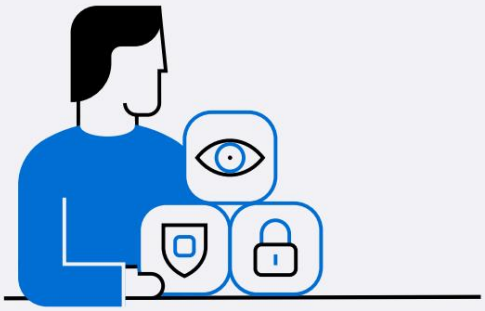


Se conformer au numérique
Loi sur les marchés

Les efforts d'Apple pour protéger la sécurité et la confidentialité des utilisateurs dans l'Union européenne

mars 2024

Contenu

L'objectif d'Apple est de protéger les utilisateurs

Chez Apple, notre plus grande priorité est de créer d'excellents produits qui enrichissent la vie de nos utilisateurs du monde entier. Nous fabriquons des produits que nous souhaitons utiliser nous-mêmes et que nous souhaitons que notre famille et nos amis les plus proches aiment autant que nous. Nous nous efforçons constamment de fournir à nos utilisateurs une expérience sûre et de haute qualité grâce à l'intégration transparente du matériel, des logiciels et des services. Et nous savons que l'une des principales raisons pour lesquelles les clients choisissent Apple (et l'iPhone) est qu'ils croient que nous concrétisons cette vision.1

Lorsque Apple a lancé l'iPhone en 2007, cela a marqué l'ère de l'informatique mobile. Et cela a inspiré de nouveaux produits, dont près de deux millions d'applications de développeurs tiers qui sont devenues essentielles à la vie quotidienne des gens, créant une toute nouvelle économie d'applications responsable de millions d'emplois et facilitant des milliards d'euros de commerce dans le monde.2

Malheureusement, nous vivons également dans un monde où les attaques contre la sécurité et la vie privée présentent des menaces évolutives et de plus en plus sophistiquées pour tout le monde. Les mauvais acteurs créent des applications malveillantes qui peuvent modifier vos données, les prendre en otage contre une rançon ou les divulguer sur l'ensemble du Web. Ils peuvent se livrer à des activités trompeuses ou frauduleuses, chercher à vous espionner sans que vous le sachiez, ou compromettre la fonctionnalité même de votre appareil lui-même. Ils peuvent créer de faux sites Web conçus pour vous inciter à divulguer des données sensibles, vous convaincre de télécharger des logiciels dangereux ou même attaquer votre navigateur Web. Ils peuvent envoyer des e-mails de phishing pour vous convaincre de communiquer vos mots de passe. Les cybercriminels peuvent également tenter de voler vos informations en accédant à votre appareil à votre insu et sans votre consentement, en utilisant des accessoires Bluetooth et des connexions réseau ouvertes, ou simplement en obtenant un accès physique à votre appareil. D'autres acteurs malveillants peuvent même tenter de pirater vos informations et vos messages pendant leur transit numérique vers et depuis votre appareil. Ces mauvais acteurs ont constitué et continueront de constituer des menaces pour tout le monde, quel que soit l'endroit où ils viver

Nous avons conçu l'iPhone pour protéger les utilisateurs contre ce type de risques, en combinant du matériel, des logiciels et des services conçus pour fonctionner ensemble pour une sécurité maximale et une expérience utilisateur transparente au service de l'objectif ultime de protéger les informations personnelles. C'est l'une des raisons importantes pour lesquelles les applications tierces ont réussi à connaître un succès incroyable sur iPhone : car, malgré tous ces risques bien connus et omniprésents, les utilisateurs font confiance à l'engagement d'Apple pour les protéger. Voici quelques-unes des normes les plus importantes d'Apple :

SÉCURITÉ

Les utilisateurs confient à leur iPhone leurs données les plus sensibles. Nous construisons des protections de sécurité de pointe pour empêcher toute personne autre que l'utilisateur d'accéder aux données de son iPhone. Et nous pensons qu'il est essentiel que les utilisateurs disposent d'un endroit fiable où ils peuvent télécharger et découvrir des logiciels en toute sécurité, exempts de logiciels malveillants, de cybercriminels et d'escrocs.

CONFIDENTIALITÉ

Chez Apple, nous pensons que la vie privée est un droit humain fondamental et nous concevons nos produits et services avec des technologies et techniques innovantes pour protéger la vie privée de nos utilisateurs. Les utilisateurs ne doivent pas être exposés à des logiciels ou à des sites Web qui collectent, utilisent ou partagent leurs informations sans leur autorisation éclairée. Nous construisons nos produits et services pour donner aux utilisateurs le contrôle de leurs données et les protéger contre la collecte, l'utilisation ou le partage de leurs informations sans leur autorisation, et pour nous assurer que les utilisateurs savent quelles données les concernant sont partagées et comment elles sont utilisées. , et qu'ils peuvent en exercer le contrôle.

SÉCURITÉ

Les utilisateurs ne doivent pas être exposés à des dommages physiques via iOS, y compris via des applications qui prônent ou causent du tort.

Ces valeurs sont fondamentales pour qui nous sommes, pour ce que les utilisateurs d'iPhone attendent de nous et pour l'intégrité de notre plateforme.

Nous sommes reconnaissants que des utilisateurs de plus de 175 pays et régions du monde aient adopté l'iPhone, et Apple s'engage profondément à respecter ces valeurs fondamentales dans chacun de ces endroits. Cela signifie trouver un moyen de protéger et de préserver la sécurité, la confidentialité et la sûreté des utilisateurs tout en respectant la loi de chaque pays.
où nous faisons des affaires.

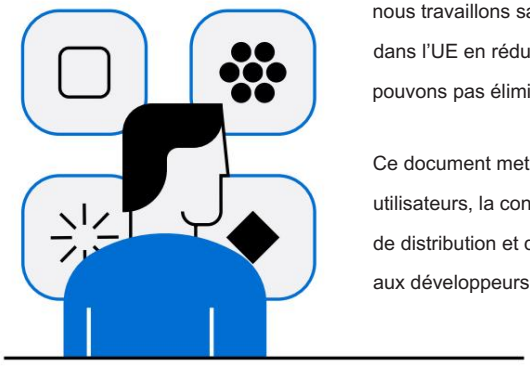
À partir de cette année, la nouvelle loi sur les marchés numériques (DMA) de l'Union européenne nous oblige à adopter une nouvelle approche dans notre travail pour servir nos utilisateurs de l'UE.

Pour nous conformer au DMA, nous avons créé de nouvelles options pour les développeurs et les utilisateurs : et créé plus de 600 nouvelles API et outils de développement pour permettre ces changements. Les nouvelles options incluent l'activation du chargement latéral afin que les utilisateurs de l'UE puissent télécharger des applications via des marchés d'applications autres que l'App Store, permettant d'autres moyens de traiter les paiements sur l'App Store, et de nombreux autres changements. 3 Cela nous a obligé à modifier l'approche particulièrement efficace que nous avons utilisée pour protéger la sécurité et la confidentialité des utilisateurs et assurer leur sécurité.

Depuis le lancement de l'iPhone en 2007, nous avons adopté la même approche pour protéger nos utilisateurs partout dans le monde, englobant de nombreuses protections étendues et à la pointe du secteur contre d'innombrables vecteurs de menaces. Sur l'App Store en particulier, depuis sa création en 2008, nous souhaitions créer un endroit sûr et fiable permettant aux utilisateurs de découvrir des applications et un moyen de fournir aux développeurs un moyen sécurisé et convivial de développer, tester et distribuer des applications aux utilisateurs du monde entier. - et au fil des années, nous avons fourni aux développeurs plus de 40 kits de développement logiciel (SDK), 250 000 interfaces de programmation d'applications (API) et de nombreux autres outils avancés.

En exigeant que toutes les applications sur iPhone soient distribuées via une seule source fiable, l'App Store, nous avons pu atteindre notre objectif de protéger les utilisateurs plus efficacement que toute autre plateforme. Bien que nos efforts pour protéger les utilisateurs et les développeurs ne soient jamais terminés, iOS n'a jamais permis une attaque généralisée de logiciels malveillants grand public contre les utilisateurs, ce qui est exceptionnel pour une plate-forme informatique moderne vieille de 17 ans.

Les nouvelles options que nous introduisons pour nous conformer au DMA signifient nécessairement que nous ne pourrons pas protéger les utilisateurs de la même manière. Afin de continuer à offrir aux utilisateurs la plateforme la plus sécurisée, la plus respectueuse de la vie privée et la plus sûre, conformément à ce que les utilisateurs attendent d'Apple, nous avons conçu et mis en œuvre de nouvelles mesures de protection qui contribueront à les protéger et à les informer. Même si les changements requis par le DMA entraîneront inévitablement un écart entre les protections sur lesquelles les utilisateurs Apple en dehors de l'UE peuvent compter et les protections disponibles pour les utilisateurs de l'UE à l'avenir, nous travaillons sans relâche pour garantir que l'iPhone reste le plus sûr de tous les téléphones. disponibles dans l'UE en réduisant les risques introduits par ces changements nécessaires – même si nous ne pouvons pas éliminer entièrement ces risques.



Ce document met en évidence les mesures clés que nous prenons sur trois fronts importants : la sécurité des utilisateurs, la confidentialité et la sûreté – pour répondre aux changements que le DMA exige en matière de distribution et de paiement des applications, et ce que nous espérons que ces changements apporteront aux développeurs et aux utilisateurs de l'UE. .

Garanties d'Apple pour la distribution d'applications et alternatives Les paiements visent à protéger la sécurité et la confidentialité des utilisateurs et Protégez les utilisateurs

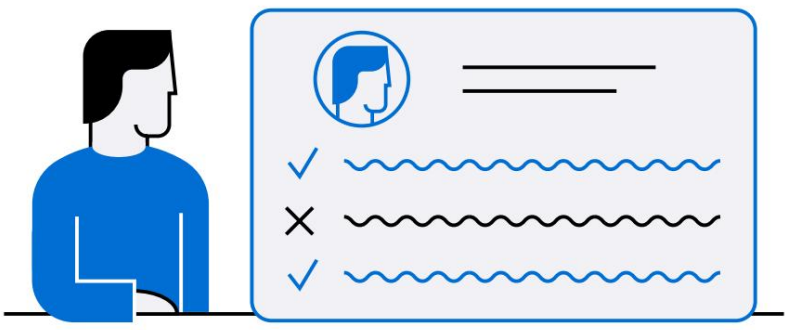
Nous introduisons et développons un certain nombre de fonctionnalités qui soutiendront la sécurité, la confidentialité et la sûreté des utilisateurs tout en permettant le chargement latéral et d'autres moyens de traiter les paiements sur l'App Store dans l'UE. Apple a développé et déployé des mesures de protection visant à garantir que nous continuons à offrir l'expérience la meilleure et la plus sécurisée possible aux utilisateurs de l'UE, même si elle n'est pas aussi sécurisée, respectueuse de la vie privée ou sûre que dans le reste du monde. .

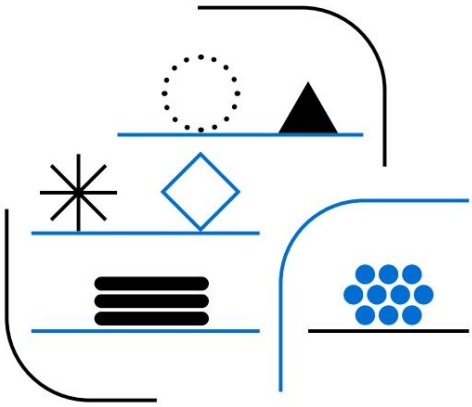
Identifier et arrêter les applications malveillantes

Pour aider à protéger nos utilisateurs de l'UE dans le nouveau paysage créé par le DMA, Apple lance la notarisation pour iOS, un examen de base de toutes les applications (qu'elles soient distribuées via l'App Store ou un marché d'applications alternatif) qui reflète le nouveau paysage de distribution d'applications. et se concentre sur l'intégrité de la plate-forme et la protection des utilisateurs.

Apple signera électroniquement chaque application distribuée sur iOS dans l'UE, quelle que soit la manière dont elle est distribuée, et cette signature sera requise pour toute application sur iOS. Avant de signer une application, Apple analysera chacune d'elles (en utilisant une combinaison d' outils automatisés et d'examen humain) pour vérifier qu'elle est exempte de logiciels malveillants connus et d'autres menaces de sécurité, qu'elle fonctionne généralement comme annoncé et qu'elle n'expose pas les utilisateurs à une fraude flagrante. En effectuant ces vérifications dès le début, nous pouvons contribuer à prévenir les cyberattaques et autres menaces avant qu'elles ne se propagent à d'autres utilisateurs. Ce processus est une extension de la notarisation pour macOS ; depuis des années, Apple analyse et signe les logiciels distribués sur macOS pour s'assurer qu'ils sont exempts de logiciels malveillants connus. Cela a bien fonctionné : nous l'avons donc adapté pour iOS, y compris de nouvelles améliorations pour répondre aux besoins uniques de la plate-forme informatique mobile la plus fiable au monde.

