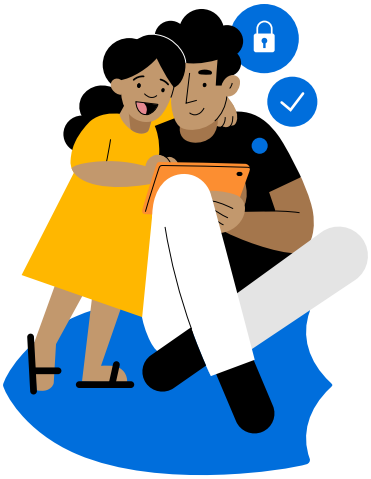


Créer un écosystème fiable pour des millions d'apps

De l'importance des mécanismes de protection fournis par l'App Store

Juin 2021

2007

« Nous essayons de concilier deux projets diamétralement opposés : proposer une plateforme avancée et ouverte aux équipes de développement, tout en protégeant les personnes utilisant l'iPhone des virus, logiciels malveillants et autres atteintes à la vie privée. La tâche est loin d'être aisée. »

Steve Jobs, 2007[1]

2016

« Utilisez uniquement le marché officiel des applications. Pour limiter au maximum le risque d'installer une application malveillante, il est recommandé de ne pas [télécharger des applications] auprès de sources tierces. Il est recommandé de ne pas se procurer des applications par sideloading (c'est-à-dire en dehors de l'App Store) si celles-ci ne proviennent pas d'une source authentique et légitime. »

Agence européenne de cybersécurité (ENISA), 2016[2]

2017

« Face aux apps malveillantes et indiscrètes, les bonnes pratiques identifiées pour réduire les menaces que font peser les apps vulnérables sont pertinentes. Par ailleurs, il est conseillé d'éviter le sideloading d'apps et le recours à des magasins d'apps non autorisés – pratiques qui devraient être interdites par les entreprises sur leurs appareils. »

U.S. Department of Homeland Security Report, 2017[3]

Aujourd'hui, nos téléphones sont bien plus que des téléphones : ils contiennent certaines des informations les plus sensibles sur nos vies personnelle et professionnelle. Ils nous suivent partout, et nous les utilisons pour appeler les personnes que nous aimons, échanger des messages, prendre et conserver des photos de nos enfants, nous repérer dans les lieux qui nous sont inconnus, compter le nombre de pas effectués dans la journée ou encore envoyer de l'argent à des proches. Ils nous accompagnent dans les moments heureux comme dans les situations d'urgence.

C'est avec cette idée en tête que nous avons conçu l'iPhone. Nous avons créé l'App Store pour offrir aux équipes de développement du monde entier un endroit où présenter des apps innovantes, capables de toucher une communauté mondiale croissante et florissante de plus d'un milliard d'utilisateurs et utilisatrices. Près de deux millions d'apps sont disponibles au téléchargement sur l'App Store, et des milliers d'autres s'y ajoutent chaque semaine. Vu l'ampleur de la plateforme de l'App Store, il était d'une importance capitale pour nous d'assurer la sécurité et la sûreté de l'iPhone dès le départ. Les équipes de recherche en matière de sécurité s'accordent à dire que l'iPhone est l'appareil mobile le plus sûr et le plus sécurisé, ce qui permet à celles et ceux qui l'utilisent de lui confier sans crainte leurs données les plus sensibles. Nous avons intégré à l'appareil des mécanismes ultra-sophistiqués de protection de la sécurité et nous avons créé l'App Store – un endroit fiable où découvrir et télécharger des apps en toute sécurité. Sur l'App Store, les apps proviennent d'entités de développement connues ayant accepté de suivre nos directives. Elles sont distribuées en toute sécurité, sans interférence de la part de tiers. Nous vérifions chaque app et chaque mise à jour afin de déterminer si elles répondent à nos normes très exigeantes. Cette procédure, que nous nous efforçons en permanence d'améliorer, est conçue pour protéger celles et ceux qui utilisent nos appareils, en barrant l'accès de l'App Store aux logiciels malveillants, à la cybercriminalité et aux escrocs. Les apps s'adressant aux enfants doivent suivre des directives strictes en matière de collecte de données et de sécurité. Ces directives sont conçues pour préserver la sécurité des enfants et doivent être étroitement intégrées aux fonctionnalités de contrôle parental d'iOS.

