en om gebruikers veilig te houden.

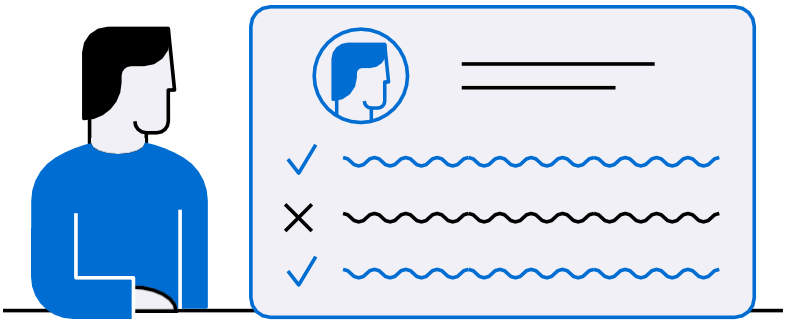
We introduceren en breiden een aantal functies uit die de veiligheid, privacy en beveiliging van gebruikers ondersteunen en tegelijkertijd sideloading en alternatieve manieren voor het verwerken van betalingen in de App Store in de EU mogelijk maken. Apple heeft waarborgen ontwikkeld en geïmplementeerd om ervoor te zorgen dat we de beste blijven leveren,
een zo veilig mogelijke ervaring voor gebruikers in de EU, ook al zal deze niet zo veilig, privacybeschermend of beveiligd zijn als in de rest van de wereld.

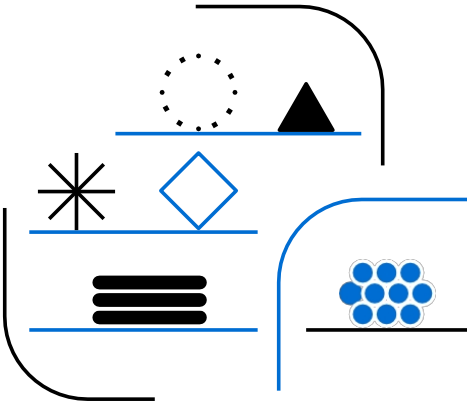
Kwaadaardige apps identificeren en stoppen

Om onze EU-gebruikers te beschermen in het nieuwe landschap dat door de DMA is gecreëerd**, lanceert Apple Notarization for iOS: een basisbeoordeling van alle apps (ongeacht of ze via de App Store of een alternatieve app-marktplaats worden gedistribueerd) die het nieuwe app-distributielandschap weerspiegelt en gericht is op platformintegriteit en bescherming van gebruikers.**

Apple zal elke app die in de EU op iOS wordt gedistribueerd elektronisch ondertekenen, ongeacht hoe deze wordt gedistribueerd, en deze ondertekening is vereist voor elke app op iOS. Alvorens een app te ondertekenen, zal Apple deze analyseren (met behulp van een combinatie van ***geautomatiseerde tools*** en ***menselijke beoordeling***) om te controleren of de app vrij is van bekende malware en andere beveiligingsrisico's, over het algemeen werkt zoals geadverteerd en gebruikers niet blootstelt aan flagrante fraude. Door deze controles aan de voorkant uit te voeren, kunnen we cyberaanvallen en andere bedreigingen helpen voorkomen *voordat* ze zich verspreiden onder andere gebruikers.
Dit proces is een uitbreiding van Notarization for macOS; Apple scant en ondertekent al jaren software die op macOS wordt gedistribueerd om ervoor te zorgen dat deze vrij is van bekende malware. Dit heeft goed gewerkt, dus hebben we het aangepast voor iOS,
inclusief nieuwe verbeteringen om te voldoen aan de unieke behoeften van het meest vertrouwde mobiele computerplatform ter wereld.

Om zeker te zijn, zal Notarization niet alles afdekken, zoals hieronder verder wordt besproken, zoals app inhoud, zakelijke praktijken en andere App Store bescherming voor gebruikers.





De bescherming die we hebben ingesteld, begint al bij de allereerste stap die een app-ontwikkelaar moet nemen om een app op iOS in de EU te kunnen distribueren.

App Ontwikkeling

Ongeacht hoe een ontwikkelaar een app op de iPhone distribueert, hij moet zich aanmelden voor het Developer Program van Apple voordat hij een app voor iOS kan bouwen (in de EU of ergens anders). Als onderdeel van het aanmeldingsproces vraagt Apple ontwikkelaars om hun identiteit te verifiëren door een wettelijke naam, telefoonnummer en adres te vragen (of, voor een organisatie, andere specifieke identificatiegegevens). In sommige gevallen kan een ontwikkelaar worden gevraagd om hun regeringsidentificatienummer of om op een andere manier hun identiteit te bewijzen. Deze initiële beveiliging is een belangrijke antifraudemaatregel, die het mogelijk maakt om ontwikkelaars kunnen worden geïdentificeerd en verantwoordelijk worden gehouden voor wat ze distribueren - Apple heeft in 2022 voorkomen dat bijna 105.000 frauduleuze ontwikkelaarsaccounts werden aangemaakt vanwege vermeende frauduleuze activiteiten.[4]

Wanneer ontwikkelaars zich aanmelden voor het programma, gaan **ze akkoord met onze licentieovereenkomst voor het ontwikkelaarsprogramma**. Hierdoor kan Apple basisregels opstellen waaraan ontwikkelaars zich moeten houden om hun apps op de apparaten van Apple te mogen distribueren. Ontwikkelaars stemmen ermee in zich niet in te laten met fraude, zich te houden aan toepasselijke wet- en regelgeving en hun apps niet te ontwerpen of op de markt te brengen met als doel ze lastig te vallen, te misbruiken, te spammen, te stalken, te bedreigen of anderszins te schenden. de wettelijke rechten van anderen. Als een ontwikkelaar de overeenkomst schendt, kunnen we de overeenkomst beëindigen, en dat doen we ook. In 2022 heeft Apple meer dan 400.000 accounts van ontwikkelaars beëindigd wegens fraude.[5]

Inzending

Daarnaast biedt Apple **ontwikkelaars hulpmiddelen** die bescherming bieden tegen bepaalde risico's die zich tijdens de ontwikkelingsfase, voorafgaand aan de indiening, zouden kunnen voordoen. Voor

We hebben bijvoorbeeld SDK-pakketondertekening geïmplementeerd om ontwikkelaars te helpen de bron van code van derden te verifiëren. Dit helpt ontwikkelaars te beschermen tegen het onbedoeld gebruiken van code die kwaadwillig is aangepast tijdens het bouwen van hun apps.

Notarisatie begint wanneer een ontwikkelaar zijn app binair indient bij Apple. Daarbij geeft de ontwikkelaar aan op welke app-marktplaatsen hij de app wil distribueren, waaronder - indien gewenst - de App Store.

Beoordeling

Tijdens de **Notarization** voert Apple zowel ***geautomatiseerde*** als ***menselijke controles*** uit om te voorkomen dat apps die de integriteit van het platform bedreigen, zoals bedreigingen voor de veiligheid, privacy en beveiliging van gebruikers, de gebruiker bereiken.

De **geautomatiseerde beoordeling maakt** gebruik van machinaal leren, heuristiek en jaren van verzamelde gegevens om problematische apps te identificeren, waarbij de binary van de app wordt gescand op gevallen van bekende malware of andere beveiligingsrisico's.

De **menselijke beoordeling** dient als een kritieke verdedigingslinie om gebruikers te beschermen tegen slechte actoren. Onze menselijke beoordelaars analyseren elke app en specialisten wijzen apps af die de Notarisatierichtlijnen schenden. Het team lanceert en draait elke app ook op een geïsoleerd platform om te testen of de app werkt zoals beschreven en veilig lijkt voor gebruikers. Omdat geautomatiseerde beoordeling gebaseerd is op bedreigingen uit het verleden, is aanvulling met menselijke beoordeling essentieel om opkomende en nieuwe bedreigingen te detecteren. Omdat cybercriminelen steeds creatiever en geavanceerder worden, zorgt het menselijke element in ons proces ervoor dat Apple op de hoogte blijft van nieuwe bedreigingen. En menselijke controle is ook essentieel voor onze inspanningen om te voorkomen dat apps die geen op software gebaseerde bedreigingen vormen, zoals flagrante fraude, op de iPhone terechtkomen. Menselijke beoordeling is vooral belangrijk bij het identificeren van slechte actoren die proberen social engineering-technieken te gebruiken om gebruikers te manipuleren zodat ze toegang krijgen tot hun apparaat en informatie door zich voor te doen als iemand die ze niet zijn. Mensen kunnen controleren of een schadelijke app een gebruiker probeert te misleiden, bijvoorbeeld door zich voor te doen als een andere app of door een gebruiker te misleiden zodat hij toegang krijgt tot zijn gevoelige gegevens, en controleer op andere kwaadaardige technieken die een machine niet kan vinden.

We zullen dezelfde controles toepassen op **alle app-updates**, met als doel te voorkomen dat kwaadwillenden malware of andere gevaarlijke functies in elke app binnensmokkelen na de eerste download.

Om duidelijk te zijn: de geautomatiseerde en door mensen geleide beoordelingsprocessen die samen Notarization vormen zijn geen App Review. Ze analyseren of inzendingen voldoen aan slechts een deelverzameling van de App Store beoordelingsrichtlijnen - en ze omvatten ***niet*** veel van de belangrijkste App

Store beoordelingsrichtlijnen. Notarisatie ***zal*** controles omvatten die nodig zijn om onze gebruikers te beschermen en die essentieel zijn voor de ***integriteit van het platform***, inclusief controles die specifiek gericht zijn op de bescherming van de veiligheid, privacy en beveiliging van gebruikers.

- **Beveiliging:** Notarisatie controleert apps op beveiligingsrisico's voor het apparaat. Notarisatie zorgt er bijvoorbeeld voor dat apps geen bekende malware bevatten. We zullen ook geen apps toestaan die proberen te lezen of te schrijven buiten hun aangewezen

Beoordeling

gegevensmakelaars.

Met locatieservices kunnen apps en websites informatie van mobiele, Wi-Fi-, GPS- en Bluetooth-netwerken gebruiken om de locatie van een gebruiker met een hoge mate van nauwkeurigheid en precisie te bepalen.

Onder ons kader **voor app-traceringstransparantie** moeten gebruikers toestemming geven voordat een ontwikkelaar toegang kan krijgen tot hun unieke apparaatidentificator die wordt gebruikt door adverteerders (IDFA) om hen te volgen op websites of andere apps met als doel te adverteren of te delen met

containe
rgebied,
waardoo
r deze
apps
andere
apps
zouden
kunnen
manipul
eren of
toegang
zouden
kunnen
krijgen
tot
ongeaut
oriseerd
e
gegeven
s van
het
apparaat
van de
gebruike
r.

Gebruik
ers
verleide
n tot het
downloa
den van
een app
onder
valse
voorwen
dselen -
hetzij
omdat
de
gebruike
r denkt
dat het
een
andere
bestaan
de app
is, hetzij

omdat de app die wordt gedownload anders is dan wat de app ***wordt - is*** een belangrijke methode die kwaadwillenden gebruiken om malware of andere virussen op een apparaat over te brengen zonder dat de gebruiker dit merkt. kennis van de gebruiker, of om de veiligheid van het apparaat op andere manieren te bedreigen. Om dit te voorkomen, zullen we in Notarization ook kijken of apps valse informatie bevatten over hun functies of mogelijkheden, zich voordoen als andere apps of verborgen, slapende of ongedocumenteerde functies hebben. We zullen ook onderzoeken of apps bronnen kunnen downloaden die functionaliteiten introduceren of wijzigen na het downloaden.