Certes, la notarisation ne couvrira pas tout, comme indiqué ci-dessous, comme le contenu des applications, les pratiques commerciales et les autres protections de l'App Store pour les utilisateurs.





Les protections que nous avons mises en place commencent dès la toute première étape qu'un développeur d'application doit franchir pour distribuer une application sur iOS dans l'UE.

Développement d'applications

Quelle que soit la manière dont un développeur distribue une application sur iPhone, il doit s'inscrire au programme pour développeurs d'Apple avant de créer une application pour iOS (que ce soit dans l'UE ou ailleurs). Dans le cadre du processus d'inscription, Apple demande aux développeurs de vérifier leur identité en exigeant un nom légal, un numéro de téléphone et une adresse (ou, pour une organisation, d'autres identifiants spécifiques). Dans certains cas, il peut être demandé à un développeur son numéro d'identification gouvernemental ou de prouver son identité. Cette protection initiale est une mesure antifraude importante, permettant aux développeurs d'être identifiés et tenus responsables de ce qu'ils distribuent : Apple a empêché la création de près de 105 000 comptes de développeurs frauduleux en 2022 en raison d'activités frauduleuses présumées.4

Lorsque les développeurs s'inscrivent au programme, ils acceptent notre contrat de licence du programme pour développeurs. Cela permet à Apple d'établir des règles de base que les développeurs doivent suivre afin de distribuer leurs applications sur les appareils Apple. Les développeurs s'engagent à ne pas commettre de fraude, à respecter les lois et réglementations applicables et à s'abstenir de concevoir ou de commercialiser leurs applications dans le but de harceler, d'abuser, de spammer, de traquer, de menacer ou de violer de toute autre manière les droits légaux d'autrui. Si un développeur viole l'accord, nous pouvons – et nous le faisons – résilier son accord. En 2022, Apple a supprimé plus de 400 000 comptes de développeurs pour fraude.5

Soumission

De plus, Apple fournit aux développeurs des outils qui les protègent contre certains risques pouvant survenir lors de la phase de développement, avant la soumission. Par exemple, nous avons implémenté la signature du package SDK pour aider les développeurs à vérifier la source du code tiers. Cela permet d'empêcher les développeurs d'utiliser par inadvertance du code modifié de manière malveillante lors de la création de leurs applications.

La notarisation commence lorsqu'un développeur soumet le binaire de son application à Apple. Ce faisant, le développeur indiquera sur quels marchés d'applications il envisage de distribuer l'application, y compris, s'il le souhaite, l'App Store.

Revoir

Lors de la notarisation, Apple effectue un examen à la fois automatisé et humain dans le but d'empêcher les applications qui menacent l'intégrité de la plate-forme, y compris les menaces à la sécurité, à la confidentialité et à la sûreté des utilisateurs, d'atteindre l'utilisateur.

L' examen automatisé utilise l'apprentissage automatique, l'heuristique et des années de données accumulées pour aider à identifier les applications problématiques, en analysant le binaire de l'application à la recherche d'instances de logiciels malveillants connus ou d'autres menaces de sécurité.

L' examen mené par l'homme constitue une ligne de défense essentielle pour aider à protéger les utilisateurs contre les mauvais acteurs. Nos évaluateurs humains analysent chaque application et les spécialistes rejetteront les applications qui enfreignent les directives de notarisation. L'équipe lance et exécute également chaque application sur une plate-forme isolée pour tester si elle fonctionne comme décrit et semble sûre pour les utilisateurs. L'examen automatisé s'appuyant sur les menaces passées, il est essentiel de le compléter par un examen humain pour tenter de détecter les menaces émergentes et nouvelles. Alors que les cybercriminels deviennent de plus en plus créatifs et sophistiqués, l'élément humain de notre processus permet à Apple de rester au courant de l'évolution des menaces. Et l'examen humain est également essentiel dans nos efforts visant à empêcher les applications qui posent des menaces non logicielles, telles que des fraudes flagrantes, d'accéder à l'iPhone. L'examen humain est particulièrement important pour identifier les acteurs malveillants qui tentent d'utiliser des techniques d'ingénierie sociale pour manipuler les utilisateurs afin de leur accorder l'accès à leur appareil et à leurs informations en prétendant être quelque chose qu'ils ne sont pas. Les humains peuvent vérifier si une application malveillante tente de tromper un utilisateur, par exemple en se faisant passer pour une autre application ou en tentant de tromper un utilisateur pour qu'il donne accès à ses données sensibles, et rechercher d'autres techniques malveillantes qu'une machine ne peut pas trouver.

Nous appliquerons ces mêmes contrôles à toutes les mises à jour d'applications, dans le but d'empêcher les acteurs malveillants d'introduire des logiciels malveillants ou d'autres fonctionnalités dangereuses dans chaque application après la mise à jour. téléchargement initial.

Pour être clair : les processus d'examen automatisés et dirigés par l'homme qui constituent ensemble la notarisation ne sont pas des examens d'application. Ils analysent les soumissions pour vérifier leur conformité à un sous-ensemble seulement des directives d'évaluation de l'App Store, et n'incluent pas la plupart des directives d'évaluation les plus importantes de l'App Store. La légalisation englobera les contrôles nécessaires à la protection de nos utilisateurs et essentiels à l'intégrité de la plateforme, y compris ceux qui visent spécifiquement à protéger la sécurité, la confidentialité et la sûreté des utilisateurs.

- Sécurité : la notarisation vérifie les applications pour détecter les menaces de sécurité sur l'appareil. Pour Par exemple, la notarisation garantit que les applications ne contiennent pas de logiciels malveillants connus. Nous n'autoriserons pas non plus les applications qui tentent de lire ou d'écrire en dehors de leur emplacement désigné.

Revoir

zone de conteneur, ce qui permettrait à ces applications de manipuler d'autres applications ou accéder à des données non autorisées à partir de l'appareil de l'utilisateur.

Inciter les utilisateurs à télécharger une application sous de faux prétextes, que ce soit parce qu'ils pensent qu'il s'agit d'une application existante différente ou parce que l'application téléchargée est différente de ce qu'elle devient, est une méthode clé qui les mauvais acteurs utilisent pour transmettre des logiciels malveillants ou d'autres virus sur un appareil sans le connaissance de l'utilisateur, ou pour menacer la sécurité de l'appareil d'une autre manière. Pour éviter cela, dans Notarisation, nous examinerons également si les applications incluent de fausses informations sur leurs fonctionnalités ou capacités ; usurper l'identité d'autres applications ; ou ont des fonctionnalités cachées, dormantes ou non documentées. Nous examinerons également si les applications peuvent télécharger des ressources qui introduiront ou modifieront des fonctionnalités après le téléchargement.

• Confidentialité : la notarisation cherchera à prévenir les menaces à la vie privée des utilisateurs en garantissant que chaque application prend correctement en charge (et ne tente pas de contourner) les fonctionnalités de confidentialité intégrées et essentielles à l'intégrité de tous les appareils Apple. Pour protéger la confidentialité des utilisateurs et assurer la transparence des utilisateurs sur la manière dont leurs données seront utilisées, Apple utilise des mesures techniques pour empêcher les applications d'accéder aux informations sensibles des utilisateurs. iOS n'autorise les applications à accéder à ce type de données qu'après avoir obtenu le consentement de l'utilisateur, que celui-ci peut révoquer à tout moment. Cela s'applique aux données et services tels que :

- le micro
- l'appareil photo
- Identification faciale
- mots de passe enregistrés
- données de localisation fournies par les services de localisation
- données de santé
- l'identifiant unique de l'appareil utilisé par les annonceurs (IDFA)
- Bluetooth
- Portefeuille
- Contacts
- Photos
- Données de l'application pour la maison
- Calendrier
- Liste d'amis du Game Center
- Rappels
- Bibliothèque Apple Musique

La notarisation vérifiera que les applications demandant ces autorisations sont claires et concises quant aux raisons pour lesquelles l'accès est nécessaire, afin que l'utilisateur puisse faire un choix éclairé sur les autorisations à accorder et rester aux commandes lorsque il s'agit de leurs propres données.

Les services de localisation permettent des applications et des sites Web pour utiliser les informations du cellulaire, Wi-Fi, GPS et Bluetooth réseaux pour déterminer un localisation de l'utilisateur avec un haut degré d'exactitude et de précision.

Sous notre suivi des applications Cadre de transparence , les utilisateurs doivent consentir avant un développeur peut accéder à son identifiant d'appareil unique utilisé par les annonceurs (IDFA) pour les suivre sur des sites Web ou autres applications à des fins de publicité ou de partage avec courtiers en données.

La notarisation évaluera également si les applications traitent les données utilisateur de la manière attendue par les utilisateurs. Par exemple, la notarisation cherchera à garantir que les applications obtiennent le consentement de l'utilisateur pour la collecte et le partage de données, et ne tentent pas de manipuler, tromper ou forcer les utilisateurs à consentir à l'accès d'une application à leurs données ; il examinera également si les applications fournissent une politique de confidentialité afin que les utilisateurs puissent comprendre comment leurs données sont collectées, utilisées et vendues. En raison de la sensibilité des données personnelles de santé, nous exigeons également que les applications n'utilisent ni ne divulguent les données recueillies dans le contexte de la santé, de la forme physique et de la recherche médicale à des fins de publicité, de marketing ou à d'autres fins d'exploration de données basées sur l'utilisation.

• Sécurité : pour passer la notarisation, les applications ne doivent pas risquer de causer des dommages physiques aux utilisateurs ou d'endommager leurs appareils. Par exemple, nous interdirons les applications qui incitent les clients à participer à des activités ou à utiliser leurs appareils d'une manière qui risque de nuire physiquement à autrui. La notarisation recherchera également les applications susceptibles de mettre en péril les fonctionnalités de l'appareil, notamment en vidant rapidement la batterie d'un iPhone, en générant une chaleur excessive ou en mettant inutilement à rude épreuve. ressources de l'appareil, ce qui pourrait rendre un iPhone non fonctionnel dans un situation d'urgence.

Les directives d'examen de la notarisation n'incluront pas le contenu et le commerce politiques dans les directives d'examen de l'App Store, et n'interdira donc pas ni ne vérifiera si les applications vont à l'encontre de ces politiques. Cela signifie qu'Apple ne pourra pas empêcher les applications dont le contenu n'est pas autorisé sur l'App Store, comme les applications qui distribuent de la pornographie, les applications qui encouragent la consommation de tabac ou de produits de vapotage, de drogues illégales ou de quantités excessives d'alcool, ou les applications qui contiennent du contenu piraté (ou qui volent des idées ou de la propriété intellectuelle à d'autres développeurs) — de devenir disponibles sur des marchés d'applications alternatifs. Seules les applications qui choisissent d'être distribuées sur l'App Store seront soumises au processus standard d'examen des applications, en plus de la notarisation, qui inclut l'application de ces politiques réservées à l'App Store.

Installation

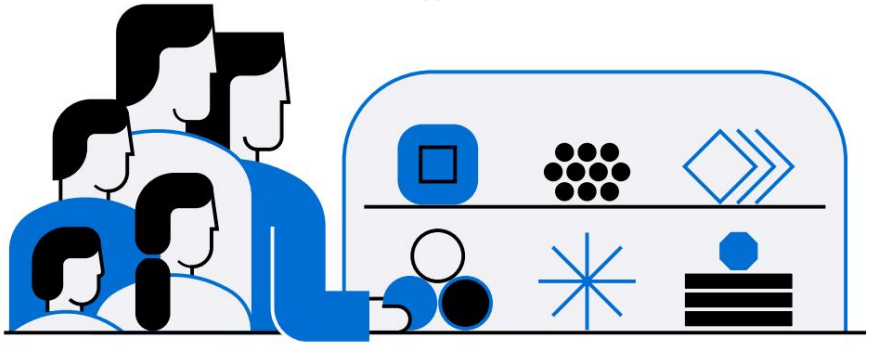
Une fois qu'une application a passé ces examens, nous la légalisons, ce qui donne au développeur la signature requise pour pouvoir distribuer cette application sur iOS. Afin de garantir que rien ne change entre la signature de l'application par Apple et le moment où l'utilisateur installe réellement l'application sur son iPhone, les applications notariées seront également soumises à une série de vérifications de base lors de l'installation. Cela permettra de garantir que l'application n'a pas été falsifiée depuis qu'elle a été notariée et que l'installation a été lancée via une source autorisée.