Quant au respect de la vie privée, pour nous, ce n'est pas juste important – c'est un droit humain fondamental. C'est ce principe qui sous-tend les normes de confidentialité élevées que nous intégrons toujours à nos produits : nous ne recueillons que les données personnelles strictement nécessaires à la fourniture d'un produit ou d'un service ; nous plaçons la personne utilisatrice en position de contrôle en lui demandant son autorisation avant que les apps ne puissent accéder à des données sensibles ; et nous fournissons des indications claires lorsque des apps accèdent à certaines fonctionnalités sensibles comme le micro, l'appareil photo ou encore la localisation de l'appareil. Dans le cadre de notre engagement continu pour le respect de la vie privée, deux de nos toutes nouvelles fonctionnalités de confidentialité – les étiquettes de confidentialité sur l'App Store et la transparence du suivi par les apps – offrent à notre clientèle un contrôle sans précédent sur les données de sa vie privée, avec une transparence accrue et des informations permettant de faire des choix éclairés. Toutes ces mesures de protection permettent de télécharger n'importe quelle app depuis l'App Store avec une parfaite tranquillité d'esprit. Tranquillité d'esprit qui profite également aux équipes de développement, puisqu'elle leur permet de toucher un large public qui se sent en confiance au moment de télécharger les apps.

Le saviez-vous ?

Apple vérifie toutes les apps et mises à jour publiées sur l'App Store afin d'intercepter celles susceptibles de porter préjudice aux personnes qui seraient amenées à les utiliser. Il peut s'agir d'apps qui proposent des contenus inappropriés, qui ne respectent pas la vie privée ou qui contiennent des logiciels malveillants identifiés, c'est-à-dire des logiciels utilisés à des fins nuisibles ou dangereuses.

Une étude a montré que les appareils qui fonctionnent sous Android étaient 15 fois plus atteints par des logiciels malveillants que les iPhone, la principale raison de cet état de fait étant que les apps Android « peuvent être téléchargées de n'importe où, ou presque », alors que les personnes utilisant un iPhone ne peuvent télécharger des apps que d'une seule source : l'App Store[4].

Cette approche de la sécurité et de la confidentialité se révèle particulièrement efficace. Aujourd'hui, il est extrêmement rare de faire face à des logiciels malveillants sur iPhone[5]. On nous a parfois suggéré de donner aux équipes de développement les moyens de diffuser leurs apps en dehors de l'App Store, par le biais de sites web ou de magasins d'apps tiers, processus appelé « sideloading ». Autoriser le sideloading aurait pour effet de détériorer la sécurité de la plateforme iOS et d'exposer les utilisateurs et utilisatrices à de réels risques de sécurité, non seulement sur les magasins d'apps tiers, mais aussi sur l'App Store. Étant donné l'immense communauté utilisant l'iPhone et les données sensibles qui y sont conservées (photos, données de localisation, informations de santé et financières), l'autorisation du sideloading déclencherait un déluge de nouveaux investissements dans des attaques visant la plateforme. Des personnes et entreprises mal intentionnées pourraient profiter de cette occasion pour dédier plus de ressources à la mise au point d'attaques sophistiquées ciblant les personnes utilisant iOS. Par exemple en développant l'ensemble des attaques et « exploits » (éléments de programme permettant d'exploiter une faille de sécurité informatique) hostiles, souvent désigné par l'expression « modèle de menace », contre lesquels il est essentiel de se prémunir. Ce risque accru d'attaques par des logiciels malveillants expose tout le monde à un risque plus grand encore, même celles et ceux qui ne téléchargent des apps que depuis l'App Store. En outre, même les personnes qui préfèrent ne télécharger des apps que depuis l'App Store peuvent être contraintes de télécharger une app indispensable à leur activité professionnelle, scolaire ou universitaire depuis un magasin d'apps tiers si l'app en question n'est pas mise à disposition sur l'App Store. Elles peuvent aussi être trompées et amenées à télécharger des apps depuis des magasins d'apps tiers se présentant sous les traits de l'App Store.

Des études montrent que les magasins d'apps tiers pour les appareils Android, où les apps ne font pas l'objet d'une vérification, exposent à beaucoup plus de risques et sont plus susceptibles de receler des logiciels malveillants que les magasins d'apps officiels[6]. Le résultat, c'est que les spécialistes de la sécurité déconseillent au public d'utiliser ces magasins d'apps tiers, car ils sont jugés peu sûrs[3,7]. Autoriser le sideloading ouvrirait les portes d'un monde où l'on n'aurait d'autre choix que d'accepter ces risques parce que certaines apps pourraient ne plus être disponibles sur l'App Store, et des arnaques viseraient à tromper les personnes en leur faisant croire qu'elles sont en train de télécharger en toute sécurité des apps depuis l'App Store, alors que ce ne serait pas le cas. Le sideloading exposerait celles et ceux qui utilisent nos appareils à des escrocs, qui pourraient alors exploiter les apps pour tromper le public, attaquer les fonctionnalités de sécurité de l'iPhone et menacer la vie privée. Il deviendrait aussi plus difficile de compter sur la fonctionnalité de contrôle parental permettant aux parents de gérer les téléchargements d'apps et les achats intégrés de leurs enfants, ainsi que sur Temps d'écran, fonctionnalité permettant de gérer le temps passé sur les écrans par les parents et les enfants. Les escrocs auraient l'occasion de tromper les enfants et les parents en travestissant la nature de leurs apps, réduisant ainsi l'efficacité de ces deux fonctionnalités.