- **Privacy:** Notarization probeert bedreigingen voor de privacy van gebruikers te voorkomen door ervoor te zorgen dat elke app de privacyfuncties die zijn ingebouwd in en essentieel zijn voor de integriteit van alle Apple apparaten, naar behoren ondersteunt en niet probeert te omzeilen. Om de privacy van gebruikers te beschermen en gebruikers inzicht te geven in de manier waarop hun gegevens worden gebruikt, gebruikt Apple technische maatregelen om te voorkomen dat apps toegang krijgen tot gevoelige informatie van gebruikers. iOS geeft apps alleen toegang tot dit soort gegevens nadat ze daarvoor toestemming hebben gekregen van de gebruiker, die deze toestemming op elk moment kan intrekken. Dit geldt voor gegevens en diensten zoals:

  - de microfoon
  - de camera
  - Gezicht ID
  - opgeslagen wachtwoorden
  - locatiegegevens zoals geleverd door Locatiediensten
  - gezondheidsgegevens
  - de unieke apparaat-id die wordt gebruikt door adverteerders (IDFA)
  - Bluetooth
  - Portemonnee
  - Contacten
  - Foto's
  - Gegevens home app
  - Kalender
  - Game Center-vriendenlijst
  - Herinneringen
  - Apple Muziek-bibliotheek

  Notariële vastlegging controleert of apps die deze toestemmingen aanvragen duidelijk en beknopt aangeven waarom de toegang nodig is, zodat de gebruiker een weloverwogen keuze kan maken over welke toestemmingen hij/zij wil geven en baas blijft over zijn/haar eigen gegevens.

Notarisatie zal ook evalueren of apps op een manier met gebruikersgegevens omgaan die gebruikers verwachten. Notarisatie zal er bijvoorbeeld voor proberen te zorgen dat apps toestemming van gebruikers krijgen voor het verzamelen en delen van gegevens en niet proberen gebruikers te manipuleren, misleiden of dwingen om toestemming te geven voor de toegang van een app tot hun gegevens; er zal ook worden onderzocht of apps een privacybeleid bieden zodat gebruikers kunnen begrijpen hoe hun gegevens worden verzameld, gebruikt en verkocht. Vanwege de gevoeligheid
van persoonlijke gezondheidsgegevens, eisen we ook dat apps geen gegevens gebruiken of openbaar maken die zijn verzameld in de context van gezondheid, fitness en medisch onderzoek voor reclame, marketing of andere op gebruik gebaseerde datamining.

- **Veiligheid:** Om voor Notarization te slagen, mogen apps geen risico vormen voor lichamelijk letsel van gebruikers of schade aan hun apparaten. We verbieden bijvoorbeeld apps die klanten aansporen om deel te nemen aan activiteiten of hun apparaten te gebruiken op een manier die het risico inhoudt dat anderen lichamelijk letsel oplopen. Bij Notarization wordt ook gekeken naar apps die de functionaliteit van het apparaat in gevaar brengen, bijvoorbeeld door de batterij van een iPhone snel leeg te laten lopen, overmatige hitte te genereren of het apparaat onnodig te belasten.
  apparaatbronnen - dit alles kan ervoor zorgen dat een iPhone niet meer functioneert in een noodsituatie.

De richtlijnen voor het beoordelen van notariële apps zullen niet de beleidsregels voor inhoud en handel bevatten die in de richtlijnen voor het beoordelen van apps in de App Store staan, en zullen dus geen apps verbieden of controleren die tegen die beleidsregels ingaan. Dit betekent dat Apple niet kan voorkomen dat apps met inhoud die Apple niet zou toestaan in de App Store, zoals apps die pornografie verspreiden, apps die aanzetten tot het gebruik van tabak of vape-producten, illegale drugs of buitensporige hoeveelheden alcohol, of apps die illegaal gekopieerde inhoud bevatten (of die op een andere manier ideeën of intellectueel eigendom van andere ontwikkelaars stelen), beschikbaar komen op alternatieve app-marktplaatsen. Alleen apps die ervoor kiezen om gedistribueerd te worden via de App Store zullen het standaard App Review proces doorlopen, bovenop de Notarization, die handhaving van dit App Store-only beleid omvat.

Installatie

Zodra een app deze beoordelingen heeft doorstaan, notariëren we de app, waardoor de ontwikkelaar de **handtekening krijgt** die nodig is om de app op iOS te distribueren. Om er zeker van te zijn dat er niets verandert tussen het moment dat Apple de app ondertekent en het moment dat een gebruiker de app daadwerkelijk op zijn iPhone installeert, ondergaan notariële apps ook een reeks van basiscontroles tijdens de installatie. Dit zal ervoor zorgen dat er niet met de app is geknoeid sinds deze notarieel is vastgelegd en dat de installatie is gestart door een geautoriseerde bron.

Hoewel we weten dat Notarisatie een belangrijk hulpmiddel zal zijn in ons werk om gebruikers te beschermen tegen bedreigingen van hun veiligheid, privacy en beveiliging - het dient als een eerste verdedigingslinie tegen potentiële bedreigingen en kwaadaardige functies - weten we ook dat het beperkingen heeft. Om onze gebruikers te blijven beschermen, zelfs nadat apps zijn geïnstalleerd, hebben we ook **basiscriteria** opgesteld **voor alternatieve apps.**
marktplaatsen om ervoor te zorgen dat ze ten minste over de minimale capaciteiten beschikken die nodig zijn om de belangrijke verantwoordelijkheid voor de *permanente* bescherming van gebruikers uit te voeren. Deze omvatten:

- ***Inzetten op voortdurende bewaking om schadelijke apps te detecteren en te verwijderen.*** Deze bewaking is nodig om apps op te sporen die niet worden geblokkeerd tijdens de notariële controle of die na de notariële controle veranderen. Onze ervaring heeft ons geleerd dat voortdurende bewaking voor nieuwe bedreigingen die kunnen opduiken na de eerste controle, het volgende is
  noodzakelijk om de veiligheid, beveiliging en privacy van gebruikers te beschermen. We hebben ook ontdekt dat monitoring signalen vereist die specifiek zijn voor de marktplaats, zoals gebruikersbeoordelingen, feedback van klanten en analyse van marktplaatsgegevens; Apple heeft geen toegang tot deze signalen buiten de App Store. Als niet elke alternatieve app marktplaats voortdurend toezicht houdt, zullen de veiligheid, privacy en beveiliging van gebruikers ernstig in gevaar komen.

- ***Garanderen dat alternatieve app-marktplaatsen gebruikers kunnen beschermen.*** Een app-marktplaats exploiteren die de distributie van apps van derden faciliteert zonder de beveiliging, veiligheid en privacy aanzienlijk in gevaar te brengen.
  is niet eenvoudig.[6] App-marktplaatsen hebben middelen nodig om deze belangrijke verantwoordelijkheden uit te voeren, zoals het voortdurend controleren op schadelijke apps. Marktplaatsen moeten ook in staat zijn om gebruikers en ontwikkelaars doorlopend ondersteuning te bieden, zodat ontwikkelaars hun bedrijf kunnen runnen en gebruikers kunnen vertrouwen op hun apps.
  op apps die zijn gedownload via alternatieve app-marktplaatsen dat ze werken zoals ze verwachten, en hulp krijgen als dat niet het geval is. Een marktplaats die niet de
  middelen die nodig zijn om gebruikers te beschermen of die gebruikers en ontwikkelaars geen verhaal bieden wanneer dat nodig is, zou de iPhone in gevaar brengen.

Deze vereisten zijn het minimum van wat nodig is voor een app marktplaats om de gegevens van gebruikers veilig en privé te houden en gebruikers te beschermen. Ze omvatten niet alle inspanningen die Apple heeft geïnvesteerd in de hoge

standaarden voor beveiliging, privacy en veiligheid van de App Store.

We hebben ook app-installatiebladen gemaakt die gebruikers in staat stellen een weloverwogen keuze te maken over de apps die ze downloaden.
Gebruikers kiezen deels voor Apple producten vanwege de transparantie en controle die we ze bieden, waardoor ze weloverwogen beslissingen kunnen nemen over wat ze op hun apparaten willen hebben. Deze nieuwe app-installatiebladen zijn een belangrijke manier waarop we ons blijven inzetten voor de transparantie die gebruikers van ons verwachten.

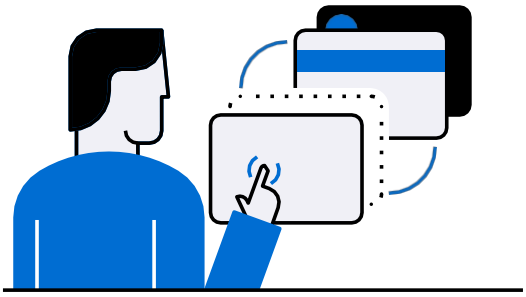
De bladen geven informatie weer die tijdens de notarisatie is bekeken, zoals de naam van de app, de naam van de ontwikkelaar, de beschrijving van de app, schermafbeeldingen en de leeftijdsclassificatie van het systeem, en identificeren de marktplaats waar een gebruiker de app van downloadt, gestandaardiseerd formulier. Ontwikkelaars kunnen de inhoud van dit formulier niet meer wijzigen nadat hun apps notarieel zijn goedgekeurd zonder het proces opnieuw te doorlopen.

Om alle veranderingen die de DMA vereist mogelijk te maken, heeft Apple meer dan 600 nieuwe API's en tools voor ontwikkelaars gemaakt. We hebben gegevensbeveiliging, privacy en gebruikersveiligheid in deze API's ingebouwd.
MarketplaceKit bijvoorbeeld, het raamwerk waarmee alternatieve app-marktplaatsen kunnen werken.
op iOS vergemakkelijkt de *veilige* installatie van apps die vanaf alternatieve marktplaatsen worden gedistribueerd: wanneer gebruikers een app downloaden via een alternatieve app-marktplaats,

stelt onze API de webserver van de marktplaats in staat om rechtstreeks te communiceren met iOS, waarbij verificatieservices, app-licenties en app-gegevens worden geleverd om een veilige ervaring te creëren.
Deze API's zijn ook ontworpen om

ervoor zorgen dat app-installaties vanaf een marktplaats plaatsvinden als gevolg van de interactie van de gebruiker met de marktplaats, dat wil zeggen dat de gebruiker
en niet door een bug of automatische download. En deze API's maken ook eenvoudige updates van de app mogelijk, wat ontwikkelaars stimuleert om apps up-to-date te houden.

Apple heeft ook andere nieuwe API's gemaakt die gebruikers beschermen, zoals AdAttributionKit, dat privacybeschermende advertenties mogelijk maakt, adverteerders en ontwikkelaars in staat stellen om statistieken over advertentiegegevens te verkrijgen zonder individuele gebruikers te volgen of apparaten in apps die eigendom zijn van andere bedrijven. Deze nieuwe tools zorgen ervoor dat de veranderingen die we hebben doorgevoerd om te voldoen aan de DMA zo naadloos mogelijk werken, terwijl gebruikers tegelijkertijd zo veilig mogelijk blijven.



Door gebruikers in een oogopslag een samenvatting van deze informatie te geven, weten gebruikers welke app ze downloaden en hoe de app eruit zag toen deze door de Notarisatie kwam, zelfs als andere marktplaatsen geen gestandaardiseerde vereisten hebben voor app-openbaarmakingen of als de presentatie van de app is veranderd na de Notarisatie. De openbaarmakingen maken het gebruikers gemakkelijk om te kiezen met welke apps ze in zee willen gaan. Een gebruiker kan er ook voor kiezen om de schermen voor elke marktplaats uit te schakelen. De bladen zullen automatisch verdwijnen als een gebruiker de marktplaats als standaard instelt, omdat de gebruiker dan de keuze heeft gemaakt om die marktplaats te prefereren.