Même si nous savons que la notarisation sera un outil important dans notre travail pour protéger les utilisateurs contre les menaces pesant sur leur sécurité, leur vie privée et leur sûreté (servant de première ligne de défense contre les menaces potentielles et les caractéristiques malveillantes), nous savons également qu'elle a des limites. Afin d'établir des garanties continues pour nos utilisateurs même après l'installation des applications, nous avons également créé des critères de base pour les marchés d'applications alternatifs afin de garantir qu'ils disposent au moins des capacités minimales nécessaires pour assumer l'importante responsabilité de protéger les utilisateurs de manière continue . Ceux-ci inclus:

- S'engager dans une surveillance continue pour détecter et supprimer les logiciels malveillants. applications. Cette surveillance est nécessaire pour détecter les applications qui ne sont pas bloquées pendant la notarisation ou qui changent après la notarisation. Notre expérience nous a montré qu'une surveillance continue des nouvelles menaces pouvant émerger après un examen initial est impérative pour protéger la sûreté, la sécurité et la confidentialité des utilisateurs. Nous avons également constaté que la surveillance nécessite des signaux spécifiques au marché, tels que les avis des utilisateurs, les commentaires des clients et l'analyse des données du marché ; Apple n'aura pas accès à ces signaux en dehors de l'App Store. Sans une surveillance continue de chaque marché d'applications alternatif, la sécurité, la confidentialité et la sûreté des utilisateurs seront sérieusement compromises.

- Garantir que les marchés d'applications alternatifs ont la capacité de protéger les utilisateurs. Il n'est pas facile d'exploiter un marché d'applications qui facilite la distribution d'applications tierces sans mettre en danger de manière significative la sécurité, la sûreté et la confidentialité.6 Les marchés d'applications ont besoin de ressources pour s'acquitter de ces responsabilités importantes, telles que la surveillance continue des applications malveillantes. Les marchés doivent également être en mesure de fournir une assistance continue aux utilisateurs et aux développeurs afin que les développeurs puissent gérer leur entreprise et que les utilisateurs puissent compter sur les applications téléchargées via d'autres marchés d'applications pour fonctionner comme ils l'attendent et obtenir de l'aide lorsqu'ils ne le font pas. Un marché qui ne dispose pas des ressources nécessaires pour protéger les utilisateurs ou qui laisse les utilisateurs et les développeurs sans recours en cas de besoin compromettrait l'iPhone.

Ces exigences constituent le minimum nécessaire pour qu'un marché d'applications assure la sécurité et la confidentialité des données des utilisateurs et la sécurité des utilisateurs. Ils n'englobent pas l'ensemble des efforts investis par Apple pour respecter les normes élevées de sécurité, de confidentialité et de sûreté de l'App Store.

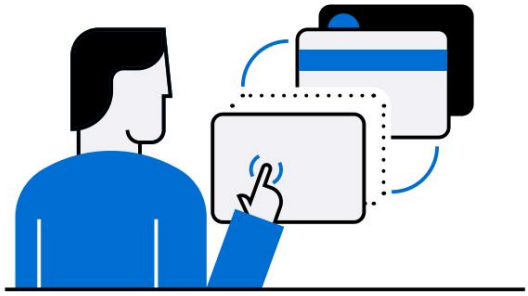


Nous avons également créé des fiches d'installation d'applications qui permettent aux utilisateurs de faire des choix éclairés concernant les applications qu'ils téléchargent. Les utilisateurs choisissent les produits Apple en partie en raison de la transparence et du contrôle que nous leur offrons, ce qui leur permet de prendre des décisions éclairées sur ce qu'ils veulent sur leurs appareils.
Ces nouvelles fiches d'installation d'applications sont un moyen essentiel pour que nous puissions poursuivre notre engagement envers la transparence que les utilisateurs attendent de nous.

Les feuilles affichent les informations examinées lors de la notarisation, telles que le nom de l'application, le nom du développeur, la description de l'application, les captures d'écran et l'âge du système, et identifient le marché à partir duquel un utilisateur télécharge l'application, le tout sous une forme claire et standardisée. Les développeurs ne pourront pas modifier le contenu de cette feuille une fois leurs applications notariées sans recommencer le processus.

Pour permettre toutes les modifications requises par le DMA, Apple a créé plus de 600 nouvelles API et outils de développement.
Nous avons intégré la sécurité, la confidentialité des données et la sécurité des utilisateurs dans ces API.
Par exemple, MarketplaceKit, le cadre qui permet des alternatives les marchés d'applications pour fonctionner sur iOS, facilite la sécurité installation d'applications distribuées à partir de places de marché alternatives : lorsque les utilisateurs téléchargent une application via une place de marché d'applications alternative, notre API permet au serveur Web de la place de marché de s'interfacer directement avec iOS, en fournissant des services d'authentification, des licences d'application et des données d'application pour créer une expérience sécurisée.
Ces API sont également conçues pour s'assurer que les installations d'applications à partir d'un marché se produisent en conséquence de l'interaction de l'utilisateur avec le marché, c'est-à-dire que l'utilisateur choisit de manière affirmative de télécharger l'application, et non par le biais d'un bug ou d'un bug. téléchargement automatisé. Et ceux-ci
Les API permettent également des mises à jour faciles de l'application, incitant les développeurs à maintenir les applications à jour.

Apple a également créé d'autres nouvelles API qui protègent les utilisateurs, comme AdAttributionKit, qui permet des publicités respectueuses de la vie privée, permettant aux annonceurs et aux développeurs d'obtenir des mesures de données publicitaires sans suivre les utilisateurs ou les appareils individuels dans les applications appartenant à d'autres sociétés. Ces nouveaux outils contribueront à garantir que les modifications que nous avons apportées pour nous conformer au DMA fonctionnent de la manière la plus transparente possible...
tout en assurant la sécurité des utilisateurs autant que possible.



Fournir aux utilisateurs un résumé rapide de ces informations permettra aux utilisateurs de savoir quelle application ils téléchargent et à quoi ressemblait l'application lorsqu'elle a été notarisée, même si d'autres marchés n'ont pas d'exigences standardisées en matière de divulgation des applications ou si l'application a changé. sa présentation après notarisation. Ces divulgations permettront aux utilisateurs de choisir facilement les applications avec lesquelles ils souhaitent interagir. Un utilisateur peut également choisir de désactiver les feuilles de n'importe quelle place de marché. Les feuilles disparaîtront automatiquement si un utilisateur définit la place de marché par défaut, car l'utilisateur a alors fait le choix de préférer cette place de marché.

Informer les utilisateurs des risques liés aux paiements

Pour prendre en charge les changements que nous avons annoncés pour nous conformer au DMA, nous introduisons également la possibilité pour les développeurs de l'App Store d'utiliser des options de paiement alternatives pour effectuer des transactions de biens et services numériques au sein de leurs applications dans l'UE. Cela ouvre de nouvelles options aux développeurs, mais cela signifie également que les utilisateurs de ces applications ne bénéficieront pas des mêmes protections et avantages sur lesquels ils comptent grâce au système de commerce privé et sécurisé d'Apple, y compris les achats intégrés (IAP), tels que l'achat facile. l'annulation d'abonnement, une page d'historique d'achat centralisée, des contrôles parentaux comme Ask to Buy ou des protections contre les tactiques prédatrices comme celles qui visent à inciter les utilisateurs à payer un montant différent de celui annoncé pour un bien numérique. Il incombera aux utilisateurs de déterminer eux-mêmes, application par application, les avantages et les protections qui pourraient leur être offerts, ainsi que la personne à contacter pour obtenir de l'aide en cas de transaction erronée, car les agents AppleCare auront des possibilités limitées (le cas échéant) capacité à les aide

Comme toujours, Apple est guidé par les valeurs de transparence et d'information des utilisateurs. Par conséquent, nous informons les utilisateurs que les protections d'Apple ne seront pas disponibles afin que l'utilisateur ait les connaissances nécessaires pour décider s'il souhaite finaliser la transaction. Avant qu'un utilisateur télécharge une application, l'App Store affichera une bannière d'information sur la page produit de l'application pour informer l'utilisateur que le développeur utilise une solution de paiement alternative, et non le système de commerce sécurisé d'Apple. Et avant qu'un utilisateur effectue une transaction en dehors du système commercial d'Apple, il verra une feuille d'information dans l'application qui lui permettra de savoir qu'il n'effectue plus de transactions avec Apple. Ces informations permettront de garantir que les utilisateurs savent qu'ils doivent être en alerte face aux développeurs qui utilisent des informations de paiement trompeuses, des prix d'éviction et des informations d'abonnement manquantes.

Sécurité, confidentialité et sûreté dès la conception

Il est important de noter que l'architecture et la conception du système Apple continuent de protéger la sécurité, la confidentialité et la sûreté des utilisateurs. Apple a placé la sécurité au cœur de ses plates-formes grâce à sa protection de sécurité puissante et multicouche. Cette conception signifie que même si l'iPhone dans l'UE n'est pas aussi sécurisé que dans le reste du monde, nous pensons qu'il reste l'option la plus sécurisée de l'UE. Au niveau de base, les fonctionnalités de sécurité clés, telles que le chiffrement matériel des appareils, ne peuvent pas être désactivées. Apple fournit également des couches de protection qui fournissent une plate-forme stable et sécurisée pour les applications. Par exemple, toutes les applications sont mises en sandbox, elles ne peuvent donc pas accéder aux fichiers stockés par d'autres applications ou apporter des modifications à l'appareil. Les fichiers et ressources système sont également protégés des applications de l'utilisateur. Si une application a besoin d'accéder à des informations autres que les siennes, elle le fait uniquement via des services explicitement fournis par iOS. Cela signifie qu'une application ne peut généralement pas affecter d'autres applications ou le système iOS, ce qui réduit le risque de logiciels malveillants affectant d'autres parties de la plateforme. Apple intègre également la signature de code, ce qui signifie que tout le code des applications tierces est lié au développeur dont l'identité réelle a été vérifiée lors de son inscription au programme pour développeurs. Au lancement, iOS garantit que le code de l'application est celui que le développeur a signé lors de la soumission de l'application.

Apple a également conçu iOS autour de la confidentialité. Par exemple, iOS exige que les utilisateurs choisissent si les applications ont accès aux données de leurs services de localisation et, si c'est le cas, si l'application peut accéder à la position précise de l'utilisateur ou seulement à une approximation générale de sa position. Les applications ne peuvent pas accéder au microphone ou à la caméra de l'iPhone sans l'autorisation de l'utilisateur. Lorsqu'une application utilise le microphone ou la caméra d'un appareil, celui-ci affiche un indicateur pour en informer l'utilisateur. Pour des raisons similaires, Apple a interdit aux applications d'accéder à la caméra si elles s'exécutent en arrière-plan, afin qu'elles ne puissent pas espionner subrepticement les utilisateurs.

Bien entendu, Apple intègre également de nombreuses autres protections, notamment la sécurité matérielle et la biométrie, telles que le silicium Apple, Secure Enclave, Face ID et Touch ID ; les fonctions matérielles et logicielles intégrées qui assurent le démarrage, la mise à jour et le fonctionnement continu en toute sécurité des systèmes d'exploitation Apple ; et les protocoles réseau qui assurent une authentification sécurisée et un cryptage des données en cours de transmission. Les appareils Apple incluent également des fonctionnalités de protection des données et de cryptage pour protéger les appareils qui ont été perdus ou volés et pour se défendre contre les personnes non autorisées qui tentent d'utiliser ou de modifier un appareil. De plus, Apple fournit des « kits » de cadre pour une gestion sécurisée et privée du domicile et de la santé des utilisateurs, auxquels les applications tierces peuvent également accéder via des API, afin que les données les plus sensibles et personnelles d'un utilisateur restent sécurisées et privées.

Ce ne sont là que quelques exemples de l'architecture système d'Apple et des protections de confidentialité dès la conception qui, avec les nouveaux changements que nous introduisons, continuent de protéger nos utilisateurs de l'UE dans ce nouveau paysage.

Préoccupations des gouvernements et des utilisateurs

Nous espérons que beaucoup accueilleront favorablement ces protections, car nous sachez qu'il y a de réelles inquiétudes sur les changements qu'Apple apporte à sa plateforme. Depuis que nous avons annoncé des modifications liées au DMA sur iOS, Safari et l'App Store dans l'UE le 25 janvier 2024, nous avons entendu des préoccupations de la part des gouvernements : y compris les agences gouvernementales des États membres de l'UE – et utilisateurs sur les risques liés à l'autorisation d'autres magasins d'applications et de processeurs de paiement alternatifs sur iOS, et demandant comment et si nous prévoyons de mettre en place des garanties contre ces risques.

Les agences gouvernementales, tant dans l'Union européenne qu'en dehors de celle-ci, ont rapidement reconnu les risques créés par ces nouvelles options de distribution et la nécessité de mesures de protection. Ces agences, notamment celles qui remplissent des fonctions essentielles telles que la défense, services bancaires et d'urgence— nous ont contactés à ce sujet de nouveaux changements, cherchant l'assurance qu'ils auront la capacité d'empêcher les employés du gouvernement de télécharger des applications sur des iPhones achetés par le gouvernement.

Plusieurs nous ont dit qu'ils prévoyaient de bloquer le chargement latéral sur chaque appareil qu'ils gèrent. Une agence gouvernementale de l'UE nous a informés qu'elle ne disposait ni du financement ni du personnel nécessaires pour examiner et approuver les applications pour ses appareils et qu'elle prévoyait donc de continuer à s'appuyer sur Apple et l'App Store, car elle nous fait confiance pour contrôler de manière exhaustive les applications.