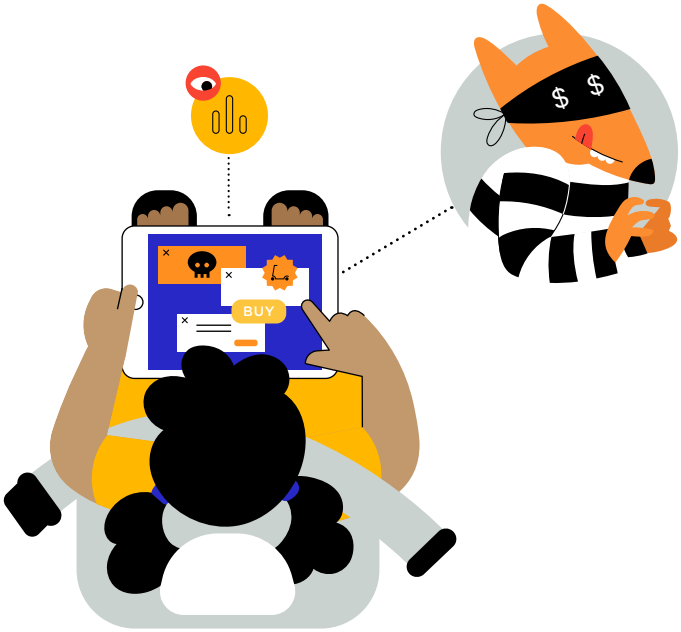
Au final, les utilisateurs et utilisatrices devraient être en permanence sur leurs gardes pour déjouer les arnaques, sans plus savoir à qui ni à quoi se fier. Ce qui aboutirait, pour un grand nombre de personnes, à télécharger moins d'apps provenant d'un nombre plus restreint d'équipes de développement. Ces dernières deviendraient alors plus vulnérables face aux menaces de certaines entités, qui pourraient proposer des outils de développement infectés contenant et propageant des logiciels malveillants. Elles seraient également plus menacées par la piraterie, ce qui saperait leurs possibilités de se faire rémunérer pour leur travail.

Des attaques bien réelles sur les plateformes autorisant le sideloading

On a découvert que certaines apps Android s'adressant aux enfants mettaient en œuvre des pratiques de collecte de données portant atteinte à leur vie privée. Ces apps continuent de prospérer et de cibler les utilisateurs et utilisatrices Android sur des magasins d'apps tiers, même après avoir été éliminées du Google Play Store[8].

Des entités malveillantes ont placé des publicités inconvenantes ou obscènes sur des apps ciblant les enfants[9].

Voyons en quoi l'expérience quotidienne d'une famille utilisant l'iPhone serait différente avec le sideloading. Nous allons, pour cela, suivre Nicolas et Emma, sa fille de 7 ans, tout au long d'une journée dans ce monde devenu plus incertain.



Un jeu téléchargé par sideloading contourne les contrôles parentaux

Emma demande à son père si elle peut jouer à un jeu dont elle a entendu parler par des camarades d'école. Nicolas recherche le jeu sur l'App Store, mais l'équipe de développement l'a rendu disponible uniquement sur des magasins d'apps tiers. Bien que mal à l'aise, il télécharge quand même le jeu, parce qu'Emma veut absolument l'essayer et que le magasin d'apps tiers le décrit comme adapté aux enfants. Sur le chemin du parc, alors qu'Emma est en train de jouer à ce jeu sur le siège arrière de la voiture, l'app se met à la bombarder de liens vers des sites web externes et des publicités ciblées. Au moment de télécharger le jeu, Nicolas a indiqué ses coordonnées de carte bancaire pour acheter à Emma un pack de démarrage, mais il n'a pas réalisé que le contrôle parental Demander l'autorisation d'achat ne fonctionnerait pas avec cette app obtenue par sideloading. En jouant, Emma achète de nombreuses parties en plus et des articles spéciaux, sans se rendre compte que son père n'a pas approuvé ces achats. L'app intègre également des traqueurs tiers qui recueillent, analysent et vendent les données d'Emma à des courtiers en données, alors même que l'app s'adresse aux enfants.