Gebruikers informeren over betalingsrisico's

Ter ondersteuning van de veranderingen die we hebben aangekondigd om te voldoen aan de DMA, introduceren we ook de mogelijkheid voor ontwikkelaars in de App Store om alternatieve betalingsopties te gebruiken voor het voltooien van transacties voor digitale goederen en diensten binnen hun apps in de EU. Dit opent nieuwe mogelijkheden voor ontwikkelaars, maar het betekent ook dat gebruikers van die apps niet dezelfde bescherming en voordelen zullen hebben waarop ze zijn gaan vertrouwen via het besloten en veilige handelssysteem van Apple, inclusief In-App Purchase (IAP) - zoals eenvoudige opzegging van een abonnement, een gecentraliseerde pagina met aankoopgeschiedenis, ouderlijk toezicht zoals Ask to Buy, of bescherming tegen uitbuitingstactieken zoals die welke erop gericht zijn gebruikers een ander bedrag voor een digitaal product te laten betalen dan geadverteerd. Het is aan gebruikers om zelf, per app, uit te zoeken welke voordelen en beschermingen voor hen beschikbaar zijn en met wie ze contact moeten opnemen voor hulp als transacties misgaan, aangezien AppleCare-agenten beperkte (of geen) mogelijkheden zullen hebben om hen te helpen.

Zoals altijd laat Apple zich leiden door de waarden van transparantie en het op de hoogte houden van gebruikers. Daarom **laten we gebruikers weten dat de bescherming van Apple niet beschikbaar zal zijn, zodat de gebruiker over de nodige kennis beschikt om te beslissen of hij al dan niet om de transactie te voltooien**. Voordat een gebruiker een app downloadt, toont de App Store een informatiebanner op de productpagina van de app om de gebruiker te informeren dat de ontwikkelaar een alternatieve betalingsoplossing

gebruikt en niet het beveiligde handelssysteem van Apple. En voordat een gebruiker een transactie verricht buiten het Apple handelssysteem om, krijgt hij een in-app informatieblad te zien dat hem laat weten dat hij niet langer een transactie verricht met Apple. Deze informatie zorgt ervoor dat gebruikers weten dat ze op hun hoede moeten zijn voor ontwikkelaars die misleidende betalingsinformatie, afbraakprijzen en ontbrekende abonnementsvermeldingen gebruiken.

Beveiliging, privacy en veiligheid door ontwerp

Belangrijk is dat de systeemarchitectuur en het ontwerp van Apple de veiligheid, privacy en beveiliging van gebruikers blijven beschermen. Apple heeft beveiliging in de kern van zijn platforms ingebouwd door middel van krachtige en gelaagde beveiliging. Dit ontwerp betekent dat zelfs als de iPhone in de EU niet zo veilig is als in de rest van de wereld, wij ervan overtuigd zijn dat het blijft de veiligste optie in de EU. Op basisniveau kunnen belangrijke beveiligingsfuncties, zoals hardwarematige apparaatversleuteling, niet worden uitgeschakeld. Apple b i e d t ook lagen van bescherming die een stabiel, veilig platform bieden voor apps. Alle apps zijn bijvoorbeeld voorzien van **een sandbox**, zodat ze geen toegang hebben tot bestanden die door andere apps zijn opgeslagen of wijzigingen in het apparaat kunnen aanbrengen. Systeembestanden en -bronnen zijn ook afgeschermd van de apps van de gebruiker. Als een app toegang nodig heeft tot andere informatie dan zijn eigen informatie, doet hij dat alleen via services die expliciet door iOS worden geleverd. Dit betekent dat een app over het algemeen geen invloed kan hebben op andere apps of het iOS systeem, waardoor het risico kleiner wordt.
van malware die andere delen van het platform aantast. Apple heeft ook **code signing** ingebouwd, wat betekent dat alle code in apps van derden wordt gekoppeld aan de ontwikkelaar wiens echte identiteit is geverifieerd toen hij zich inschreef voor het Developer Program. Bij de lancering zorgt iOS ervoor dat de code in de app overeenkomt met wat de ontwikkelaar heeft ondertekend toen hij de app indiende.

Apple heeft iOS ook ontworpen met het oog op **privacy**. iOS vereist bijvoorbeeld dat gebruikers kiezen of apps überhaupt toegang hebben tot hun locatiegegevens en zo ja, of de app toegang heeft tot de exacte locatie van de gebruiker of alleen tot een algemene locatie.
benadering van hun locatie. Apps hebben zonder toestemming van de gebruiker geen toegang tot de microfoon of camera van de iPhone, en als een app de microfoon of camera van een apparaat gebruikt, geeft het apparaat een indicator weer om de gebruiker dat te laten weten. Om soortgelijke redenen heeft Apple apps de toegang tot de camera ontzegd als ze op de achtergrond actief zijn, zodat ze gebruikers niet stiekem kunnen bespioneren.

Natuurlijk bouwt Apple ook vele andere beveiligingen in, waaronder hardwarebeveiliging en biometrie, zoals Apple silicon, Secure Enclave, Face ID en Touch ID; de geïntegreerde hardware- en softwarefuncties die zorgen voor het veilig opstarten, updaten en blijven werken van Apple besturingssystemen; en de netwerkprotocollen die zorgen voor veilige authenticatie en versleuteling van gegevens tijdens de overdracht. Apple apparaten bevatten ook gegevensbeschermings- en coderingsfuncties om zoekgeraakte of gestolen apparaten te beschermen en om onbevoegden te weren die een apparaat proberen te gebruiken

of aan te passen. Bovendien biedt Apple "kits" voor veilig en privébeheer van het huis en de gezondheid van gebruikers, die ook toegankelijk zijn voor apps van derden via API's, zodat de meest gevoelige en persoonlijke gegevens van een gebruiker veilig en privé blijven.

Dit zijn slechts een paar voorbeelden van de systeemarchitectuur en de ingebouwde privacybescherming van Apple die - samen met de nieuwe wijzigingen die we nu doorvoeren - onze EU-gebruikers in dit nieuwe landschap blijven beschermen.

Zorgen van overheden en gebruikers

We verwachten dat velen deze bescherming zullen verwelkomen, omdat we weten dat er reële zorgen bestaan over de wijzigingen die Apple in zijn platform aanbrengt. Sinds we op 25 januari 2024 DMA-gerelateerde wijzigingen in iOS, Safari en de App Store in de EU hebben aangekondigd, hebben we van regeringen, waaronder overheidsinstanties, de volgende zorgen gehoord van EU-lidstaten en gebruikers over de risico's van het toestaan van alternatieve app stores en alternatieve betalingsverwerkers op iOS, en vragen hoe en of we van plan zijn om beveiligingen in te bouwen tegen deze risico's.

Overheidsinstanties, zowel in de Europese Unie als daarbuiten, hebben de risico's die deze nieuwe distributiemogelijkheden met zich meebrengen en de behoefte aan beschermende maatregelen snel onderkend. Deze agentschappen, met name agentschappen die essentiële functies vervullen, zoals defensie, Het bankwezen en hulpdiensten hebben contact met ons opgenomen over deze nieuwe veranderingen en willen de garantie dat ze kunnen voorkomen d a t overheidsmedewerkers apps kunnen sideloaden op iPhones die ze van de overheid hebben gekocht.

Verschillende instanties hebben ons verteld dat ze van plan zijn om sideloading te blokkeren op elk apparaat dat ze beheren. Eén overheidsinstantie in de EU liet ons weten dat ze noch de financiële middelen, noch de het personeel om apps voor haar apparaten te beoordelen en goed te keuren, en was daarom van plan om te blijven vertrouwen op Apple en de App Store, omdat ze erop vertrouwt dat wij apps uitgebreid onderzoeken.

Deze instanties hebben allemaal erkend dat sideloading (het downloaden van apps van buiten de App Store) de beveiliging in gevaar kan brengen en overheidsgegevens en -apparaten in gevaar kan brengen.

En ***gebruikers hebben*** Tim Cook talloze e-mails gestuurd waarin ze hun vrees uiten dat deze veranderingen hun ervaring op de iPhone minder veilig zullen maken. Deze klanten hebben ons verteld dat wat ze zo leuk en waardevol vinden aan Apple en haar producten, ons streven is om hun privacy en veiligheid te beschermen, en dat ze vrezen de risico's die de nieuwe

veranderingen met zich meebrengen voor hun eigen apparaten en die van hun gezin.

We hoorden - en anticipeerden - deze zorgen. Daarom hebben we beveiligingen geïmplementeerd en zullen we onvermoeibaar blijven innoveren om onze gebruikers zo goed mogelijk te beschermen.

Beste Tim

Echte e-mails ontvangen door Tim Cook over wijzigingen aan iPhone in de Europese Unie

Aan: **Tim Cook**
Van: **EU Burger**
Onderwerp: **Bedankt**
Datum: **27 januari 2024**

Bedankt voor het leiden van een bedrijf dat klanten op de eerste plaats zet, of het nu gaat om hun privacy, gezondheid of mensenrechten.

Als EU-burger ... zal ik sideloading niet toestaan op mijn apparaten

Aan: **Tim Cook**
Van: **Apple klant**
Betreft: **Ernstig verontrust door recente EU-wetgeving**
Datum: **28 januari 2024**

Ik ben al meer dan tien jaar een tevreden klant en gebruiker van Apple. Ik geloof echt dat wat Apple heeft gecreëerd magisch is. Ik wil de dag niet meemaken dat ik gedwongen word om een winkel van een derde partij te downloaden als de ontwikkelaar van een app die ik wil gebruiken ervoor kiest om de App Store te omzeilen en me dwingt om me bij hen aan te melden, of een betalingsapp van een derde partij te gebruiken als mijn bank besluit om Apple Pay niet meer te ondersteunen. Op dit moment werkt het allemaal als bij toverslag en is het een genot om te gebruiken.

Ik hoop van harte dat jij en Apple blijven opkomen voor wat juist is en de beste klantervaring blijven leveren en dat we de iPhone nooit vol zien staan met App-winkels van derden, zoals Samsung- of Google-telefoons.

Aan: **Tim Cook**
Van: **EU iPhone-gebruiker**
Betreft: **Betreft Europese wet digitale markten**
Datum: **27 januari 2024**

Onlangs is er veel discussie geweest over het openstellen van iPhones voor alternatieve app stores, naar aanleiding van de Europese Wet Digitale Markten. Als consument maak ik me zorgen over deze ontwikkeling.
Ik heb voor de iPhone gekozen vanwege de sterke betrokkenheid bij privacy en beveiliging, een kenmerk van de filosofie van Apple.

Ik begrijp dat ik onder de nieuwe regelgeving niet verplicht ben om apps van buiten de App Store te downloaden. Ik zou echter de voorkeur geven aan een optie waarmee ik zelfs de mogelijkheid kan vermijden om apps van externe bronnen tegen te komen, inclusief het vermijden van pop-ups of meldingen daarover. In wezen wil ik de huidige gebruikerservaring van de iPhone behouden, waarbij de App Store de enige bron voor apps is.

Zou Apple kunnen overwegen om een functie te introduceren waarmee gebruikers zoals ik hun iPhone kunnen beperken om alleen apps uit de Apple App Store te downloaden?
Deze optie handhaaft het recht van de consument om het niveau van beveiliging en privacy te kiezen waar hij of zij zich prettig bij voelt, wat volgens mij in overeenstemming is met de beginselen van eerlijke concurrentie.

Aan: **Tim Cook**
Van: **Apple Gebruiker**
Onderwerp: **Sideloading**
Datum: **16 januari 2024**

Kun je wel veiligheid garanderen aan mensen die geen sideloading op hun apparaten willen?

Veel mensen geven er toch de voorkeur aan om normale programma's te krijgen. Een manier om zijwaarts laden niet te accepteren en "normale Apple programma's" te hebben bij installatie zou een mooie manier zijn.

Google-programma voorkomt Sideloading

Android heeft sideloading sinds het begin toegestaan, maar het lijkt erop dat Google heeft ingezien dat deze praktijk gebruikers met een hoge beveiligingsgraad in gevaar brengt.