Ces agences ont toutes reconnu que le chargement latéral (téléchargement d'applications depuis l'extérieur de l'App Store) pourrait compromettre la sécurité et mettre les données et les appareils gouvernementaux risque.

Et les utilisateurs ont envoyé Tim Cook de nombreux emails exprimant leurs craintes que ces changements ne nuisent à leur expérience sur iPhone sûr. Ces clients ont dit nous que ce qu'ils aiment et apprécient chez Apple et ses produits, c'est notre engagement à protéger leur vie privée et leur sécurité, et qu'ils craignent les risques que les nouveaux changements peuvent entraîner pour leurs propres appareils - et ceux de leurs familles.

Nous avons entendu – et anticipé – ces préoccupations. C'est pourquoi nous avons mis en place des mesures de protection et pourquoi nous travaillerons sans relâche pour innover afin de protéger nos utilisateurs dans la mesure du possible en vertu de la loi.

Cher Tim

De vrais e-mails reçus par Tim Cook concernant les changements apportés à l'iPhone dans l'Union européenne

À : Tim Cook
De : Citoyen de l'UE
Objet : Merci
Date : 27 janvier 2024

Merci de diriger une entreprise qui donne la priorité aux clients, qu'il s'agisse de leur vie privée, de leur santé ou de leurs droits humains.

En tant que citoyen de l'UE,… Je n'autoriserai pas le chargement latéral sur mes appareils

À : Tim Cook
De : Client Apple
Objet : Profondément préoccupé par la récente législation de l'UE
Date : 28 janvier 2024

Je suis un client et utilisateur satisfait d'Apple depuis plus d'une décennie. Je crois sincèrement que ce qu'Apple a créé est magique. Je ne veux pas voir le jour où je serai obligé de télécharger une boutique tierce lorsque le développeur d'une application que je souhaite utiliser choisit de contourner l'App Store et m'oblige à m'inscrire sur la leur ou à utiliser une application de paiement tierce. si ma banque décide qu'elle ne souhaite plus prendre en charge Apple Pay. Tout fonctionne actuellement comme par magie et c'est un plaisir à utiliser.

J'espère sincèrement que Apple et vous-même continuerez à défendre ce qui est juste. et continue de fournir le meilleur client expérience et que nous ne voyons jamais l'iPhone rempli d'App Store tiers comme les téléphones Samsung ou Google.

À : Tim Cook
De : Utilisateur d'iPhone dans l'UE
Objet : Préoccupations concernant la loi européenne sur les marchés numériques
Date : 27 janvier 2024

Récemment, de nombreuses discussions ont eu lieu sur l'ouverture des iPhones à des magasins d'applications alternatifs, à la suite de la loi européenne sur les marchés numériques. En tant que consommateur, cette évolution me préoccupe. J'ai choisi l'iPhone pour son engagement fort en matière de confidentialité et de sécurité, une caractéristique de la philosophie d'Apple.

Je comprends qu'en vertu de la nouvelle réglementation, je ne suis pas obligé de télécharger des applications en dehors de l'App Store. Cependant, je préférerais une option qui me permettrait d'éviter même la possibilité de rencontrer des applications provenant de sources externes, notamment en évitant les pop-ups ou les notifications à leur sujet. Essentiellement, je cherche à maintenir l'expérience utilisateur actuelle de l'iPhone, où l'App Store est la seule source d'applications.

Apple pourrait-il envisager d'introduire une fonctionnalité permettant aux utilisateurs comme moi de restreindre leurs iPhones à télécharger uniquement des applications depuis l'App Store d'Apple ? Cette option respecterait le droit du consommateur de choisir le niveau de sécurité et de confidentialité avec lequel il est à l'aise, ce qui, à mon avis, est conforme aux principes de concurrence loyale.

À : Tim Cook
De : Utilisateur Apple
Objet : Chargement latéral
Date : 16 janvier 2024

Pouvez-vous même garantir la sécurité aux personnes qui ne souhaitent pas de chargement latéral sur leurs appareils ?

Beaucoup de gens préfèrent sûrement recevoir des applications normales, comme d'habitude. Un moyen de refuser le chargement latéral et d'avoir des « applications Apple normales » lors de l'installation serait une bonne manière.

Le programme Google empêche le chargement latéral

Android autorise le chargement latéral depuis sa création, mais il semble que Google ait reconnu que cette pratique met en danger les utilisateurs hautement sécurisés.

Google a conçu son programme de protection avancée pour les utilisateurs dont « les comptes contiennent des fichiers particulièrement précieux ou des informations sensibles » et recommande fortement « des journalistes, des militants, des dirigeants d'entreprise et des personnes impliquées dans les élections » s'inscrivent au programme. L'une des principales caractéristiques du programme est qu'il empêche le chargement latéral pour aider à lutter contre les « téléchargements nuisibles ». Les inscrits au programme ne peuvent installer que des applications provenant de « magasins vérifiés, comme Google Play Store et la boutique d'applications du fabricant de votre appareil ».

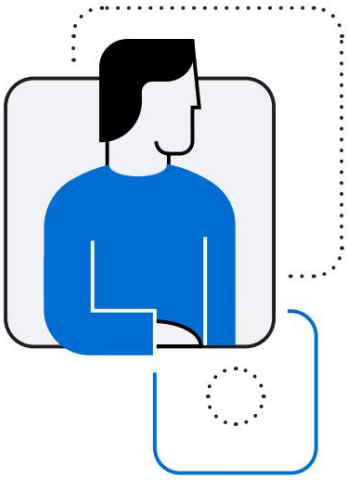
Les risques réduits (mais non éliminés) par Garanties d'Apple pour la distribution d'applications et alternatives Systèmes de paiement

Ces mesures de protection contribueront à garantir que l'expérience iPhone des utilisateurs de l'UE soit aussi sécurisée, respectueuse de la vie privée et sûre que possible, mais pas au même degré que dans le reste du monde. Cette section fournit plus de détails sur les catégories de risques que ces mesures de protection chercheront à traiter.

NOTARISATION

La notarisation vise à détecter les applications malveillantes en identifiant les menaces sérieuses pour la sécurité, la confidentialité et la sûreté des utilisateurs. Par exemple:

- Une manière courante pour les applications malveillantes de se frayer un chemin sur les appareils consiste à l'ingénierie sociale : en manipulant les utilisateurs pour qu'ils accordent l'accès à leur appareil en prétendant être quelque chose qu'ils ne sont pas, notamment en imitant des applications populaires et légitimes. La notarisation cherche à réduire cette menace en vérifiant si la façon dont une application se présente à travers ses métadonnées représente fidèlement son fonctionnement lors de l'examen. La notarisation analysera les applications dans le but d'empêcher ces types de prétendants malveillants de s'introduire sur les appareils.



À titre d'exemple, grâce à sa combinaison d'examens humains et automatisés, Apple a identifié un ensemble d'applications qui usurpaient l'identité d'une plate-forme publicitaire légitime afin de voler les informations de connexion. La notarisation recherchera les applications malveillantes comme celles-ci. L'examen humain est essentiel pour détecter ces stratagèmes.
l'examen automatisé ne peut pas vérifier les attaques conçues pour manipuler les utilisateurs.

- Les mauvais acteurs peuvent également déformer leurs intentions auprès de l'utilisateur afin de convainquez-les de donner volontairement accès aux zones protégées de leur iPhone, telles que les services de localisation, HealthKit (qui stocke les données de santé), le microphone, l'appareil photo, les contacts, les photos, etc. Les mauvais acteurs pourraient utiliser cet accès illicite pour cibler des utilisateurs avec un ransomware, où le mauvais acteur aurait accès aux fichiers d'un utilisateur et les chiffrerait, les déchiffrerait seulement après le paiement d'une rançon, ou menacerait de divulguer les fichiers publiquement à moins qu'ils ne reçoivent de l'argent.

  ce qui peut entraîner la perte de l'accès à des fichiers critiques, des dommages financiers si l'utilisateur paie la rançon, ou des dommages émotionnels et psychologiques si les notes privées, les photos et autres fichiers de l'utilisateur sont rendus publics. La notarisation, et en particulier nos évaluateurs humains, chercheront également à identifier et à bloquer les logiciels malveillants susceptibles de tenter de tromper les utilisateurs sur les raisons pour lesquelles ils demandent leur autorisation pour accéder à d'autres parties de l'iPhone – autorisation essentielle pour que l'application malveillante puisse accéder aux données au-delà de son accès étroit. bac à sable contrôlé.

- Les mauvais acteurs pourraient également utiliser cet accès frauduleux pour déployer des les logiciels espions, un genre de logiciels malveillants qui s'installent sur un appareil à l'insu de l'utilisateur final et volent des informations sensibles, notamment des contacts, des photos et des vidéos. Les logiciels espions grand public peuvent être utilisés pour violer la vie privée d'un partenaire intime, ou par des pirates informatiques cherchant à extraire des données monétisables telles que des secrets d'affaires, ou à obtenir un effet de levier sur l'utilisateur dans le cadre d'un autre stratagème criminel. Des acteurs malveillants peuvent également vendre ces données sensibles sans l'autorisation de l'utilisateur, notamment en violation des droits de l'utilisateur ou des politiques de protection de la vie privée d'Apple. La notarisation et nos évaluateurs humains rechercheront également les applications qui cachent leur véritable objectif et leurs capacités afin de déployer des logiciels espions grand public.

- Les outils de développement eux-mêmes peuvent potentiellement contenir des logiciels malveillants, qu'ils soient intentionnellement malveillants ou qu'ils soient infectés, ce qui constitue une menace pour les utilisateurs et les développeurs. Les SDK malveillants qu'un développeur inclut sciemment ou inconsciemment dans son application pourraient collecter des données de localisation et les vendre à des entités sans scrupules, collecter de manière opportuniste des données protégées pour lesquelles l'application elle-même a obtenu le consentement légitime de l'utilisateur ; ou tenter de suivre clandestinement un utilisateur sur des sites Web et des applications sans autorisation. La notarisation examinera les applications pour identifier si elles contiennent des outils de développement compromis intégrés dans leurs applications :
  comme ces SDK, dont nous savons qu'ils contiennent des logiciels malveillants, qui protègent les développeurs eux-mêmes contre les menaces d'acteurs malveillants qui pourraient proposer des logiciels infectés.
  outils de développement qui contiennent et propagent des logiciels malveillants.

En savoir plus sur les menaces liées au chargement latéral

Vous pouvez en savoir plus sur comment des acteurs malveillants peuvent essayer d'utiliser des applications téléchargées pour menacer la sécurité, la confidentialité et la sûreté des utilisateurs ; particulièrement absent des nouvelles garanties d'Apple – dans les articles de 2021 « Building a Trusted Ecosystem for Millions of Apps » : « A Threat Analysis of Sideloading » et « Le rôle important des protections de l'App Store ».

• Les applications malveillantes peuvent même causer des dommages physiques aux utilisateurs. La notarisation examinera les applications pour ces risques. Par exemple, la notarisation vérifiera si les applications encouragent à nuire aux utilisateurs ou à autrui, en détectant les « applications de défi », comme une variété d'applications créées par de mauvais acteurs en réponse à un défi en ligne dangereux qui assignait des tâches aux utilisateurs sur une période de 50 jours pour encourager les inciter à se suicider. Ces applications ont été conçues pour introduire progressivement des éléments d'automutilation, le défi final obligeant le « joueur » à se suicider. Apple a détecté et rejeté ces applications depuis iOS. La notarisation vise à continuer de garder les applications dangereuses comme celle-ci hors d'iOS.

À : Tim Cook
De : Utilisateur Apple
Objet : Déçu
Date : 15 janvier 2024

Bientôt, vous n'aurez plus rien pour vous différencier des autres.
Cette décision va affecter un grand nombre de mes amis et de ma famille qui comptent sur la capacité de l'iPhone à les protéger. de mauvais acteurs. Je suis je vais avoir du mal à justifier qu'ils dépensent de l'argent pour un iPhone maintenant…. Je ne suis pas sûr si vous lirez ceci personnellement, mais j'espère qu'Apple aura un moyen d'assurer la sécurité des gens si c'est la voie qu'ils envisagent de suivre.

EXIGENCES POUR LES MARCHÉS D'APPLICATIONS ALTERNATIVES

Les critères d'éligibilité pour l'exploitation d'un marché d'applications alternatif contribueront à empêcher d'autres types de comportements malveillants de nuire aux utilisateurs sur iOS en exigeant une surveillance continue. Même si Apple propose la plateforme informatique mobile la plus sûre et la plus sécurisée au monde – comme les experts indépendants l'ont confirmé à plusieurs reprises7 – les acteurs malveillants tenteront toujours de contourner nos protections.
Malgré des outils sophistiqués et des équipes d'experts, une surveillance persistante et continue est nécessaire pour détecter les applications malveillantes de pointe et déguisées qui ne sont pas détectées par la notarisation en premier lieu.