Des attaques bien réelles sur les plateformes autorisant le sideloading

Les apps téléchargées sur Android par le biais du sideloading sont connues pour lancer des attaques de rançongiciels « verrouilleurs ». Si elles sont installées, ces apps malveillantes empêchent la personne d'accéder à son téléphone ou cible ses photos jusqu'à obtention du paiement d'une rançon[10,11].

Des personnes utilisant Android ont été piégées et amenées à utiliser des méthodes non sécurisées pour télécharger de fausses versions d'apps telles que Netflix ou Candy Crush. Ces fausses apps, soit parce que l'accès leur est accordé, soit parce qu'elles exploitent les vulnérabilités des plateformes, sont capables d'espionner les personnes utilisant Android via le micro, de prendre des captures d'écran de leurs appareils, de voir la localisation de la personne, d'échanger des messages et des contacts, de voler les identifiants de connexion et d'apporter des changements au téléphone[12,13,14]. D'autres ont servi à dérober des identifiants bancaires et à prendre le contrôle de comptes en banque[15,16,17,18].

Une récente arnaque au rançongiciel implique une app Android se présentant comme une app de traçage des contacts liés au COVID-19. Si cette app est installée, elle chiffre toutes les données personnelles, ne laissant qu'une adresse e-mail à contacter pour récupérer les données[19].

Une app se trouvant sur les magasins d'apps Android tiers piège le public en se faisant passer pour une mise à jour du système. Une fois installée, l'app affiche une notification « Recherche de mise à jour ». Pendant ce temps, elle accède aux données personnelles telles que messages, contacts et images, et les vole[20,21].

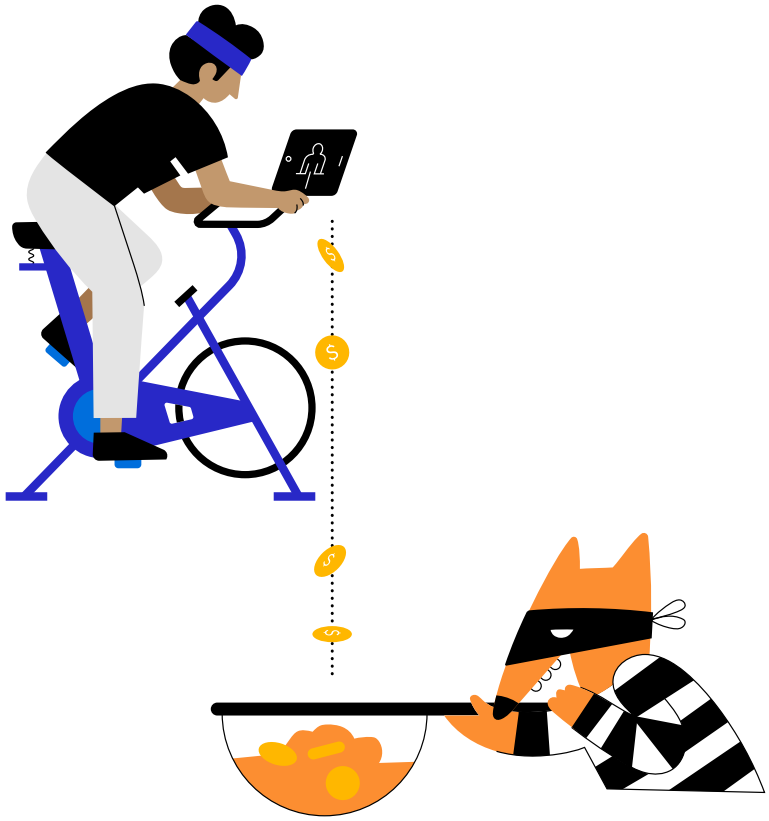
Au parc, la fausse app de filtres, imitant la vraie, qu'a téléchargée Nicolas par sideloading, menace de supprimer toutes ses photos – à moins qu'il ne paie

En compagnie d'Emma, au parc, Nicolas voit une publicité pour une app de filtres pour selfies qu'il trouverait amusant d'essayer avec Emma. Elle provient d'une société de développement connue. Cette publicité le mène à une page permettant de télécharger l'app qui ressemble à la page de la société de développement sur l'App Store. Se croyant protégé, Nicolas ne réalise pas qu'il est en train de télécharger une imitation de l'app depuis un magasin d'apps tiers. Comme il pense que l'app de filtres provient d'une société de développement fiable, il lui donne l'autorisation d'accéder à ses photos. Mais dès que l'app se lance, il comprend qu'il a fait une erreur : l'app menace de supprimer toutes les photos que contient son appareil photo à moins qu'il ne saisisse les coordonnées de sa carte bancaire et paie une rançon. Les protections intégrées à l'iPhone permettent à Nicolas de contrôler quelles apps sont autorisées à accéder à ses photos, mais cette app l'a berné et amené à donner cette autorisation en se faisant passer pour une app de filtres pour selfies.