Google ontwierp zijn **Advanced Protection Program** voor gebruikers wiens "accounts bijzonder waardevolle bestanden of gevoelige informatie bevatten" en **raadt** "journalisten, activisten, bedrijfsleiders en mensen die betrokken zijn bij verkiezingen" **sterk aan** om zich in te schrijven voor het programma. Een van de belangrijkste kenmerken van het programma is dat het sideloading voorkomt om "schadelijke downloads" tegen te gaan. Deelnemers aan het programma kunnen alleen apps installeren van "geverifieerde winkels, zoals Google Play Store en de app store van de fabrikant van je apparaat".

De risico's die worden verminderd (maar niet geëlimineerd) door Apple's waarborgen voor de distributie van apps en alternatieve betalingssystemen

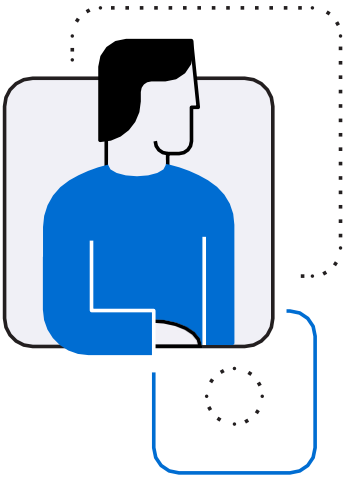
Deze beveiligingen helpen om de iPhone-ervaring van EU-gebruikers zo veilig, privacybeschermend en betrouwbaar mogelijk te houden, hoewel niet in dezelfde mate als in de rest van de wereld. In dit gedeelte wordt nader ingegaan op de categorieën risico's die met deze beveiligingen worden aangepakt.

NOTARISATIE

Notarization is gericht op het detecteren van schadelijke apps door het identificeren van ernstige bedreigingen voor de veiligheid, privacy en beveiliging van gebruikers. Bijvoorbeeld:

- Een veel voorkomende manier waarop schadelijke apps hun weg vinden naar apparaten is via ***social engineering - door*** gebruikers te manipuleren om toegang te verlenen tot hun apparaat door zich voor te doen als iets wat ze niet zijn, bijvoorbeeld door populaire, legitieme apps te imiteren. Notarization probeert deze bedreiging te verminderen door te controleren of de manier waarop een app zichzelf via zijn metadata presenteert, nauwkeurig weergeeft hoe de app werkt tijdens de beoordeling. Notarization zal apps analyseren met

als doel te voorkomen dat dit soort kwaadwillende imitators op apparaten terechtkomen.



Door een combinatie van menselijke en geautomatiseerde beoordeling heeft Apple bijvoorbeeld een aantal apps geïdentificeerd die zich voordeden als een legitiem advertentieplatform om inloggegevens te stelen. Notarization controleert op schadelijke apps zoals deze. Menselijke beoordeling is essentieel om deze oplichtingspraktijken te ontdekken - geautomatiseerde beoordeling kan niet controleren op aanvallen die zijn ontworpen om gebruikers te manipuleren.

- Slechteriken kunnen ***hun bedoelingen*** ook ***verkeerd voorstellen*** aan de gebruiker om hem te overtuigen vrijwillig toegang te verlenen tot beschermde delen van hun iPhone, zoals locatieservices, HealthKit (waarin gezondheidsgegevens worden opgeslagen), microfoon, camera, contacten, foto's en meer. Dit kan leiden tot het verlies van toegang tot belangrijke bestanden, financiële schade als de gebruiker het losgeld betaalt of emotionele en psychologische schade als de privénotities, foto's en andere bestanden van de gebruiker openbaar worden gemaakt. Notarization, en in het bijzonder onze menselijke reviewers, zullen ook malware identificeren en blokkeren die gebruikers probeert te misleiden over de reden waarom het hun toestemming vraagt om toegang te krijgen tot andere delen van de iPhone - toestemming die essentieel is voor de kwaadwillende app om toegang te krijgen tot gegevens buiten de streng gecontroleerde sandbox.

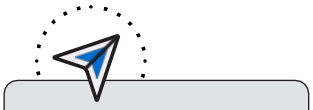
- Dit is een vorm van malware die zonder medeweten van de eindgebruiker op een apparaat wordt geïnstalleerd en gevoelige informatie steelt, zoals contacten, foto's en video's. ***Consumenten spyware kan worden*** gebruikt om de privacy van een intieme partner te schenden. Consumer spyware kan worden gebruikt om de privacy van een intieme partner te schenden, of door hackers die gegevens willen ontfutselen die te gelde kunnen worden gemaakt, zoals bedrijfsgeheimen, of om een hefboomwerking te krijgen over de gebruiker als onderdeel van een ander crimineel plan. Slechte actoren kunnen dergelijke gevoelige gegevens ook verkopen zonder toestemming van de gebruiker, inclusief het schenden van de rechten van de gebruiker of het privacybeschermende beleid van Apple. Notarization, en onze menselijke beoordelaars, zullen ook op zoek gaan naar apps die hun ware doel en mogelijkheden verbergen om zo spyware voor consumenten in te zetten.

- Ontwikkelaarshulpmiddelen zelf kunnen kwaadaardige software bevatten, of ze nu bewust kwaadaardig zijn of geïnfecteerd raken, wat een bedreiging vormt voor zowel gebruikers als ontwikkelaars. Kwaadaardige SDK's die een ontwikkelaar bewust of onbewust in zijn app opneemt, kunnen locatiegegevens verzamelen en deze verkopen aan gewetenloze entiteiten, opportunistisch beschermde gegevens verzamelen waarvoor de app zelf legitieme toestemming van de gebruiker heeft verkregen; of proberen een gebruiker zonder toestemming clandestien te volgen op websites en in apps. Notarization zal apps controleren om te identificeren of ze

Meer over bedreigingen van Sideloading

In de artikelen "Building a Trusted Ecosystem for Millions of Apps" uit 2021 kun je meer lezen over hoe kwaadwillenden kunnen proberen om sideloaded apps te gebruiken om de beveiliging, privacy en veiligheid van gebruikers te bedreigen, vooral zonder de nieuwe beveiligingen van Apple: "**A Threat Analysis of Sideloading**" en "**The Important Role of App Store Protections**".

gecompromitteerde ontwikkelaarshulpmiddelen hebben die zijn ingebed in hun apps - zoals die SDK's - waarvan we weten dat ze ***malware*** bevatten, wat ontwikkelaars zelf beschermt tegen bedreigingen van kwaadwillende actoren die geïnfecteerde ontwikkelaarshulpmiddelen zouden kunnen aanbieden die malware bevatten en verspreiden.



Aan: **Tim Cook**
Van: **Apple Gebruiker**
Onderwerp: **Teleurgesteld** Datum: **15 januari 2024**

Al snel zul je niets meer hebben om je van anderen te onderscheiden.
Dit besluit zal gevolgen hebben voor veel van mijn vrienden en familie die vertrouwen op het vermogen van de iPhone om hen te beschermen tegen slechte actoren. Ik ben zal h e t moeilijk hebben om te rechtvaardigen dat ze nu geld uitgeven aan een iPhone.... Ik weet niet zeker of u dit persoonlijk zult lezen, maar ik hoop dat Apple een manier heeft om mensen te beschermen als dit de weg is die ze van plan zijn in te slaan.

- Kwaadaardige apps kunnen zelfs ***fysieke schade*** toebrengen aan gebruikers. Notarization zal apps beoordelen op deze risico's. Notarisatie zal bijvoorbeeld controleren of apps gebruikers of anderen schade toebrengen, zoals "uitdagingsapps" - zoals een aantal apps die zijn gemaakt door kwaadwillenden als reactie op een gevaarlijke online uitdaging waarbij gebruikers gedurende 50 dagen taken kregen opgelegd om zelfmoord te plegen. Deze apps waren ontworpen om geleidelijk elementen van zelfbeschadiging te introduceren,
met als laatste uitdaging dat de "speler" zichzelf moet doden. Apple heeft deze apps betrapt en van iOS verwijderd. Notarization wil gevaarlijke apps als deze van iOS blijven weren.

VEREISTEN VOOR ALTERNATIEVE APP-MARKTPLAATSEN

De criteria om in aanmerking te komen voor het exploiteren van een alternatieve app-marktplaats zullen helpen voorkomen dat andere soorten kwaadaardig gedrag schade toebrengen aan gebruikers van iOS, doordat er voortdurend toezicht nodig is. Hoewel Apple het veiligste en veiligste mobiele computerplatform ter wereld biedt - zoals onafhankelijke deskundigen herhaaldelijk hebben [bevestigd7] - zullen kwaadwillenden altijd proberen onze bescherming te omzeilen. Ondanks geavanceerde tools en beoordelingsteams van experts, is aanhoudende en voortdurende bewaking noodzakelijk om geavanceerde, vermomde schadelijke apps te onderscheppen die niet in eerste instantie door Notarization worden gedetecteerd.

We hebben ook apps gezien die zichzelf kunnen transformeren van onopvallend tot kwaadaardig ***nadat*** ze zijn goedgekeurd. Apps die onschuldig lijken en dus door de Notarisatie komen, kunnen worden geactiveerd door een extern signaal dat kwaadaardige functies inschakelt na goedkeuring, waardoor ze veranderen in crypto-oplichting, copycats, witwastools of nog erger. Dit worden **bait and switch apps genoemd**. Deze apps kunnen een component bevatten die informatie van de server van de ontwikkelaar weergeeft, zodat de cybercrimineel de gebruikersinterface die aan de gebruiker wordt getoond na de notaris kan wijzigen, zodat de app kwaadaardig wordt.

Of een app kan versleutelde code bevatten die niet meteen kwaadaardig lijkt, maar wordt geactiveerd door een externe omstandigheid, zoals geolocatie, IP-adres (dat wil zeggen, als de app niet wordt geopend op locaties of door apparaten die Apple werknemers zouden kunnen zijn), of hoe lang het geleden is sinds indiening (dat wil zeggen, lang genoeg dat de slechte actor denkt dat de app waarschijnlijk de Notarisatie heeft voltooid). Een app die tijdens de Notarisatie bijvoorbeeld een rekenmachine leek te zijn - en dus door de Notarisatie kwam - kan code bevatten die Apple niet kent en die, nadat de app

door de Notarisatie kwam, de app in een illegale gok-app verandert.

Deze apps kunnen alleen worden geïdentificeerd door middel van voortdurende bewaking. Door middel van voortdurende controle heeft Apple de volgende apps ontdekt die kwaadaardig werden nadat ze in de App Store terecht waren gekomen:

- Een app die zich voordeed als een app die reisinformatie en -diensten aanbood, maar na goedkeuring overschakelde naar een illegale lening-app van een niet-geverifieerde dienstverlener.

- Een populaire chat-app voor volwassenen die in het geheim was ingesloten met ransomware; de app vroeg eerst om toegang tot de contactenlijst van de gebruiker en als de gebruiker vervolgens geen losgeld betaalde, dreigde de app alle gebruikers in hun contactenlijst op de hoogte te stellen van hun gebruik van de chat-app voor volwassenen.

- Een app die zich voordeed als een app die informatie verschafte over dieren, maar na goedkeuring overschakelde naar een app die illegaal gokken mogelijk maakte.

Apple voert deze voortdurende controle uit op apps die via de App Store worden gedistribueerd en kan elke schadelijke app die we identificeren snel verwijderen. Sommige van deze beschermingen zullen worden toegepast in het nieuwe landschap in de EU. Deze omvatten geautomatiseerde tools die proberen te detecteren of apps zijn gewijzigd sinds de Notarisatie, zoals door periodiek apps te installeren en te starten alsof ze zijn geïnstalleerd via een alternatieve app-marktplaats. Apple gebruikt echter ook andere signalen, waaronder marktspecifieke signalen, zoals gegevensanalyse van gebruikersrecensies en downloads in de App Store. We kunnen deze marktspecifieke signalen niet gebruiken om deze voortdurende beoordeling uit te voeren voor apps die op alternatieve app-marktplaatsen worden gedistribueerd, waardoor we veel minder hulpmiddelen hebben om te begrijpen wanneer een app mogelijk kwaadaardig is geworden. Als gevolg hiervan moeten alternatieve app-marktplaatsen zich inzetten voor het monitoren op schadelijke apps om gebruikers te beschermen tegen deze zeer reële bedreigingen.