Nous avons également vu des applications qui peuvent passer de banales à malveillantes après avoir été examinées. Les applications qui peuvent sembler inoffensives (et donc passer la notarisation) pourraient être déclenchées par un signal externe qui active des fonctionnalités malveillantes après l'approbation, se transformant en escroqueries cryptographiques, en copieurs, en outils de blanchiment d'argent ou pire. Celles-ci sont appelées applications d'appât et de commutation. Ces applications peuvent inclure un composant qui restitue les informations à partir du serveur du développeur : afin que le cybercriminel puisse modifier l'interface utilisateur proposée à l'utilisateur après la notarisation afin que l'application devienne malveillante.

Une application peut également contenir du code obscurci qui ne semble pas immédiatement malveillant, mais qui est déclenché par une condition externe, telle que la géolocalisation, l'adresse IP (c'est-à-dire s'il n'est pas ouvert dans des emplacements ou par des appareils qui pourraient être des employés d'Apple), ou combien de temps s'est écoulé depuis la soumission (c'est-à-dire suffisamment longtemps pour que le mauvais acteur pense que l'application aura probablement terminé la notarisation). Par exemple, une application qui est apparue lors de la notarisation comme une calculatrice (et a donc réussi la notarisation) pourrait contenir un code inconnu d'Apple qui, une fois l'application passée la notarisation, l'a transformée en une application de jeu illégale.

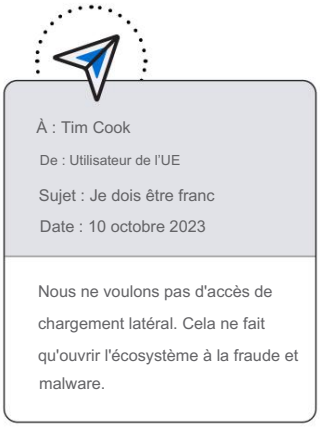
Ces applications ne peuvent être identifiées que grâce à une surveillance continue. En effet, grâce à une surveillance continue, Apple a détecté les applications suivantes qui sont devenues malveillantes après leur arrivée sur l'App Store :

- Une application qui s'est présentée comme une application fournissant des informations et des services de voyage mais, après approbation, est passée à une application de prêt illégale par un fournisseur de services non vérifié.

- Une application de chat pour adultes populaire qui était secrètement intégrée à un ransomware ; le L'application a d'abord demandé l'accès à la liste de contacts de l'utilisateur, puis, si l'utilisateur ne payait pas de rançon, l'application menaçait d'informer tous les utilisateurs de sa liste de contacts de leur utilisation de l'application de chat pour adultes.

- Une application qui se présentait comme fournissant des informations sur les animaux mais qui, après approbation, est passée à une application facilitant les jeux illégaux.

Apple effectue cet examen continu des applications distribuées via l'App Store et peut rapidement supprimer toute application malveillante que nous identifions. Certaines de ces protections seront déployées dans le nouveau paysage de l'UE. Il s'agit notamment d'outils automatisés qui tentent de détecter si les applications ont changé depuis la notarisation, par exemple en installant et en lançant périodiquement des applications comme si elles avaient été installées via un marché d'applications alternatif. Cependant, Apple utilise également d'autres signaux, notamment des signaux spécifiques au marché, tels que l'analyse des données des avis des utilisateurs et des téléchargements sur l'App Store. Nous ne pouvons pas utiliser ces signaux spécifiques au marché pour effectuer cet examen continu des applications distribuées sur d'autres marchés d'applications, ce qui nous laisse avec beaucoup moins d'outils pour comprendre quand une application est devenue malveillante. En conséquence, les marchés d'applications alternatifs doivent s'engager à surveiller les applications malveillantes afin de protéger les utilisateurs de ces menaces bien réelles.



Et sans critères garantissant que les marchés sont des entreprises légitimes disposant des ressources nécessaires pour distribuer des applications au nom des développeurs, des marchés dangereux pourraient également facilement se frayer un chemin sur les appareils des utilisateurs. Il peut s'agir de marchés frauduleux qui s'installent pendant une courte période, convainquent les utilisateurs d'acheter des applications fausses ou contrefaites, puis ferment le marché.
devient très difficile à suivre, avant que les utilisateurs ne se rendent compte qu'ils ont été victimes d'une arnaque. Cela pourrait également inclure des marchés qui ne sont pas en mesure de surveiller de manière significative les applications qu'ils proposent pour des raisons de sécurité, de confidentialité et de sûreté. Ou cela pourrait inclure des marchés qui fonctionnent sans aucun moyen financier clair, facilitant les transactions entre développeurs et utilisateurs pour ensuite fermer en raison d'un manque de ressources, laissant les utilisateurs sans aucun recours s'ils rencontrent des problèmes avec les applications qu'ils ont téléchargées sur le marché. devez demander un remboursement ou signaler une arnaque. Apple a développé des critères pour minimiser le risque de marchés d'applications aussi dangereux, tout en conservant des options pour les marchés légitimes.

À : Tim Cook
De : Client Apple
Objet : S'il vous plaît, NE PAS AUTORISER LE CHARGEMENT LATÉRAL OU APPLICATION TIERS MAGASINS sur iOS17 ou mises à jour iOS ultérieures
Date : 11 janvier 2023

J'envoie cet e-mail pour vous informer que la plupart des utilisateurs, y compris moi, à travers le monde, espèrent que vous n'autorisez pas le chargement latéral. Comme je le sais, beaucoup des utilisateurs quitteront le Écosystème iOS si Apple autorise le chargement latéral. J'ai utilisé Apple appareils pour plus de 10 ans, et je crois que App Store est le cœur d'iOS/ Appareils iPad OS. Ce sera un désastre pour iOS actuel et futur utilisateurs Si vous autorisez le chargement latéral sur iOS… Je crois que tu en sais beaucoup mieux que moi comment il est nuisible et dangereux d'autoriser le chargement latéral sur l'écosystème iOS.

FICHES D'INSTALLATION DE L'APPLICATION

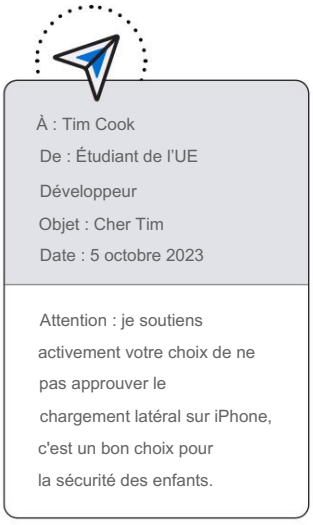
Les fiches d'installation de l'application informent également les utilisateurs et les aident à éviter les escroqueries et les attaques d'ingénierie sociale. Les acteurs malveillants tentent souvent d'inciter les utilisateurs à télécharger des programmes malveillants, notamment via des applications copiées, des escroqueries propagées via les réseaux sociaux, de fausses mises à jour du système, des méthodes de phishing par courrier électronique, de la publicité sur des sites Web d'apparence légitime et de nombreuses autres tactiques malveillantes. Par exemple, des acteurs malveillants peuvent présenter faussement des applications sur des sites Web qui dirigent ensuite les utilisateurs vers un marché alternatif, ce qui permet au développeur de donner une fausse image de son application. Étant donné que les fiches d'installation des applications aideront à informer chaque utilisateur sur ce qu'il télécharge et d'où, elles réduiront considérablement, mais n'élimineront pas, le risque que des acteurs malveillants incitent les utilisateurs à télécharger une application malveillante.
Ces fiches aideront également à se prémunir contre — mais ne peuvent pas non plus empêcher complètement — les applications qui se présentent sous une fausse image sur les marchés d'applications alternatifs.
Les marchés d'applications pourraient choisir de ne pas avoir de règles concernant la manière dont une application se commercialise sur sa plateforme. Sur ces marchés, non seulement une application pourrait se présenter comme une application totalement différente, mais elle pourrait également proposer des prix ou des abonnements différents de ceux qu'elle facturera réellement à l'utilisateur, ou prétendre faussement qu'elle dispose de fonctionnalités ou de services différents. La feuille d'installation de l'application, qui reflète les données que le développeur soumet sur son application et dont l'exactitude est ensuite vérifiée lors de la notarisation, crée un filet de sécurité afin que les utilisateurs puissent être informés de la façon dont l'application est apparue et de son objectif déclaré lorsqu'elle a été soumise. à Apple pour examen.

INFORMATIONS SUR LES OPTIONS ALTERNATIVES DE PAIEMENT

Pour les options de paiement alternatives, nos bannières d'information aideront à informer les utilisateurs des risques inévitables qui peuvent survenir, tels que les techniques prédatrices spécifiques que le système de commerce sécurisé d'Apple empêche. Notre système protège contre les acteurs malveillants qui utilisent des conceptions et des textes intentionnellement confus pour inciter les utilisateurs à acheter ou à s'abonner à des conditions qu'ils n'avaient pas prévues ou comprises, ou qui rendent presque impossible l'annulation pour l'utilisateur. En outre:

- Étant donné que toutes les applications sur iOS qui vendent des biens et services numériques au sein de l'application utilisaient jusqu'à présent le système de commerce sécurisé d'Apple, Apple a pu garantir que les utilisateurs peuvent facilement annuler chaque abonnement auquel ils souscrivent d'un simple toucher. Et grâce au cadre de développement StoreKit qui alimente l'achat intégré, Apple garantit que le prix et les conditions de l'achat intégré correspondent exactement à ceux que le développeur a configurés sur son SKU dans App Store Connect. Quelle que soit la manière dont l'application commercialise ses prix et ses conditions, l'utilisateur reçoit toujours une confirmation du prix qui lui sera facturé avant d'effectuer l'achat. Sans ce système, les applications peuvent empêcher les utilisateurs de comprendre comment annuler leurs abonnements afin de les dissuader de partir, ou utiliser des tactiques trompeuses pour les tromper.

à s'abonner à des conditions ou à des prix que l'utilisateur n'a pas compris au départ, par exemple en déformant la durée d'un essai gratuit, ou la fréquence ou le montant qu'un utilisateur paiera pour l'abonnement.8

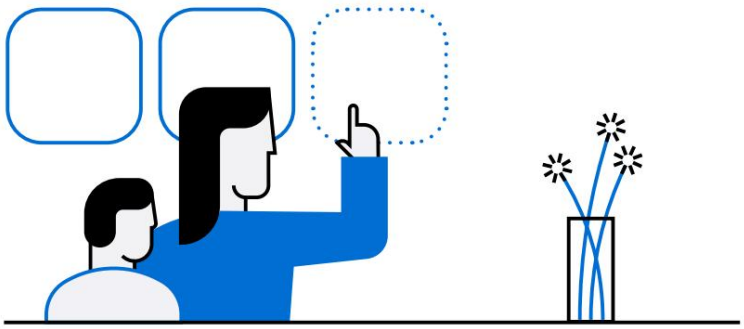


- Le système de commerce sécurisé de l'App Store empêche le chargement des applications. plus pour un bien numérique que ce qu'ils divulguent. Lorsque l'application est soumise à Apple en vue d'une éventuelle inclusion dans l'App Store, elle doit inclure le prix de ses biens et services numériques. Apple peut vérifier si cette application facture réellement le montant annoncé à l'utilisateur et peut vérifier si une application surcharge considérablement les biens ou services numériques fournis. Nous avons pris des mesures contre des centaines d'applications au cours de la dernière année en raison de leurs prix manipulateurs. Dans le cadre du flux de paiement standard et cohérent pour les biens et services numériques utilisant l'achat intégré, les API du système de commerce d'Apple garantissent également que l'application affiche le prix qu'elle a soumis à Apple à l'utilisateur (ainsi que d'autres informations sur le produit soumises et les achats importants). conditions) avant que l'utilisateur finalise l'achat, afin que l'utilisateur sache combien il lui sera facturé, que l'application lui ait divulgué ou non le montant réel. Sans ce système sur lequel les utilisateurs se sont appuyés, l'utilisateur n'aura peut-être pas l'assurance que le prix commercialisé par le développeur est une représentation précise de ce qu'il paiera finalement.

- Apple protège davantage les enfants et les familles grâce à des services comme Ask to Buy, qui exigent l'approbation parentale sur chaque article que leurs enfants souhaitent acheter ou télécharger sur iPhone, afin que les parents puissent être sûrs que les fraudeurs ne ciblent pas leurs enfants.

- Les mesures antifraude d'Apple protègent les utilisateurs contre les développeurs frauduleux, mais elles protègent également les développeurs contre les utilisateurs frauduleux (tels que ceux qui effectuent des transactions avec des cartes de crédit volées), notamment grâce à l'analyse par Apple des données de son système de paiement pour identifier les tendances et les évolutions, ce qui permet à Apple pour éradiquer les escroqueries et les individus sans scrupules.

- Le système de commerce de l'App Store peut également contribuer à garantir que les applications tiennent leurs promesses. Lorsqu'un utilisateur effectue un achat via le système Apple, cette transaction est inscrite dans l'historique des achats de l'utilisateur. Si l'application ne fournit pas de biens ou de services numériques après le paiement de l'utilisateur, Apple peut utiliser la transaction



Cher Tim

De vrais e-mails reçus par Tim Cook concernant les changements apportés à l'iPhone dans l'Union européenne

À : Tim Cook
De : Utilisateur Apple
Sujet : Pas d'Android
Date : 21 avril 2023

Nous sommes très satisfaits d'iOS car ce n'est pas comme Android, il a une haute sécurité, il a une interface conviviale et il ne ralentit jamais, mais nous avons entendu des sources dire que le chargement latéral est possible dans iOS 17 et qu'il peut
être téléchargé à partir de magasins autres que le Magasin d'applications. Il peut également être téléchargé. S'il vous plaît, arrêtez de faire ça. Nous voulons simplement télécharger depuis l'App Store et assurer notre sécurité. Veuillez ne pas activer le chargement latéral. Nous voulons qu'iOS soit comme l'ancien, avec des règles strictes et une sécurité extrêmement élevée.

À : Tim Cook
De : Utilisateur Apple de l'UE
Objet : D'un utilisateur Apple concerné et citoyen de l'UE
Date : 24 octobre 2023

Je me sens de plus en plus préoccupé et effrayé par ma vie privée numérique et ma sécurité en ligne dans l'UE.
En tant que citoyen de l'UE et utilisateur Apple, j'ai toujours pensé avoir trouvé l'équilibre parfait entre la protection réglementaire (comme le RGPD) et les fonctionnalités de sécurité d'Apple (comme la transparence du suivi des applications et l'App Store). Cependant, récemment... cela a changé.

Moi, ma famille, mes amis et mes collègues sommes des utilisateurs Apple et avons spécifiquement choisi l'écosystème Apple pour notre travail et notre temps libre en raison de la façon dont les produits et logiciels sont conçus pour être privés et sécurisés. Sans oublier bien sûr les dispositifs de sécurité introduits au fil des années.
C'est une idée effrayante, mais il semble qu'une nouvelle réglementation de la Commission européenne compromettrait bon nombre de ces fonctionnalités de sûreté et de sécurité sur lesquelles je compte actuellement.

À : Tim Cook
De : Utilisateur d'iPhone dans l'UE
Objet : Chargement latéral de l'UE
Date : 25 janvier 2024

J'espère vraiment que vous m'offrirez, en tant que client européen, la possibilité de ne pas utiliser de chargeurs latéraux. Je veux m'appuyer sur l'App Store éprouvé et non sur des bêtises…

À : Tim Cook
De : Utilisateur Apple de l'UE
Objet : Préoccupations et suggestions concernant
Le mandat de chargement latéral de l'UE
Date : 26 janvier 2024

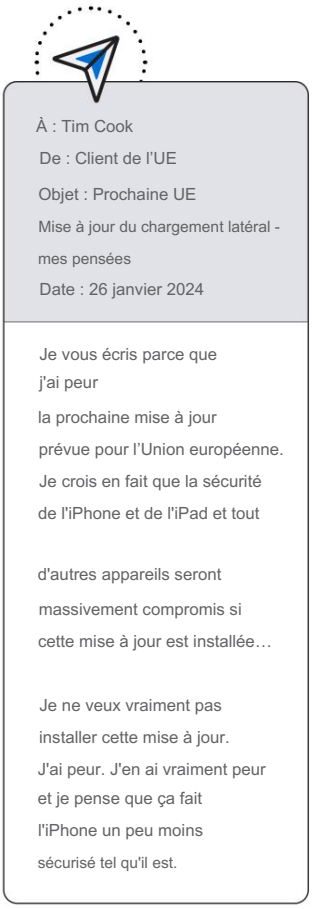
Je vous écris pour exprimer mes inquiétudes concernant la récente exigence imposée par le Parlement européen
L'Union (UE) demande à Apple d'autoriser le chargement latéral sur iOS dispositifs. Je comprends que cette décision a été
faite dans l'intérêt de promouvoir la concurrence et le choix des consommateurs, mais je crois que cela soulève d'importantes considérations en matière de confidentialité et de sécurité.

... L'App Store est une source fiable pour les applications iOS, offrant un niveau de confiance et de sécurité crucial à l'ère numérique d'aujourd'hui.
Personnellement, je me suis toujours senti en sécurité en sachant que les applications que je télécharge depuis l'App Store sont soumises à des processus de contrôle stricts pour protéger mon appareil et mes informations personnelles.

Cependant, avec l'introduction du chargement latéral, il existe un risque potentiel que les utilisateurs installent sans le savoir des applications malveillantes ou non vérifiées à partir de sources externes, compromettant ainsi la sécurité globale des appareils iOS. Ce changement pourrait exposer les utilisateurs à diverses menaces de cybersécurité, et je suis préoccupé par les conséquences potentielles du chargement latéral sur iOS.

historique pour valider si la transaction a eu lieu et prendre des mesures contre les applications qui ne remplissent pas leur part de la transaction. Sans cet historique, Apple ne pourra pas aider les utilisateurs si les applications renoncent à une transaction.

- Apple dispose également de milliers d'agents AppleCare que les utilisateurs peuvent appeler. assistance pour les remboursements ou autre support client. Ces agents ne seront pas en mesure de fournir une assistance pour les achats effectués via un paiement alternatif systèmes.



Les utilisateurs en sont venus à compter sur les avantages et les protections offerts par le système de commerce sécurisé et privé d'Apple après l'avoir utilisé pour acheter des biens et services numériques pendant près de deux décennies. Les bannières d'information informeront les utilisateurs qu'ils doivent être à l'affût des techniques trompeuses contre lesquelles, jusqu'à présent, Apple les a protégés.

Le rôle des marchés d'applications alternatifs et Processeurs de paiement alternatifs en outre Réduire les risques

Dans les mois à venir, de nombreux utilisateurs de l'UE pourront télécharger des applications sur iOS à partir de marchés d'applications alternatifs et effectuer des paiements à l'aide de processeurs de paiement alternatifs. Cela marquera un changement radical par rapport à la façon dont les choses ont toujours fonctionné sur iPhone. Étant donné que les utilisateurs font confiance à Apple pour protéger leurs appareils, ils n'ont pas eu à se soucier de savoir si leur source d'applications tierces ou leur système de paiement intégré constituait une menace pour eux. Les utilisateurs ne pourront plus assumer cette protection.

Apple prend des mesures substantielles et significatives pour protéger les utilisateurs de l'UE dans le nouveau monde de distribution alternative et de paiements alternatifs ouvert par le DMA. Mais la portée de ces mesures est nécessairement limitée par la loi. Apple doit donc transférer la responsabilité des fonctions de protection des utilisateurs qu'elle n'est plus autorisée à exercer seule aux marchés d'applications alternatifs et aux processeurs de paiement eux-mêmes.

Cela signifie que les marchés d'applications alternatifs et les processeurs de paiement alternatifs ont probablement un rôle inévitable à jouer dans la protection des utilisateurs, même si ceux-ci ne souhaitent pas les utiliser. De nombreux utilisateurs nous ont contactés pour nous demander s'ils pouvaient simplement se désinscrire des modifications annoncées par Apple pour se conformer au DMA. Et certains commentateurs ont fait valoir que les utilisateurs n'ont aucune obligation de profiter des nouvelles options qu'Apple propose dans l'UE s'ils ne le souhaitent pas ; au lieu de cela, disent ces commentateurs, les utilisateurs peuvent simplement continuer à télécharger des applications exclusivement à partir de l'App Store.

À : Tim Cook
De : Utilisateur d'iPhone dans l'UE
Objet : Client européen

Zone économique
Date : 23 janvier 2024

C'était mon libre choix
d'acheter un iPhone Apple,
et je l'ai fait
parce que je me sens plus
sécurisé avec iOS que
avec un appareil fonctionnant
sous Android. Maintenant, ma
vraie question : ne serait-il
pas possible pour moi, en tant que
un client à avoir
la liberté de choisir
si j'installe l'iOS
version destinée au
marché européen à l'avenir,
ou si je peux
installer la version iOS
utilisé dans le reste du
monde?

Une application Android utilisée
Phishing par SMS pour
inciter les gens à télécharger
une application se faisant passer
pour une application de
service postal légitime, mais qui a
ensuite volé des informations sensibles à
le dispositif. Il a répété cette
arnaque en se faisant passer
pour des services de messagerie
dans plusieurs pays différents.
Comme il exécutait des
applications légèrement
différentes pour chaque arnaque,
il serait plus difficile pour
chaque marché de détecter ce modèle.10

Les utilisateurs n'auront probablement pas d'autre choix que de créer plusieurs comptes sur chaque marché d'applications et option de paiement alternative qu'ils utilisent. Non seulement cela sera gênant pour l'utilisateur et dégradera son expérience, mais cela augmentera également le risque de vol de ses données. Plus il y a de comptes

L'utilisateur dispose, plus ses informations personnelles et financières sont stockées dans des endroits différents, ce qui augmente le risque que ces données soient exposées lors d'une violation de données, ce qui est de plus en plus probable.9 En outre, les utilisateurs pourraient être encore plus conditionnés à partager sans discernement leurs informations personnelles et financières. informations et confiance aux distributeurs d'applications, même si les distributeurs ne sont pas légitimes. Un mauvais acteur pourrait tromper un utilisateur en se faisant passer pour un marché d'applications légitime sur un site Web hors iOS, incitant l'utilisateur à fournir un paiement ou ses informations, après quoi l'utilisateur découvrirait que le mauvais acteur n'a jamais eu de marché du tout.

Mais dans la pratique, les utilisateurs de l'UE perdront le choix de rester uniquement sur l'App Store et de conserver toutes les protections de pointe d'Apple, même si c'est ce qu'ils préféreraient. Certains développeurs choisiront de rendre leurs applications exclusivement disponibles sur des marchés d'applications alternatifs. Il peut s'agir d'applications dont les utilisateurs ont besoin au travail ou à l'école, ou dont ils ont besoin pour rester en contact avec leur famille et leurs amis – des applications que les utilisateurs doivent télécharger, même s'ils préfèrent ne pas utiliser d'autres marchés d'applications. En fin de compte, les développeurs contrôleront où un grand nombre d'utilisateurs de l'UE doivent se rendre pour obtenir les applications dont ils ont besoin, que les utilisateurs soient ou non satisfaits des protections fournies par ces magasins. Malgré tous nos efforts, de nombreux utilisateurs peuvent ne pas remarquer ou comprendre que les développeurs leur demandent de télécharger des applications à partir d'un marché d'applications alternatif, malgré la préférence des utilisateurs de ne pas effectuer de transactions avec ce marché.

DÉCISIONS POUR LES MARCHÉS ALTERNATIFS ET LES PROCESSEURS DE PAIEMENT

Dans l'UE, la sécurité et la protection de la vie privée de chaque utilisateur dépendront en partie de deux questions. Premièrement, les marchés alternatifs et les processeurs de paiement sont-ils capables de protéger les utilisateurs ? Et deuxièmement, sont-ils intéressés à le faire ?
Les mesures mises en œuvre par Apple établiront une base de référence importante, mais cela ne signifie pas qu'elles soient suffisantes à elles seules. L'expérience des utilisateurs variera considérablement en fonction de la manière dont chaque marché et fournisseur de paiement choisit de mener ses activités. Cela ouvre des opportunités de différenciation et, tout comme le voulait le DMA, Apple a l'intention de rivaliser vigoureusement pour garantir que l'App Store reste l'option la plus sûre, la plus sécurisée et la plus respectueuse de la vie privée pour les consommateurs. Mais cela crée également des lacunes potentielles.

Magasin d'applications

Signaux

150 millions

transactions chacune

journée comprenant tous les

téléchargements

d'applications gratuites et payantes et

achats intégrés

3,12 millions de

notes et d'avis chaque

jour

Il s'agit notamment des

applications décrites à la

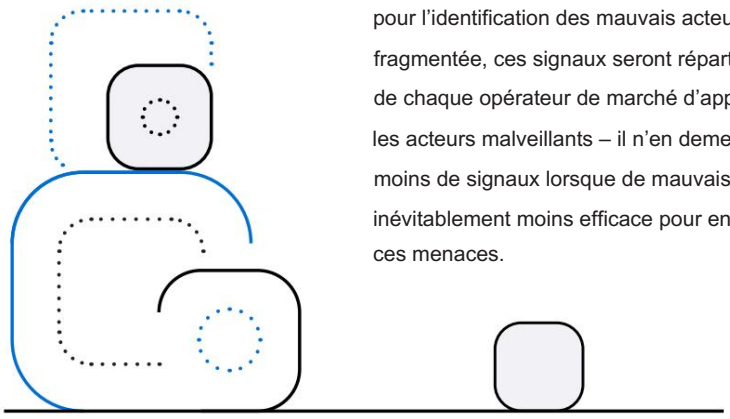
page 20 qui se sont transformées en un

application de prêt non vérifiée,

attaque de ransomware de chat pour

adultes, l'application de jeu illégale

qu'Apple a capturée.