En zonder criteria om ervoor te zorgen dat marktplaatsen legitieme bedrijven zijn die over de nodige middelen beschikken om apps te distribueren namens ontwikkelaars, kunnen gevaarlijke marktplaatsen ook gemakkelijk hun weg vinden naar de apparaten van gebruikers. Het zou bijvoorbeeld kunnen gaan om zwendelmarkten die zich voor een korte periode vestigen, gebruikers overtuigen om valse of namaak-apps te kopen en vervolgens de marktplaats sluiten - waardoor het erg moeilijk wordt om op te sporen - voordat gebruikers zich realiseren dat ze zijn opgelicht. Het kan ook gaan om marktplaatsen die niet in staat zijn om de apps die ze aanbieden zinvol te controleren op beveiligings-, privacy- en veiligheidsproblemen. Of het kan gaan om marktplaatsen die opereren zonder duidelijke financiële middelen, die transacties tussen ontwikkelaars en gebruikers faciliteren en vervolgens sluiten vanwege een gebrek aan middelen, waardoor gebruikers geen verhaalsmogelijkheid hebben als ze problemen ondervinden met de apps die ze van de marktplaats hebben gedownload, een terugbetaling willen aanvragen of aangifte willen doen... oplichterij. Apple heeft criteria ontwikkeld om het risico van dergelijke gevaarlijke

app-marktplaatsen te minimaliseren, terwijl er opties blijven bestaan voor legitieme marktplaatsen.

APP INSTALLATIEBLADEN

De app-installatiebladen informeren gebruikers ook en helpen gebruikers oplichting en social engineering-aanvallen te voorkomen. Kwaadwillenden proberen gebruikers vaak te verleiden tot het downloaden van schadelijke programma's, onder andere via namaak-apps, zwendel verspreid via sociale media, valse systeemupdates, phishing-methoden via e-mail, reclame op websites die er legitiem uitzien en vele andere kwaadwillende tactieken. Slechte actoren kunnen bijvoorbeeld apps valselijk presenteren op websites die gebruikers vervolgens naar een alternatieve markt leiden, waardoor de ontwikkelaar op zijn beurt een verkeerde voorstelling van zijn app kan geven. Omdat installatiebladen voor apps helpen om elke gebruiker te informeren over wat hij downlaadt en waarvandaan, zullen ze het risico dat kwaadwillenden gebruikers verleiden tot het downloaden van een kwaadaardige app aanzienlijk verkleinen - maar niet uitsluiten.

Deze sheets zullen ook helpen beschermen tegen apps die zichzelf verkeerd voorstellen op alternatieve app-marktplaatsen, maar kunnen dit ook niet volledig voorkomen. App-marktplaatsen zouden ervoor kunnen kiezen om geen regels te hebben met betrekking tot de manier waarop een app zichzelf aanprijst op hun platform. Op die marktplaatsen kan een app zich niet alleen presenteren als een totaal andere app, maar kan hij ook andere prijzen of abonnementen voorstellen dan hij de gebruiker daadwerkelijk in rekening brengt, of ten onrechte beweren dat hij andere functies heeft...

of diensten. Het installatieblad van de app, dat de gegevens weergeeft die de ontwikkelaar indient over zijn app en dat vervolgens op juistheid wordt gecontroleerd tijdens de notariële akte, creëert een achtervang zodat gebruikers geïnformeerd kunnen worden over hoe de app eruit zag en wat het verklaarde doel ervan was toen de app ter beoordeling werd ingediend bij Apple.

INFORMATIE OVER ALTERNATIEVE BETALINGSOPTIES

Voor alternatieve betalingsopties helpen onze informatieve banners om gebruikers te informeren over de onvermijdelijke risico's die zich kunnen voordoen, zoals specifieke rooftechnieken die het beveiligde handelssysteem van Apple voorkomt. Ons systeem beschermt tegen kwaadwillende actoren die opzettelijk verwarrende ontwerpen en teksten gebruiken om gebruikers te verleiden tot aankopen of abonnementen onder voorwaarden die ze niet bedoelen of begrijpen, of die het voor de gebruiker bijna onmogelijk maken om te annuleren. Bovendien:

- Omdat alle apps op iOS die digitale goederen en diensten verkopen binnen de app tot nu toe gebruik maakten van het beveiligde handelssysteem van Apple, heeft Apple ervoor kunnen zorgen dat gebruikers elk abonnement waarvoor ze zich aanmelden eenvoudig kunnen opzeggen met één simpele

tik. En via het StoreKit-ontwikkelaarsraamwerk dat In-App Purchase mogelijk maakt, zorgt Apple ervoor dat de prijzen en voorwaarden van de
in-app aankopen zijn precies wat de ontwikkelaar heeft ingesteld op zijn SKU in App Store Connect. Ongeacht de manier waarop de app zijn prijzen en voorwaarden aanprijst, krijgt de gebruiker altijd een bevestiging van de prijs die hij zal moeten betalen.
in rekening gebracht voordat de aankoop wordt gedaan. Zonder dit systeem kunnen apps het moeilijk maken voor gebruikers om uit te zoeken hoe ze hun abonnement kunnen opzeggen om deze gebruikers te ontmoedigen om weg te gaan, of misleidende tactieken gebruiken om hen te misleiden.

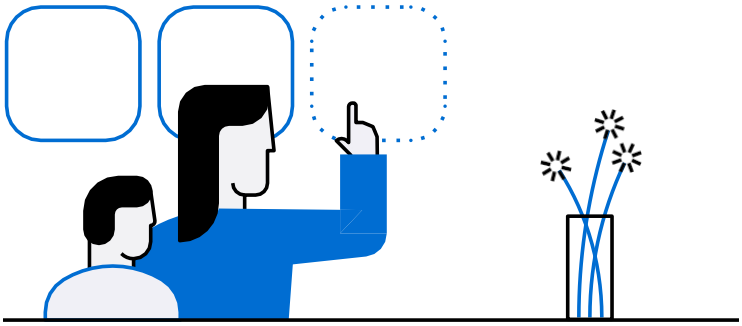
om een abonnement af te sluiten onder voorwaarden of tegen prijzen die de gebruiker in eerste instantie niet begreep, bijvoorbeeld door een verkeerde voorstelling van hoe lang een gratis proefabonnement duurt of hoe vaak of hoeveel een gebruiker voor het abonnement moet betalen.[8]

- Het beveiligde handelssysteem van de App Store helpt voorkomen dat apps meer voor een digitaal goed vragen dan ze vermelden. Wanneer een app bij Apple wordt ingediend voor mogelijke opname in de App Store, moet deze de prijs van de digitale goederen en diensten vermelden. Apple kan testen of de app daadwerkelijk kosten in rekening brengt het bedrag dat aan de gebruiker werd geadverteerd, en kan controleren of een app de geleverde digitale goederen of diensten veel te duur aanbiedt. We hebben het afgelopen jaar actie ondernomen tegen honderden apps vanwege hun manipulatieve prijzen. Als onderdeel van de standaard, consistente afrekenstroom voor digitale goederen en diensten die gebruikmaken van In-App Purchase, zorgen de API's van het handelssysteem van Apple er ook voor dat de app het volgende weergeeft de prijs die hij aan Apple heeft doorgegeven aan de gebruiker (samen met andere ingediende productinformatie en belangrijke aankoopvoorwaarden) voordat de gebruiker de aankoop voltooit, zodat de gebruiker weet wat hem in rekening zal worden gebracht, ongeacht of de app het werkelijke bedrag aan hem heeft bekendgemaakt. Zonder dit systeem waarop gebruikers hebben vertrouwd, heeft de gebruiker mogelijk niet de zekerheid dat de prijs die de ontwikkelaar op de markt brengt een nauwkeurige weergave is van wat hij uiteindelijk zal betalen.

- Apple beschermt kinderen en gezinnen verder met diensten zoals **Ask to Buy**, waarbij toestemming van de ouders is vereist voor elk item dat hun kinderen willen kopen of downloaden op iPhones, zodat ouders er zeker van kunnen zijn dat scammers hun kinderen niet als doelwit kiezen.

- De antifraudemaatregelen van Apple beschermen gebruikers tegen frauduleuze ontwikkelaars, maar ze beschermen ontwikkelaars ook tegen frauduleuze gebruikers (zoals mensen die transacties verrichten met gestolen creditcards), onder andere doordat Apple de gegevens van zijn betalingssysteem analyseert om trends en ontwikkelingen te identificeren, waardoor Apple oplichtingspraktijken en gewetenloze individuen kan uitroeien.

- Het handelssysteem van de App Store kan er ook voor zorgen dat apps doen wat ze beloven. Wanneer een gebruiker een aankoop doet via het systeem van Apple, wordt die transactie weggeschreven naar de aankoopgeschiedenis van de gebruiker. Als de app geen digitale goederen of diensten levert nadat de gebruiker heeft betaald, kan Apple de transactie gebruiken



Beste Tim

Echte e-mails ontvangen door Tim Cook over wijzigingen aan iPhone in de Europese Unie

Aan: **Tim Cook**
Van: **Apple Gebruiker**
Onderwerp: **Geen Android** Datum: **21 april 2023**

We zijn erg tevreden met iOS omdat het niet is zoals Android, het heeft een hoge veiligheid, het heeft een gebruiksvriendelijke interface en het heeft nooit
vertraagt, maar we hebben uit bronnen vernomen dat sideloading mogelijk is in iOS 17 en dat het kan worden gedownload uit andere winkels dan de
App Store. Het kan ook worden gedownload. Stop hier alstublieft mee. We willen gewoon downloaden uit de App Store en onze veiligheid waarborgen. Schakel sideloading niet in. We willen dat iOS net zo wordt als het oude, met strenge regels en extreem hoge beveiliging.

Aan: **Tim Cook**
Van: **EU Apple** gebruiker
Betreft: **Van een bezorgde Apple gebruiker en EU burger**
Datum: **24 oktober 2023**

Ik maak me steeds meer zorgen en ben bang voor mijn digitale privacy en online veiligheid in de EU. Als EU-burger en Apple-gebruiker dacht ik altijd dat ik de perfecte balans had tussen bescherming door regelgeving (zoals GDPR) en veiligheidsfuncties van Apple (zoals App Tracking Transparency en App Store). Maar onlangs... is dat veranderd.

Ik, mijn familie, vrienden en collega's zijn Apple gebruikers en hebben specifiek gekozen voor het Apple ecosysteem voor ons werk en vrije tijd vanwege de manier waarop de producten en software zijn ontworpen om privé en veilig te zijn. Plus natuurlijk de veiligheidsfuncties die in de loop der jaren zijn geïntroduceerd. Het is een eng idee, maar het ziet ernaar uit dat nieuwe regelgeving van de EU-Commissie veel van die veiligheids- en beveiligingsfuncties waar ik nu op vertrouw in gevaar zou brengen.

Aan: **Tim Cook**
Van: **EU iPhone Gebruiker**
Onderwerp: **Sideloading EU**
Datum: **25 januari 2024**

Ik hoop echt dat u mij als EU-klant de optie biedt om geen gebruik te maken van
zijladers. Ik wil kunnen vertrouwen op de App Store en niet op een of andere onzin...

Aan: **Tim Cook**
Van: **EU Apple gebruiker**
Betreft: **Bezorgdheid en suggesties met betrekking tot het mandaat van de EU om Sideloading toe te passen**
Datum: ~~**26 januari 2024**~~

Ik schrijf om mijn bezorgdheid te uiten over de recente eis van de Europese Unie (EU) aan Apple om sideloading toe te staan op iOS-apparaten. Ik begrijp dat dit besluit is genomen om de concurrentie en de keuze voor de consument te bevorderen, maar ik ben van mening dat het belangrijke privacy- en veiligheidsoverwegingen oproept.