Gérer l'App Store pendant près de deux décennies a été une entreprise énorme. Nous travaillons constamment pour trouver et arrêter les mauvais acteurs et leurs applications malveillantes en constante évolution. En plus des milliers d'ingénieurs qui créent le matériel et les logiciels destinés à empêcher les acteurs malveillants de nuire aux utilisateurs, des centaines d'employés Apple à temps plein participent à App Review, examinant les applications dans plus de 80 langues sur trois fuseaux horaires. Chaque année, nous examinons plus de 6 millions de candidatures soumises. Au cours de la dernière année complète pour laquelle les données sont disponibles, Apple a approuvé près de 4,5 millions d'applications et en a rejeté 1,6 million d'autres, la plupart parce qu'elles ne fonctionnaient pas correctement sur l'appareil et d'autres parce qu'elles violaient nos règles de sécurité et de confidentialité. Cette persistance est l'une des principales raisons pour lesquelles iOS est resté la plate-forme informatique mobile la plus sûre au monde depuis son lancement et pourquoi la plupart des acteurs malveillants ont conclu qu'essayer d'infecter iOS avec des logiciels malveillants n'est pas un investissement rentable en termes de temps, d'énergie et de ressources. .

Même avec notre expérience et nos évaluateurs humains 24 heures sur 24, nous avons retiré plus de 185 000 applications de l'App Store chaque année, car il s'est avéré plus tard qu'elles violaient les directives d'Apple. Pour rechercher et supprimer ces applications, Apple surveille attentivement l'App Store lui-même, où chaque jour plus de 150 millions de transactions ont lieu et plus de 3,1 millions de notes et d'avis sont soumis, afin d'identifier les applications problématiques. Apple prend en compte divers indicateurs dans son suivi. Il s'agit notamment des avis des utilisateurs, des rapports via notre outil Signaler un problème, des commentaires adressés aux milliers d'agents AppleCare qui assistent les utilisateurs et des modèles suspects dans les données, comme une activité inhabituelle dans les avis, des pics soudains du nombre de téléchargements ou des comportements d'achat inhabituels. Ce n'est qu'en prêtant une attention particulière à ces signaux que l'équipe d'Apple pourra éliminer les mauvais acteurs.

Les opérateurs de marchés d'applications alternatifs devront désormais entreprendre une surveillance continue nécessaire pour protéger les utilisateurs de l'UE contre les appâts et autres applications malveillantes en dehors de l'App Store.

Même si les marchés d'applications alternatifs consacrent des ressources importantes à ce travail de surveillance, il sera plus difficile d'identifier ces applications malveillantes qu'avant le DMA. Jusqu'à présent, tous ces signaux de fiabilité des applications et des développeurs pouvaient être trouvés et analysés en un seul endroit : l'App Store, créant ainsi un riche ensemble de données pour l'identification des mauvais acteurs. Mais comme la distribution des applications sera désormais fragmentée, ces signaux seront répartis sur plusieurs marchés. Quelle que soit la responsabilité de chaque opérateur de marché d'applications – et Apple espère que chacun surveille avec diligence les acteurs malveillants – il n'en demeure pas moins que tout le monde (Apple inclus) recevra moins de signaux lorsque de mauvais acteurs frappent. Cela signifie que chaque marché sera inévitablement moins efficace pour enraciner ces menaces.

À : Tim Cook
De : Utilisateur iPhone
Objet : Gardez l'iOS d'Apple fermé s'il vous plaît
Date : 27 janvier 2024

Si je voulais un système d'exploitation open source comme Google ou Samsung j'aurais acheté eux. Le principal - et Je ne peux pas le dire assez fort, la principale raison pour laquelle j'achète et possède un téléphone Apple est parce que vous sont un iOS fermé et le iOS est plus sécurisé que Android. Mais si vous voulez ouvrir les portes et ne plus être aussi en sécurité, autant changer. Veuillez garder iOS fermé, s'il vous plaît.

Apple se préoccupe depuis longtemps de protéger les développeurs et l'écosystème d'applications contre les applications piratées contraires à l'éthique et malveillantes. Ces applications dites « crackées », dont certaines sont des applications payantes qui ont été modifié pour être disponible pour gratuitement, et dont certains ont eu leur code réécrit pour inclure des modifications non intentionnelles par leurs créateurs – non seulement volent les développeurs qui travaillent dur et violent leurs droits, mais présentent également de graves risques pour les utilisateurs. Ces applications piratées sont souvent un vecteur de malware.

Dans les semaines qui ont suivi notre annonce des changements requis par le DMA, nous avons travaillé avec un certain nombre de développeurs intéressés par la création de marchés d'applications alternatifs. Nous sommes ravis de voir ce qu'ils construisent. Mais nous avons également appris des développeurs de mauvaise foi qui semblent intéressés par ces changements uniquement pour pouvoir créer des marchés qui volent la propriété intellectuelle d'autres développeurs et distribuent des applications piratées. Un développeur a en fait programmé une réunion avec Apple pour nous poser des questions sur les modifications que nous apportons en réponse au DMA, ce à quoi nous avons répondu de bonne foi, pour découvrir plus tard que le développeur était associé à un célèbre distributeur de logiciels piratés, et qu'ils avaient illégalement enregistré la conversation et l'avaient mise en ligne. Malheureusement, leurs questions semblent avoir été destinées à rechercher les meilleurs moyens de tirer parti des changements à venir d'Apple dans l'UE afin de créer un marché officiel pour les applications piratées sur iOS.

Au cours des quinze dernières années, nous avons consacré beaucoup de temps et d'ingénierie à combattre de mauvais acteurs comme ceux-ci, qui ont essayé d'exploiter toutes les opportunités qu'ils pouvaient trouver pour voler et distribuer les droits de nos développeurs. PI. Mais la notarisation ne vérifiera pas voir si les applications sur un marché d'applications alternatif portent atteinte à la propriété intellectuelle d'autrui, ce qui signifie qu'il sera beaucoup plus difficile de détecter et d'empêcher les distributeurs pirates de créer des marchés qui vérifier les violations de propriété intellectuelle dans le nom seulement. Ces distributeurs de mauvaise foi ont été parmi les plus bruyants des voix réclament une distribution alternative justement pour cette raison. En fait, après avoir contacté le développeur qui a enregistré illégalement sa conversation avec Apple, le développeur a fait valoir que le DMA interdit à Apple de prendre des mesures à son encontre pour empêcher sa distribution d'applications piratées sur iOS.

DÉCISIONS SUR LE CONTENU ET LES RÈGLES DU MODÈLE ÉCONOMIQUE

Chaque marché d'applications alternatif développera ses propres normes de marché en matière de contenu, de modèles commerciaux, etc., et certains contenus et modèles commerciaux contre lesquels Apple a toujours protégé les utilisateurs deviendront disponibles sur iPhone. C'est ce que voulait le DMA : les places de marché pourront proposer des applications qu'Apple n'aurait pas autorisées sur l'App Store. Par exemple, aucune des nouvelles protections des utilisateurs d'Apple n'évaluera si les applications contiennent du contenu pour adultes, si les applications de jeux d'argent ou d'échange de crypto-monnaie disposent des licences requises, ou si les applications avec du contenu généré par les utilisateurs ont des politiques de modération du contenu. Nous n'examinerons pas si les applications encouragent l'utilisation imprudente des armes ou si elles cherchent à profiter de crises nationales et mondiales comme les épidémies. Chaque marché d'applications devra décider s'il autorisera ce type de contenu et d'entreprises sur ses marchés, et combien investir dans l'application de ses règles pour garantir que les applications qui les violent restent en dehors de leurs plateformes.

DÉCISIONS SUR LES PROTECTIONS DES UTILISATEURS ET DE LEURS ENFANTS

Les marchés d'applications alternatifs devront également décider quelles protections offrir aux utilisateurs de leurs plateformes, en particulier aux parents et aux enfants. Par exemple, Ask to Buy empêche les enfants d'acheter ou de télécharger des articles sur leur iPhone sans l'autorisation parentale, et Apple affiche bien en évidence la tranche d'âge d'une application sur sa page de téléchargement de l'App Store. L'App Store exige également que les développeurs fournissent des étiquettes nutritionnelles de confidentialité sur leurs listes d'applications, qui expliquent à l'utilisateur

[redacted]

Sur les appareils Android, de nombreuses applications et jeux pornographiques différents peuvent être téléchargés, y compris des marchés d'applications spécifiquement destinés au contenu pour adultes.

[redacted]

Apple a supprimé les applications de l'App Store, car elles étaient principalement utilisées pour faciliter la cyberintimidation anonyme. L'une de ces applications était utilisée pour envoyer des messages anonymes à des enfants d'âge scolaire leur disant qu'ils espéraient se suicider.11

[redacted]

Apple a identifié lors de l'examen des applications des applications qui semblent à première vue inoffensives mais contiennent signaux dans leurs métadonnées indiquant une intention néfaste, comme celle d'un application qui se présentait initialement comme un programme linguistique, mais contenait des signale qu'il envisageait de se transformer en un salon de jeu censuré après avoir accédé à l'App Store. Apple a trouvé et rejeté cette application particulière.

[redacted]

Apple exige que les échanges de crypto-monnaie sur l'App Store soient correctement agréés partout où ils exercent leurs activités. Il rejette régulièrement les applications qui usurpent l'identité d'échanges de crypto-monnaie mais ont plutôt l'intention de frauder.

utilisateurs, ou qui tentent de fonctionner comme des échanges sans licence en soumettant l'application sous le couvert d'une application légitime.

[redacted]

De nombreuses applications de jeux populaires destinées aux enfants intègrent des achats intégrés, notamment des monnaie, power-ups, coffres à butin et bien plus encore. Sans fonctionnalités comme Ask Pour les acheter, les enfants peuvent dépenser des centaines de dollars pour ces produits achats sans qu'un parent ne s'en aperçoive. Par exemple, l'année dernière, la Commission fédérale du commerce des États-Unis a ordonné un développeur de jeux « va payer 245 millions de dollars aux consommateurs » pour régler les accusations selon lesquelles l'entreprise aurait utilisé des modèles sombres pour inciter les joueurs à faire des achats non désirés et laisser les enfants accumuler des frais non autorisés sans aucune implication parentale. »12

[redacted]

Apple n'autorise pas les applications visant à tirer profit des crises nationales, comme la pandémie de COVID-19— sur l'App Store. Il a supprimé une application qui faisait la promotion de soirées privées pendant la pandémie malgré les ordres de rester à la maison, et a exigé que les applications de recherche de contacts cessent d'utiliser leur fonction de santé publique pour vendre des publicités.

Des applications comme celles-ci pourraient être autorisées sur d'autres marchés d'applications.13

comment une application collectera leurs données et les suivra avant que l'utilisateur ne télécharge l'application sur son appareil. Aucune de ces fonctionnalités n'est obligatoire pour les marchés d'applications alternatifs. Les marchés peuvent choisir d'offrir des protections similaires, ou bien de ne pas le faire.

L'engagement d'Apple à protéger la confidentialité des utilisateurs signifie que sur sa politique de confidentialité Les étiquettes nutritionnelles, une application doit déclarer quelles données l'application collecte et établit un lien vers un utilisateur. Les marchés d'applications existants sur d'autres plateformes n'exigent pas ce type de divulgation claire du suivi.

Même si nous espérons que les marchés d'applications alternatifs investiront de manière significative dans la protection de la sécurité et de la confidentialité des utilisateurs, nous ne pouvons pas le garantir. Leurs modèles commerciaux peuvent offrir diverses incitations pour créer des protections pour les utilisateurs. Par exemple, les marchés d'applications alternatifs dont les modèles économiques sont basés sur la collecte et la vente de données utilisateur seraient incités commercialement à ne pas proposer de fonctionnalités telles que Étiquettes nutritionnelles de confidentialité, qui facilitent le consentement éclairé des utilisateurs à la collecte et à l'utilisation de leurs données. Cela laisserait les utilisateurs de ce marché moins informés des options qui s'offrent à eux pour protéger la confidentialité de leurs données. Ces marchés d'applications ne seraient pas non plus incités à continuer d'investir dans de nouvelles façons innovantes de protéger la vie privée des utilisateurs, comme Apple continue de le faire pour les utilisateurs de l'App Store.

DÉCISIONS SUR LE SOUTIEN AUX PAIEMENTS POUR LES CLIENTS

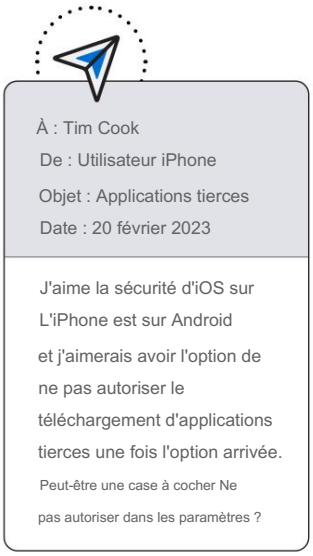
En 2021, le gouvernement fédéral américain La Commission du commerce condamnée à une amende un outil d'apprentissage en ligne basé sur l'adhésion 10 $ millions de dollars parce que cela n'a pas fonctionné correctement révéler que les consommateurs serait facturé indéfiniment après la fin d'une période d'essai gratuite initiale, et il fallait un processus long et déroutant pour annuler l'abonnement.