... De App Store is een vertrouwde bron voor iOS-applicaties en biedt een niveau van vertrouwen en veiligheid dat cruciaal is in het huidige digitale tijdperk. Persoonlijk heb ik me altijd veilig gevoeld in de wetenschap dat de apps die ik download uit de App Store strenge controleprocessen ondergaan om mijn apparaat en persoonlijke gegevens te beschermen.

Met de introductie van sideloading bestaat er echter een potentieel risico dat gebruikers onbewust kwaadaardige of niet-geverifieerde toepassingen van externe bronnen installeren, waardoor de algehele veiligheid van iOS-apparaten in gevaar komt. Deze verschuiving kan gebruikers blootstellen aan verschillende cyberbeveiligingsbedreigingen en ik maak me zorgen over de mogelijke gevolgen van sideloading op iOS.

geschiedenis om te valideren of de transactie heeft plaatsgevonden en actie te ondernemen tegen apps die hun deel van de transactie niet nakomen. Zonder deze geschiedenis kan Apple gebruikers niet helpen als apps een transactie niet nakomen.

- Apple heeft ook duizenden AppleCare-agenten die gebruikers kunnen bellen voor hulp bij terugbetalingen of andere klantenondersteuning. Deze medewerkers kunnen geen ondersteuning bieden voor aankopen die zijn gedaan via alternatieve betalingssystemen.

Gebruikers vertrouwen al bijna twintig jaar op de voordelen en bescherming van het beveiligde en private handelssysteem van Apple, dat ze gebruiken om digitale goederen en diensten te kopen. De informatieve banners houden gebruikers op de hoogte dat ze op hun hoede moeten zijn voor misleidende technieken waartegen Apple hen tot nu toe heeft beschermd.

De rol van alternatieve app-marktplaatsen en alternatieve betalingsverwerkers bij het verder terugdringen van risico's

In de komende maanden zullen veel gebruikers in de EU apps op iOS kunnen downloaden van alternatieve app-marktplaatsen en betalingen kunnen verrichten via alternatieve betalingsverwerkers. Dit betekent een grote verandering ten opzichte van de manier waarop het altijd heeft gewerkt op de iPhone. Omdat gebruikers erop vertrouwen dat Apple hun apparaten beschermt, hoefden ze zich geen zorgen te maken of hun bron van apps van derden of hun in-app betalingssysteem een bedreiging voor hen vormden. Gebruikers zullen niet langer van die bescherming uit kunnen gaan.

Apple neemt substantiële, zinvolle maatregelen om gebruikers in de EU te beschermen in de nieuwe wereld van alternatieve distributie en alternatieve betalingen die de DMA heeft geopend. Maar de reikwijdte van deze maatregelen wordt noodzakelijkerwijs beperkt door de wet. Apple moet daarom de verantwoordelijkheid voor de functies ter bescherming van gebruikers die het niet langer alleen mag uitvoeren, overdragen aan de alternatieve app-marktplaatsen en betalingsverwerkers zelf.

Dat betekent dat alternatieve app-marktplaatsen en alternatieve betalingsverwerkers waarschijnlijk een onvermijdelijke rol moeten spelen in de bescherming van gebruikers, zelfs als gebruikers hun app niet op de markt brengen.
ze niet willen gebruiken. Veel gebruikers hebben contact met ons opgenomen met de vraag of ze eenvoudigweg kunnen afzien van de wijzigingen

die Apple heeft aangekondigd om te voldoen aan de DMA. En sommige commentatoren hebben betoogd dat gebruikers niet verplicht zijn om gebruik te maken van de nieuwe opties die Apple in de EU beschikbaar stelt als ze dat niet willen; in plaats daarvan, zeggen deze commentatoren, kunnen gebruikers gewoon doorgaan met het uitsluitend downloaden van apps uit de App Store.

Aan: **Tim Cook**
Van: **EU iPhone Gebruiker** Onderwerp: **Klant uit de Europese Economische Ruimte**
Datum: **23 januari 2024**

Het was mijn vrije keuze om een Apple iPhone te kopen, en ik deed dat omdat ik me veiliger voel met iOS dan met een apparaat waarop Android. Nu mijn eigenlijke vraag: Zou het niet mogelijk zijn voor mij als klant om de vrijheid te hebben om te kiezen of ik in de toekomst de iOS-versie installeer die bedoeld is voor de Europese markt, of dat ik de iOS-versie kan installeren die in de rest van de wereld wordt gebruikt?

Gebruikers zullen waarschijnlijk ook geen andere keuze hebben dan meerdere accounts aan te maken bij elke app-marktplaats en alternatieve betalingsoptie die ze gebruiken. Dit is niet alleen onhandig voor de gebruiker en verslechtert zijn ervaring - het verhoogt ook het risico dat zijn gegevens worden gestolen. Hoe meer accounts een gebruiker heeft, hoe meer verschillende plaatsen zijn persoonlijke en financiële gegevens worden opgeslagen, waardoor het risico toeneemt dat die gegevens worden blootgelegd bij een datalek - wat steeds waarschijnlijker wordt.[9] Bovendien zouden gebruikers nog meer geconditioneerd kunnen raken om lukraak hun gegevens te delen en app-distributeurs te vertrouwen - zelfs als de distributeurs misschien niet legitiem zijn. Een slechte speler zou een gebruiker voor de gek kunnen houden door zich voor te doen als een legitieme app-marktplaats op een website buiten iOS, en de gebruiker kunnen verleiden tot het verstrekken van betaling of zijn gegevens - waarna de gebruiker ontdekt dat de slechte speler helemaal geen marktplaats had.

Maar in de praktijk zullen gebruikers in de EU de keuze verliezen om alleen in de App Store te blijven en alle toonaangevende bescherming van Apple te behouden, zelfs als ze daar de voorkeur aan geven. Sommige ontwikkelaars zullen ervoor kiezen om hun apps uitsluitend op alternatieve app-marktplaatsen beschikbaar te stellen. Dit kunnen apps zijn die gebruikers nodig hebben voor hun werk of school, of die ze nodig hebben om in contact te blijven met familie en vrienden - apps die gebruikers moeten downloaden, zelfs als ze liever geen alternatieve app-marktplaatsen gebruiken. **Ontwikkelaars zullen uiteindelijk bepalen waar grote aantallen EU-gebruikers naartoe moeten om de apps te verkrijgen die ze nodig hebben**, of gebruikers al dan niet tevreden zijn met de bescherming die deze winkels bieden. Ondanks onze inspanningen is het mogelijk dat veel gebruikers niet merken of begrijpen dat ontwikkelaars hen ertoe aanzetten apps te downloaden van een alternatieve app-marktplaats, ondanks de voorkeur van de gebruikers om geen transacties te doen met die marktplaats.

Een Android-app gebruikte SMS phishing om mensen een app te laten sideloaden die zich voordeed als een legitieme postapplicatie. service-app, maar stal vervolgens gevoelige informatie van het apparaat. Het bedrijf herhaalde deze zwendel door zich voor te doen als postservices in verschillende landen. Omdat het voor elke zwendel iets andere apps gebruikte, zou het voor elke markt moeilijker zijn om dit patroon te detecteren.[10]

In de EU zullen de veiligheid, privacy en zekerheid van elke gebruiker deels afhangen van twee vragen. Ten eerste, zijn alternatieve marktplaatsen en betalingsverwerkers in staat om gebruikers te beschermen? En ten tweede, zijn ze geïnteresseerd om dat te doen?

De maatregelen die Apple neemt vormen een belangrijke basis, maar dat betekent niet dat ze op zichzelf voldoende zijn. De ervaringen van gebruikers zullen aanzienlijk verschillen afhankelijk van de manier waarop elke marktplaats en betalingsprovider zaken doet. Dit biedt mogelijkheden voor differentiatie, en net zoals de DMA van plan was, is Apple van plan om krachtig te concurreren om ervoor te zorgen dat

blijft de App Store de meest veilige en privacybeschermende optie voor consumenten. Maar het creëert ook potentiële hiaten.

App Store-signalen

150 miljoen
transacties per dag, inclusief alle gratis en betaalde app downloads en in-app aankopen

3,12 miljoen
beoordelingen en recensies elke dag

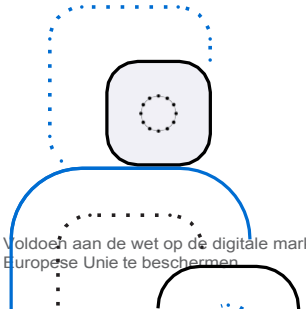
Het beheren van de App Store is al bijna twintig jaar een enorme onderneming. We werken er voortdurend aan om kwaadwillenden en hun steeds verder ontwikkelende schadelijke apps te vinden en tegen te houden. Naast de duizenden technici die
de hardware en software die moeten voorkomen dat kwaadwillenden gebruikers schade toebrengen, werken honderden fulltime Apple medewerkers mee aan App Review, waarbij ze apps beoordelen in meer dan 80 talen in drie tijdzones. Elk jaar beoordelen we meer dan 6 miljoen app-aanvragen. In het laatste volledige jaar waarover gegevens beschikbaar zijn, heeft Apple bijna 4,5 miljoen apps goedgekeurd en 1,6 miljoen apps geweigerd, veelal omdat ze niet goed functioneerden op het apparaat en soms omdat ze in strijd waren met onze beveiligings- en privacyregels. Deze hardnekkigheid is een belangrijke reden waarom iOS sinds de introductie het veiligste mobiele computerplatform ter wereld is gebleven en waarom de meeste kwaadwillenden hebben geconcludeerd dat het niet de moeite waard is om tijd, energie en middelen te investeren in het infecteren van iOS met malware.

Zelfs met onze ervaring en menselijke beoordelaars die 24 uur per dag beschikbaar zijn, hebben we per jaar meer dan 185.000 apps uit de App Store verwijderd omdat later bleek dat ze de richtlijnen van Apple hadden geschonden. Om deze apps te vinden en te verwijderen, controleert Apple zorgvuldig de App Store zelf, waar *elke dag* meer dan 150 miljoen transacties plaatsvinden en meer dan 3,1 miljoen beoordelingen en recensies worden gegeven.
ingediend om problematische apps te identificeren. Apple houdt bij het toezicht rekening met verschillende indicatoren. Dit zijn onder andere gebruikersbeoordelingen, meldingen via onze tool Meld een probleem, feedback aan de duizenden AppleCare-medewerkers die gebruikers ondersteunen en verdachte patronen in de gegevens, zoals ongebruikelijke activiteit in beoordelingen, plotselinge pieken in het aantal meldingen van apps, enzovoort. in het aantal downloads of ongewoon aankoopgedrag. Alleen door goed op deze signalen te letten, kan het team van Apple slechte spelers uitroeien.

Dit zijn onder andere de apps die worden beschreven op pagina 20 en die een niet-geverifieerde lening-app, ransomware-aanval via chat voor volwassenen, de illegale gok-app die Apple heeft gepakt.

Exploitanten van alternatieve app-marktplaatsen zullen nu voortdurend toezicht moeten houden om EU-gebruikers te beschermen tegen bait-and-switch en andere kwaadaardige apps buiten de App Store om.

Zelfs als alternatieve app marktplaatsen aanzienlijke middelen inzetten voor dit toezicht, zal het moeilijker zijn om deze kwaadaardige apps te identificeren dan vóór de DMA. Tot nu toe konden al deze betrouwbaarheidssignalen van apps en ontwikkelaars worden gevonden en geanalyseerd op één plek - de App Store - waardoor een rijke dataset ontstond voor de identificatie van slechte actoren. Maar omdat de app distributie nu ***gefragmenteerd*** zal zijn, zullen deze signalen verspreid zijn over meerdere marktplaatsen. Hoe verantwoordelijk elke individuele app marktplaats beheerder ook is - en Apple hoopt dat ze allemaal zorgvuldig controleren op kwaadwillende actoren - het feit blijft dat *iedereen* (inclusief Apple) minder signalen zal ontvangen wanneer kwaadwillenden



toeslaan. Dat betekent dat elke marktplaats onvermijdelijk minder efficiënt zal zijn in het uitroeien van deze bedreigingen.

Aan: **Tim Cook**
Van: **iPhone-gebruiker**
Onderwerp: **Houd Apple's iOS gesloten alstublieft** Datum: **27 januari 2024**

Als ik een open source besturingssysteem wilde zoals Google of Samsung
Ik zou ze gekocht hebben. De belangrijkste - en ik kan dit niet hardop zeggen
genoeg, de belangrijkste reden waarom ik een Apple telefoon koop en heb is omdat jullie een gesloten iOS hebben en het iOS veiliger is dan Android. Maar als jullie de poorten gaan openen en niet meer zo veilig zijn, dan kan ik net zo goed overstappen. Houd iOS gesloten, alsjeblieft.

Apple maakt zich al lange tijd zorgen over de bescherming van ontwikkelaars en het app-ecosysteem tegen onethische en kwaadwillende gekraakte apps. Deze zogenaamde "gekraakte" apps - waarvan sommige betaalde apps zijn die zijn aangepast om gratis beschikbaar te zijn en waarvan sommige hun code hebben herschreven om wijzigingen te bevatten die niet door de makers waren bedoeld - stelen niet alleen van
hardwerkende ontwikkelaars en schenden hun rechten, maar vormen ook een ernstig risico voor gebruikers. Deze illegale apps zijn vaak een vector voor malware.

In de weken na onze aankondiging van de wijzigingen die vereist zijn door de DMA, h e b b e n we samengewerkt met een aantal ontwikkelaars die geïnteresseerd zijn in het bouwen van
alternatieve app-marktplaatsen. We zijn benieuwd wat ze gaan bouwen. **Maar we hebben ook geleerd over ontwikkelaars met kwade bedoelingen die alleen geïnteresseerd lijken te zijn in deze veranderingen zodat ze marktplaatsen kunnen bouwen die het IP van andere ontwikkelaars stelen en illegale apps distribueren.** Eén ontwikkelaar plande zelfs een vergadering met Apple om ons te vragen naar de verandering en die we doorvoeren als reactie op de DMA, waarop we in goed vertrouwen antwoordden - om er later achter te komen dat de ontwikkelaar verbonden was aan een beruchte

distributeur van illegale software, en dat ze het gesprek illegaal hadden opgenomen en online hadden gezet. Helaas lijken hun vragen bedoeld te zijn geweest om te peilen naar de beste manieren om te profiteren van Apple's aanstaande veranderingen in de EU om een officiële marktplaats voor illegale apps op iOS te bouwen.

De afgelopen vijftien jaar hebben we veel tijd en techniek besteed aan het bestrijden van dit soort slechte actoren, die elke kans die ze konden vinden probeerden uit te buiten om
het IP van onze ontwikkelaars stelen en verspreiden. Maar Notarization zal niet controleren of de apps op een alternatieve app marktplaats inbreuk maken op andermans IP, wat betekent dat het veel moeilijker zal zijn om piraterijdistributeurs te vangen en te voorkomen dat ze marktplaatsen maken die in naam controleren op IP-overtredingen.
alleen. **Deze malafide distributeurs waren enkele van de luidste stemmen die opriepen tot alternatieve distributie om precies deze reden.** Nadat we contact hadden opgenomen met de ontwikkelaar die zijn gesprek met Apple illegaal had opgenomen, beweerde de ontwikkelaar zelfs dat de DMA Apple verbiedt om actie tegen hen te ondernemen om hun distributie van illegale apps op iOS te voorkomen.

BESLISSINGEN OVER INHOUD EN REGELS VOOR BEDRIJFSMODELLEN

Elke alternatieve app-marktplaats zal zijn eigen marktstandaarden ontwikkelen voor inhoud, bedrijfsmodellen en meer, en sommige inhoud en bedrijfsstandaarden zijn niet standaard.
Modellen waar Apple gebruikers altijd tegen heeft beschermd, zullen beschikbaar worden op de iPhone. Dit is wat de DMA bedoelde: marktplaatsen zullen apps kunnen aanbieden die Apple niet zou hebben toegestaan in de App Store. Geen van de nieuwe gebruikersbeschermingen van Apple zal bijvoorbeeld beoordelen of apps inhoud voor volwassenen bevatten, of apps voor gokken of het wisselen van cryptocurrency over de vereiste licenties beschikken, en of apps met door gebruikers gegenereerde inhoud een inhoudsbeheersingsbeleid hebben. We zullen niet kijken of apps het roekeloze gebruik van wapens aanmoedigen of dat ze proberen te profiteren van nationale en wereldwijde crises zoals epidemieën. Elke app-marktplaats zal zelf moeten beslissen of ze dit soort inhoud en bedrijven op hun marktplaatsen toestaan en hoeveel ze investeren in de handhaving van hun regels om ervoor te zorgen dat apps die deze overtreden van hun platforms blijven.

BESLISSINGEN OVER BESCHERMING VOOR GEBRUIKERS EN HUN KINDEREN

Alternatieve app-marktplaatsen zullen ook moeten beslissen welke bescherming ze gebruikers van hun platformen bieden - vooral ouders en kinderen. **Ask to Buy** voorkomt bijvoorbeeld dat kinderen zonder toestemming van hun ouders items kopen of downloaden op hun iPhone, en Apple geeft de leeftijdsclassificatie van een app duidelijk weer op de downloadpagina in de App Store. De App Store verplicht ontwikkelaars ook om het Privacy Voedingsetiket op hun app-overzichten te zetten, waarop de gebruiker het volgende wordt uitgelegd

Op Android-apparaten zijn veel verschillende pornografische apps en games beschikbaar om te sideloaden, inclusief app-marktplaatsen speciaal voor inhoud voor volwassenen.

Apple heeft apps uit de App Store verwijderd omdat ze voornamelijk werden gebruikt om anoniem cyberpesten mogelijk te maken. Eén zo'n app werd gebruikt om anonieme berichten te sturen naar kinderen van middelbare schoolleeftijd waarin ze hen vertelden dat ze hoopten dat ze zelfmoord zouden plegen.[11]

Apple heeft tijdens App Review apps geïdentificeerd die op het eerste gezicht onschuldig lijken, maar die in hun metadata signalen bevatten die duiden op snode bedoelingen, zoals een app die zich aanvankelijk voordeed als een taalprogramma, maar verborgen signalen bevatte dat het van plan was om te veranderen in een gokhal zonder vergunning nadat het op de website was beland. App Store. Apple heeft deze app gevonden en geweigerd.

Apple eist van cryptocurrency exchanges in de App Store dat ze overal waar ze zaken doen over een geldige licentie beschikken. Het weigert regelmatig apps die zich voordoen als cryptocurrency exchanges

maar in plaats daarvan van plan zijn gebruikers op te lichten, of die proberen te werken als niet-gelicentieerde exchanges door de app in te dienen onder het mom van een legitieme app.

Veel populaire spelapps die gericht zijn op kinderen bevatten in-app aankopen, waaronder valuta in het spel, power-ups, loot boxes en meer. Zonder functies zoals Vragen om te kopen, kunnen kinderen honderden dollars aan deze aankopen zonder dat een ouder het merkt. Vorig jaar nog beval de U.S. Federal Trade Commission bijvoorbeeld een spelontwikkelaar "om te betalen $245 miljoen aan consumenten voor het schikken van beschuldigingen dat het bedrijf duistere patronen gebruikte om spelers te verleiden tot het doen van ongewenste aankopen en kinderen ongeoorloofde kosten liet oplopen zonder enige betrokkenheid van de ouders."[12]

Apple staat in de App Store geen apps toe die winst willen maken met nationale crises, zoals de COVID-19 pandemie. Het verwijderde een app die tijdens de pandemie reclame maakte voor privéfeesten, ondanks thuisblijfbevelen, en eiste van apps voor het traceren van contacten dat ze hun volksgezondheidsfunctie niet meer gebruiken om advertenties te verkopen. Apps als deze zouden kunnen worden toegestaan op alternatieve app-marktplaatsen.[13]

hoe een app hun gegevens verzamelt en volgt ***voordat*** de gebruiker de app downloadt op zijn apparaat. Geen van deze functies zijn verplicht voor alternatieve app-marktplaatsen. Marktplaatsen kunnen ervoor kiezen om vergelijkbare bescherming te bieden, of ze kunnen ervoor kiezen om dat niet te doen.

Het streven van Apple om de privacy van gebruikers te beschermen betekent dat een app op zijn Privacy Nutrition Labels moet aangeven welke gegevens de app verzamelt en koppelt aan een gebruiker. Bestaande app-marktplaatsen op andere platforms vereisen een dergelijke duidelijke openbaarmaking van tracking niet.

Hoewel we hopen dat alternatieve app-marktplaatsen op een zinvolle manier zullen investeren in de bescherming van de beveiliging, privacy en veiligheid van gebruikers, kunnen we dit niet garanderen. Hun bedrijfsmodellen kunnen verschillende stimulansen bieden om bescherming voor gebruikers te creëren. Alternatieve app-marktplaatsen met bedrijfsmodellen die gebaseerd zijn op het verzamelen en verkopen van gebruikersgegevens, zouden bijvoorbeeld een commerciële drijfveer hebben om geen functies zoals Privacy Voedingslabels aan te bieden, die het gebruikers gemakkelijker maken om met kennis van zaken toestemming te geven voor het verzamelen en gebruiken van hun gegevens. Hierdoor zouden gebruikers op die marktplaats minder goed op de hoogte zijn van hun mogelijkheden om hun gegevensprivacy te beschermen. Deze app-marktplaatsen zouden ook geen stimulans hebben om te blijven investeren in innovatieve nieuwe manieren om de privacy van gebruikers te beschermen, zoals Apple blijft doen voor gebruikers in de App Store.

BESLISSINGEN OVER BETALINGSONDERSTEUNING VOOR KLANTEN

In 2021 legde de Amerikaanse Federal Trade Commission een online leermiddel met lidmaatschap een boete op van $10 miljoen dollar omdat het niet voldoende duidelijk maakte dat consumenten na afloop van een eerste gratis proefperiode onbeperkt moesten betalen, en was er een lang en verwarrend proces nodig om het abonnement op te zeggen. Met de huidige abonnementenhulpmiddelen van Apple kan een gebruiker zo'n abonnement met één klik opzeggen, maar andere marktplaatsen bieden die service misschien niet.[14]

Het is aan elke afzonderlijke marktplaats, app-ontwikkelaar en/of alternatieve betalingsverwerker om gebruikers ondersteuning te bieden bij betalingen. Sommige bieden uitstekende consumentenbescherming, maar andere niet. In al deze gevallen zal Apple echter niet langer in staat zijn om gebruikers te helpen die in de val lopen van abonnementen of worden misleid tot het doen van een onbedoelde aankoop - de vele AppleCare-agenten van Apple zullen geen ondersteuning kunnen bieden voor een betalingssysteem dat Apple niet ondersteunt.
geen controle. Deze keuzes zullen een enorme complexiteit met zich meebrengen voor gebruikers die begrijpelijkerwijs denken dat ze contact kunnen blijven opnemen met Apple voor ondersteuning nadat ze een digitaal goed of een digitale dienst hebben gekocht via een app die beschikbaar is in de App Store, maar in plaats daarvan ontdekken dat Apple hen niet kan helpen omdat de ontwikkelaar een andere betalingsoplossing heeft gekozen. Daarom is het zo belangrijk dat gebruikers zoveel mogelijk informatie hebben voordat ze een dergelijke transactie aangaan. Apple heeft een rol te spelen in het ondersteunen van gebruikers die transacties doen via alternatieve betalingsmogelijkheden, onder andere door de informatie die het verstrekt, maar derden die deze oplossingen implementeren moeten dat ook doen als ze dat niet doen, zullen de gebruikers daar slechter van worden.