Aujourd'hui, grâce aux outils d'abonnement d'Apple, un utilisateur peut annuler un abonnement comme ça en un clic, mais d'autres marchés pourraient ne pas fournir ce service.14

Il appartiendra à chaque marché individuel, développeur d'applications et/ou processeur de paiement alternatif de fournir une assistance aux paiements aux utilisateurs. Certaines peuvent offrir une excellente protection aux consommateurs, mais d'autres non. Cependant, dans tous ces cas, Apple ne sera plus en mesure d'aider les utilisateurs qui tombent dans le piège des abonnements ou qui sont amenés à effectuer un achat involontaire : les nombreux agents AppleCare d'Apple ne seront pas en mesure de fournir une assistance pour un système de paiement qu'Apple ne contrôle pas. . Ces choix introduiront une énorme complexité pour les utilisateurs qui pensent, à juste titre, qu'ils peuvent continuer à contacter Apple pour obtenir de l'aide après avoir acheté un bien ou un service numérique via une application disponible sur l'App Store.
mais constatez au contraire qu'Apple ne peut pas les aider car le développeur a choisi une solution de paiement différente. C'est pourquoi il est si important que les utilisateurs disposent d'un maximum d'informations avant de s'engager dans une telle transaction. Apple a un rôle à jouer en aidant les utilisateurs à effectuer des transactions via des options de paiement alternatives, notamment via les informations qu'elle fournit, mais les tiers mettant en œuvre ces solutions le font également : s'ils ne le font pas, les utilisateurs en souffriront.

DE NOUVELLES INCITATIONS POUR LES CYBERCRIMINELS

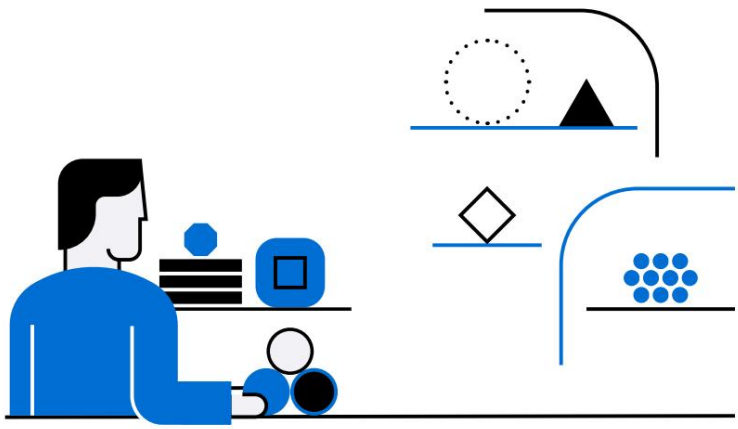
Si ces changements ouvrent de nouvelles opportunités de concurrence, ils créeront aussi inévitablement de nouveaux marchés lucratifs pour les acteurs malveillants. Les acteurs malveillants ont longtemps eu du mal à accéder à l'iPhone en raison de ses meilleures protections en matière de sécurité et de confidentialité. L'approche intégrée d'Apple en matière de sécurité des plates-formes a mis l'écosystème iOS hors de portée des logiciels malveillants courants. En fait, les cybercriminels n'ont jamais réussi à piéger un seul grand consommateur.



attaque de malware sur iOS. Ils ont appris que l'approche intégrée d'Apple en matière de sécurité des plateformes fait de la plupart des tentatives d'infection par des logiciels malveillants une cause perdue. La production et la distribution de logiciels malveillants nécessitent des ressources importantes, et les solides défenses de l'iPhone ont empêché ces efforts d'obtenir un retour sur investissement significatif, réduisant encore davantage l'attrait de l'appareil en tant que produit. cible.

De la même manière, la surveillance proactive et continue d'Apple a rendu plus difficile l'implantation d'escroqueries continues sur iOS. Par exemple, nous prenons des mesures pour empêcher que des applications par ailleurs légitimes soient utilisées pour faciliter des escroqueries, comme l'escroquerie de « boucherie de porcs » qui incite les utilisateurs à déposer des fonds à investir sur un compte de courtage frauduleux sur une application d'investissement légitime. Lorsque nous prenons connaissance de telles escroqueries, nous contactons le développeur de l'application légitime pour empêcher les escroqueries de proliférer sur cette application. Nos actions ont rendu les applications iOS moins attractives des arnaques comme celles-ci également.

Les nouveaux changements apportés à l'iPhone dans l'UE modifieront le calcul des mauvais acteurs qui, auparavant, ne cherchaient pas de moyens d'exploiter iOS et ses utilisateurs en raison des rendements relativement faibles dont ils disposaient. Outre de nouvelles options pour les développeurs, ces changements créent de nouveaux points d'entrée (et des vulnérabilités potentielles) pour les escrocs et les cybercriminels. Ces acteurs de plus en plus créatifs constituent des menaces sophistiquées. Beaucoup s'appuient sur l'ingénierie sociale pour inciter les utilisateurs à divulguer leurs informations les plus personnelles et les plus sensibles par des moyens qui pourraient plaire à n'importe qui, même à l'utilisateur le plus averti. Avec un accès plus facile aux utilisateurs d'iPhone via des canaux de téléchargement d'applications alternatifs, le retour sur investissement augmente, ce qui rend les tentatives de ciblage de l'iPhone relativement plus lucratives dans l'ensemble. Pour toutes les raisons que nous avons décrites, y compris l'incapacité d'Apple à détecter les surfacturations frauduleuses en dehors de son système commercial et la fragmentation des signaux du marché, il faudra plus de temps pour attraper les fraudeurs ou autres mauvais acteurs - et nous ne pouvons pas garantir que les marchés d'applications alternatifs prendront plus de temps. la même action rapide contre eux que nous le ferions. Cela laisse les utilisateurs exposés plus longtemps à des acteurs potentiellement malveillants et peut donner à ces acteurs malveillants plus d'espace pour trouver des moyens créatifs de tromper les utilisateurs.



Cela incite les mauvais acteurs à construire de nouveaux projets et à inventer de nouveaux malware qui cible les utilisateurs iOS. Ces acteurs malveillants auront la possibilité de déplacer leurs applications d'un marché d'applications alternatif à un autre, créant ainsi des opportunités d'utiliser la même arnaque encore et encore sur un marché après l'autre.
ou même potentiellement sur la même place de marché avec des changements mineurs. Tout cela augmente la probabilité que les mauvais acteurs voient un retour sur investissement sur iOS, encourageant encore plus de développements malveillants. Le plus inquiétant peut-être est que ce nouveau niveau d'investissement criminel dans la création d'outils, de services et d'infrastructures destinés à cibler les utilisateurs d'iOS risque de se répercuter et de réduire le coût des attaques, même pour les utilisateurs qui n'utilisent que l'App Store.

Soyons clairs : Apple intègre plusieurs couches de sécurité dans ses appareils et systèmes. Nous ferons tout notre possible pour réduire ces risques. Mais pour toutes les raisons évoquées, les risques vont augmenter.

Apple s'engage à offrir une expérience utilisateur sécurisée, respectueuse de la vie privée et sécurisée sur iPhone. Cet engagement se poursuit même si nous avons mis en place des changements pour nous conformer au DMA, de sorte que nous faisons tout notre possible pour protéger les utilisateurs dans l'UE. Même si l'expérience européenne ne sera pas la même que celle que nous sommes en mesure de proposer ailleurs, ces nouveaux outils et processus nous aideront à lutter contre les risques que ces changements créent.

La notarisation aidera à empêcher les utilisateurs d'être exposés à des applications malveillantes contenant des logiciels malveillants tels que des ransomwares ou des logiciels espions grand public, qui incitent les utilisateurs à exposer plus d'informations qu'ils ne le souhaitent ou qui mettent leur propre sécurité en danger. Les fiches d'installation des applications permettront aux utilisateurs de recevoir des informations précises sur les applications qu'ils téléchargent, de sorte que les utilisateurs seront moins susceptibles d'être amenés à installer une fausse application ou une application avec des termes qu'ils ne comprennent pas. Exiger que les marchés d'applications alternatifs effectuent une surveillance continue aidera à empêcher les applications malveillantes de se propager sans contrôle. Et des fiches d'information sur les systèmes de paiement alternatifs permettront aux utilisateurs de savoir qu'ils doivent désormais être vigilants face aux fraudes et escroqueries destinées à les inciter à payer trop cher ce qu'ils ont demandé.

Ces protections contribuent à garantir que les utilisateurs continueront à bénéficier d'une expérience iPhone enrichissante, sûre et transparente, où l'utilisateur contrôle ses propres données.
Et ils continueront à faire de l'iPhone le smartphone le plus sécurisé, le plus respectueux de la vie privée et le plus sûr disponible aujourd'hui dans l'Union européenne, offrant ainsi aux utilisateurs l'excellent produit qu'ils attendent d'Apple.

Sources

1. Enquête : près de la moitié des utilisateurs d'Android envisagent de passer à l'iPhone pour des raisons de sécurité et de confidentialité, 9to5Mac (16 août 2022), https://9to5mac.com/2022/08/16/Les utilisateurs d'Android envisagent de changer d'iphone/.

2. Les développeurs de l'App Store ont généré 1 100 milliards de dollars de facturations et de ventes totales dans l'écosystème de l'App Store en 2022, Apple (31 mai 2023), https://www.apple.com/newsroom/2023/05/developers-generated-one-point-one-trillion-in-the-app-store-ecosystem-in-2022/.

3. Pour plus d'informations, consultez Apple annonce des modifications apportées à iOS, Safari et l'App Store dans l'Union européenne, Apple (25 janvier 2023), apple.com/salle de rédaction/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/.

4. L'App Store a stoppé plus de 2 milliards de dollars de transactions frauduleuses en 2022, Apple (mai 2023), https://www.apple.com/newsroom/2023/05/l'App-Store-a-arrêté-plus-de-2-milliards-de-transactions-frauduleuses-en-2022/.

5. Rapport sur la transparence de l'App Store 2022, Apple (2023), https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf.

6. Steve Jobs a reconnu ce problème en 2007. Voir Steve Jobs, iPhone SDK Letter (17 octobre 2007), disponible sur https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter.

7. Rapport sur les renseignements sur les menaces 2023, Nokia, https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/.

8. Voir Centre européen des consommateurs d'Allemagne, Conseils contre les pièges d'abonnement sur Internet, https://www.evz.de/fr/shopping-internet/internet-fraude/abonnement-traps.html.

9. Stuart Madnick, La menace continue pour les données personnelles : facteurs clés derrière l'augmentation de 2023 (décembre 2023), https://www.apple.com/newsroom/pdfs/La menace continue pour les données personnelles, facteurs clés derrière l'augmentation de 2023.pdf.

10. Construire un écosystème de confiance pour des millions d'applications : une analyse des menaces liées au chargement latéral, Apple (octobre 2021), p. 14.

11. Elizabeth Cassin, Sarahah : Application anonyme supprimée des magasins Apple et Google après des accusations d'intimidation, BBC (25 février 2018), https://www.bbc.com/actualités/blogs-tendances-43174619.

12. La FTC finalise une ordonnance exigeant que le fabricant de Fortnite, Epic Games, paie 245 millions de dollars pour avoir incité les utilisateurs à Effectuer des frais indésirables, FTC (4 mars 2023), https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-finalise-la-commande-exigeant-la-création-de-fortnite-maker-epic-games-pay-245-million-trucking-users ; Rapport sur les jeux mobiles pour enfants : plus des deux tiers des parents s'inquiètent des dépenses excessives de leurs enfants en achats intégrés, Sell Cell (5 juin 2020), https://www.sellcell.com/blog/plus des deux tiers des parents s'inquiètent des dépenses excessives de leurs enfants en matière d'achats via l'application.

13. Application faisant la promotion de soirées privées dans le contexte du COVID-19 supprimée de l'App Store d'Apple, Bus. Insider (30 décembre 2020), https://www.businessinsider.in/tech/apps/news/application-promotion-de-parties-privées-au milieu-covid-19-supprimé-de-apple-app-store/articleshow/80020920.cms ; Khadeeja Safdar et Kevin Poulsen, Google, Apple Struggle to Regulate Covid-19 Tracing Apps, Wall St. Journal (5 juin 2020), https://www.wsj.com/articles/pourquoi-google-et-apple-stores-avaient-une-application-covid-19-avec-ads-11591365499.

14. Le programme d'apprentissage en ligne pour enfants ABCmouse paiera 10 millions de dollars pour régler les accusations de la FTC concernant des pratiques illégales de marketing et de facturation, FTC (2 septembre 2020), https://www.ftc.gov/news-events/actualités/communiqués de presse/2020/09/programme-d'apprentissage-en-ligne-pour-enfants-abcmouse-payer-10-millions-règler-les-charges-ftc-marketing-illégal.