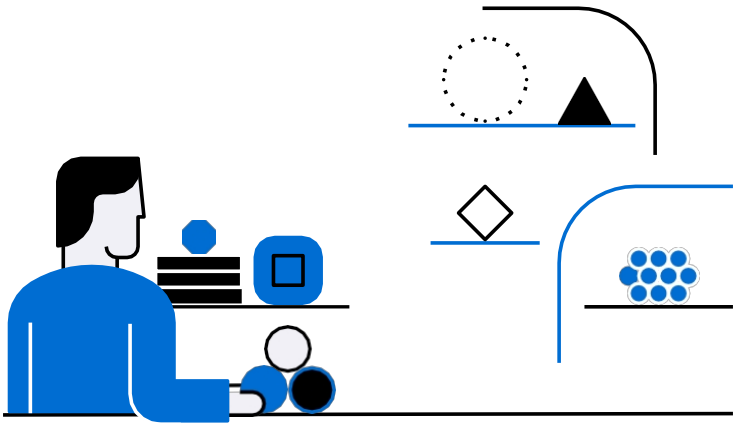
m buiten het bereik van gewone malware gehouden - cybercriminelen zijn er zelfs nog nooit in geslaagd om een enkele wijdverspreide consument te pakken te krijgen.

Hoewel deze veranderingen nieuwe kansen bieden voor concurrentie, zullen ze onvermijdelijk ook nieuwe en lucratieve markten creëren voor kwaadwillende actoren. Kwaadwillenden hebben lange tijd moeite gehad om toegang te krijgen tot de iPhone vanwege de eersteklas beveiliging en privacybescherming. Apple's geïntegreerde benadering van platformbeveiliging heeft het iOS-ecosystee

malware-aanval op iOS. Ze hebben geleerd dat Apple's geïntegreerde benadering van platformbeveiliging de meeste pogingen om malware te infecteren tot mislukken gedoemd is. De
Voor de productie en distributie van kwaadaardige software zijn aanzienlijke middelen nodig en de sterke verdediging van de iPhone heeft ervoor gezorgd dat deze inspanningen geen zinvol rendement opleverden, waardoor het apparaat nog minder aantrekkelijk werd als doelwit.

Op dezelfde manier heeft de proactieve en voortdurende bewaking door Apple het moeilijker gemaakt voor oplichters om voet aan de grond te krijgen op iOS. We ondernemen bijvoorbeeld actie om te voorkomen dat anders legitieme apps worden gebruikt om oplichting te faciliteren, zoals de "pig butchering"-oplichting waarbij gebruikers worden misleid om geld te storten op een frauduleuze beleggingsrekening in een legitieme beleggingsapp. Wanneer we van dergelijke zwendel vernemen, nemen we contact op met de ontwikkelaar van de legitieme app om te voorkomen dat de zwendel zich op die app verspreidt. Door onze acties zijn iOS-apps ook minder aantrekkelijk geworden voor dergelijke zwendelpraktijken.

De nieuwe veranderingen voor iPhone in de EU zullen de calculus veranderen voor kwaadwillenden die voorheen geen manieren zochten om iOS en zijn gebruikers uit te buiten vanwege het relatief lagere rendement dat voor hen beschikbaar was. Naast nieuwe mogelijkheden voor ontwikkelaars, creëren deze veranderingen nieuwe ingangen en potentiële kwetsbaarheden voor oplichters en cybercriminelen. Deze steeds creatievere actoren vormen geraffineerde bedreigingen. Velen vertrouwen op social engineering om gebruikers te verleiden hun meest waardevolle informatie weg te geven.
persoonlijke en gevoelige informatie op een manier waar iedereen in kan trappen, zelfs de slimste gebruiker. Met eenvoudigere toegang tot iPhone-gebruikers via alternatieve kanalen voor het downloaden van apps, neemt het rendement op hun investering toe, waardoor pogingen
iPhone relatief lucratiever te targeten. Om alle redenen die we hebben beschreven, waaronder het onvermogen van Apple om te testen op frauduleuze overbelastingen buiten zijn handelssysteem en de versnippering van marktsignalen, zal het langer duren om oplichters of andere slechte actoren te pakken te krijgen, en we kunnen niet garanderen dat alternatieve app-marktplaatsen dezelfde snelle actie tegen hen zullen ondernemen als wij zouden doen. Hierdoor worden gebruikers langer blootgesteld aan potentiële slechte actoren en krijgen deze slechte actoren mogelijk meer ruimte om creatieve manieren te vinden om gebruikers op te lichten.



Dit creëert een stimulans voor kwaadwillenden om nieuwe programma's te ontwikkelen en nieuwe malware uit te vinden die gericht is op iOS-gebruikers. Deze slechte actoren krijgen de mogelijkheid om hun apps van de ene alternatieve app-marktplaats naar de andere te verplaatsen, waardoor ze de kans krijgen om dezelfde zwendel keer op keer te gebruiken op marktplaats na marktplaats.
of zelfs mogelijk op dezelfde marktplaats met kleine wijzigingen. Dit alles vergroot de kans dat kwaadwillenden hun investering in iOS terugverdienen, wat nog meer kwaadwillende ontwikkeling stimuleert. Misschien nog wel het meest verontrustend is dat dit nieuwe gestimuleerde niveau van criminele investeringen in het bouwen van tools, diensten en infrastructuur om iOS gebruikers aan te vallen, het risico met zich meebrengt dat de kosten voor het aanvallen van zelfs die gebruikers die alleen de App Store gebruiken, zullen dalen.

Laten we duidelijk zijn: Apple bouwt meerdere beveiligingslagen in zijn apparaten en systemen in. We doen er alles aan om deze risico's te beperken. Maar om alle genoemde redenen zullen de risico's toenemen.

Apple streeft naar een veilige, privacybeschermende en beveiligde gebruikerservaring op iPhone. Die toewijding blijft bestaan, zelfs nu we veranderingen hebben doorgevoerd om te voldoen aan de DMA, zodat we er alles aan doen om gebruikers in de EU te beschermen. Ook al zal de ervaring in de EU niet dezelfde zijn als de ervaring die we elders kunnen bieden, deze nieuwe tools en processen zullen ons helpen de risico's die deze veranderingen met zich meebrengen te bestrijden.

Notarisatie zal helpen voorkomen dat gebruikers worden blootgesteld aan kwaadaardige apps die malware bevatten zoals ransomware of spyware voor consumenten, die gebruikers verleiden om meer van hun gegevens vrij te geven dan ze van plan waren, of die hun eigen veiligheid in gevaar brengen. Met app-installatiebladen kunnen gebruikers nauwkeurige informatie krijgen over de apps die ze downloaden, zodat de kans kleiner is dat ze worden misleid om een nep-app te installeren of een app met termen die ze niet begrijpen. Het verplichten van alternatieve app-marktplaatsen tot voortdurende controle zal helpen voorkomen dat schadelijke apps zich ongecontroleerd verspreiden. En informatiebladen over alternatieve betalingssystemen zullen gebruikers laten weten dat ze nu op de hoogte moeten zijn van de laatste ontwikkelingen.
kijk uit voor fraude en zwendel om ze te veel te laten betalen voor wat ze hebben

aangevraagd.

Deze beschermingen dragen ertoe bij dat gebruikers ook in de toekomst een verrijkende, veilige en transparante iPhone-ervaring zullen hebben, waarbij de gebruiker de controle heeft over zijn eigen gegevens. Ook in de toekomst zal iPhone de veiligste en meest privacybeschermende smartphone zijn die momenteel in de Europese Unie verkrijgbaar is, zodat gebruikers het geweldige product krijgen dat ze van Apple verwachten.

Bronnen

1. *Enquête: Bijna de helft van de Android-gebruikers overweegt overstap naar iPhone vanwege zorgen over beveiliging en privacy,* 9to5Mac (16 aug. 2022), https://9to5mac.com/2022/08/16/ android-users-consider-switching- iphone/.

2. *App Store-ontwikkelaars genereerden 1,1 biljoen dollar aan factureringen en verkopen in het App Store-ecosysteem in 2022*, Apple (31 mei 2023), https://www.apple. com/newsroom/2023/05/developers-genereerden-een-punt-een-biljoen-inhet-app-store-ecosysteem-in-2022/.

3. *Zie* voor meer informatie *Apple kondigt wijzigingen aan in iOS, Safari en de App Store in de Europese Unie,* Apple (25 jan. 2023), apple.com/ newsroom/2024/01/apple-announces-veranderingen-aan-ios-safari-en-de-app-winkel-in-de-europese-unie/.

4. *App Store heeft in 2022 meer dan 2 miljard dollar aan frauduleuze transacties tegengehouden*, Apple (mei 2023), https:// www.apple.com/newsroom/2023/05/ app-store-stopped-more-than-2-billion-in-fraudulent-transactions-in-2022/.

5. *2022 App Store Transparantierapport*, Apple (2023), https://www.apple.com/ legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf.

6. Steve Jobs onderkende dit probleem al in 2007. *Zie* Steve Jobs, *iPhone SDK Brief* (17 oktober 2007), *beschikbaar op* https://tidbits. com/2007/10/17/steve-jobss-iphone-sdk-brief.

7. *Threat Intelligence Report 2023*, Nokia, https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/.

8. *Zie* Europees Consumentencentrum Duitsland, *Tips tegen abonnementsvallen op internet*, https://www.evz. de/nl/shopping-internet/internet-fraud/ subscription-traps.html.

9. Stuart Madnick, *De voortdurende bedreiging van persoonlijke gegevens: Sleutelfactoren achter de stijging in 2023* (dec. 2023), https://www.apple.com/newsroom/pdfs/ De voortdurende bedreiging van persoonlijke gegevens - Sleutelfactoren achter de toename in 2023. pdf.

10. *Bouwen aan een vertrouwd ecosysteem voor miljoenen apps: Een dreigingsanalyse van sideloading*, Apple (okt. 2021), op 14.

11. Elizabeth Cassin*, Sarahah: Anonieme app verwijderd uit Apple- en Google-winkels na beschuldigingen van pesten*, BBC (25 feb. 2018), https://www.bbc.com/ news/blogs-trending-43174619.

12. *FTC rondt bevel af dat Fortnite-maker Epic Games moet betalen 245 miljoen dollar voor het misleiden van gebruikers tot*

Ongewenste kosten maken, FTC (4 maart 2023), https://www.ftc.gov/news- events/news/press-releases/2023/03/ ftc-finalizes-order-requiring-fortnite-maker-epic-games-pay-245-million- tricking-users-making; *Kids Mobile Gaming Report: More than two-thirds of Parents Worry Kids Overspending on In-App Purchases*, Sell Cell (5 juni 2020), https://www.sellcell.com/blog/. meer-dan-twee-derde-van-ouders-zeurt-kinderen-over-uitgaven-op-in-app-aankopen/.

13. *App die privéfeesten promoot te midden van COVID-19 verwijderd uit Apple App Store,* Bus. Insider (30 dec. 2020), https:// www.businessinsider.in/tech/apps/news/app-promoting-private-parties-amid- covid-19-removed-from-apple-app-store/ articleshow/80020920.cms; Khadeeja Safdar & Kevin Poulsen, *Google, Apple Struggle to Regulate Covid-19 Tracing Apps*, Wall St. Journal (5 juni 2020), https://www.wsj.com/articles/ why-google-and-apple-stores-had-a- covid-19-app-with-ads-11591365499.

14. *Online leerprogramma voor kinderen ABCmouse betaalt $10 miljoen om de aanklachten van de FTC wegens onwettige marketing- en factureringspraktijken te schikken*, FTC (2 september 2020), https://www.ftc.gov/news-events/ news/press-releases/2020/09/ childrens-online-learning-program-abcmouse-pay-10-million-settle-ftc- charges-illegal-marketing.