Des attaques bien réelles sur les plateformes autorisant le sideloading

Les recherches montrent que les apps piratées publiées sur les magasins d'apps tiers entraînent chaque année des pertes de revenus de plusieurs milliards de dollars pour les entités de développement[22].

Les apps piratées et illégitimes pour d'autres raisons sont très répandues sur Android. Parmi ces apps figurent des apps de jeu qui permettent de tricher (par exemple, une version piratée de Pokémon Go ayant la capacité de simuler la localisation de la personne), des apps modifiées pour fournir un accès piraté à des contenus ou fonctionnalités premium, et des apps de jeux illégaux et de contenus réservés à un public adulte[23,24,25].

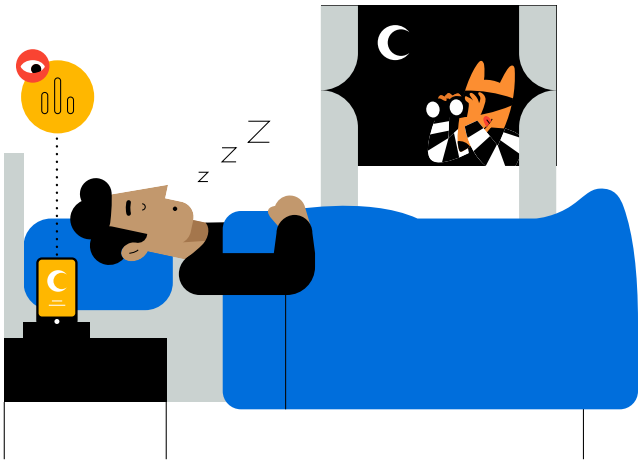


Sans le savoir, Nicolas télécharge une app piratée depuis un magasin d'apps tiers

L'amie de Nicolas utilise une app de fitness qu'elle adore et lui envoie un bon pour qu'il puisse l'essayer. Mais ce bon ne fonctionne que s'il télécharge l'app via un magasin d'apps tiers, et non via l'App Store. Il télécharge l'app et contracte un abonnement mensuel. Toutefois, ni elle ni lui n'a réalisé que cette app était piratée. L'argent qu'il verse chaque mois ne va donc pas à l'entité de développement qui a conçu et créé l'app, mais aux escrocs qui l'ont détournée. Nicolas pensait bien agir en soutenant l'équipe de développement de cette formidable app de fitness. En fait, il était en train de remplir les poches d'escrocs, encourageant sans le savoir un modèle frauduleux qui prive les propriétaires des apps de leurs revenus légitimes.

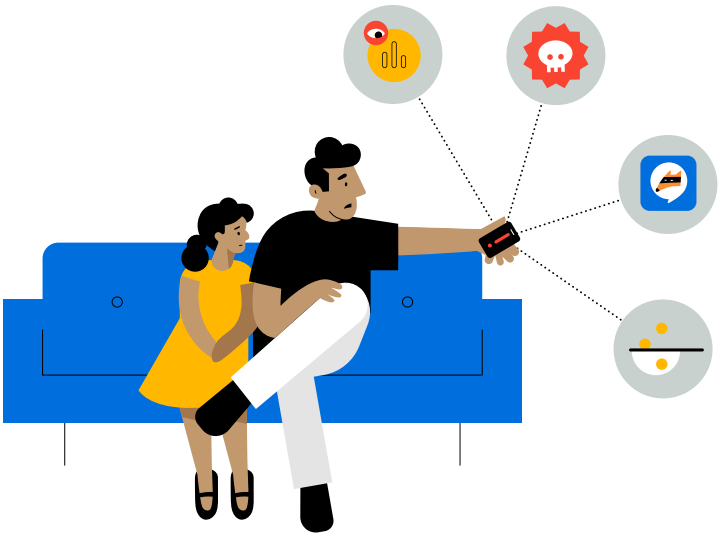
En savoir plus sur la protection de la vie privée par Apple

Pour en savoir plus sur la façon dont la transparence du suivi par les apps et les étiquettes de confidentialité de l'App Store vous donnent plus de contrôle et de transparence sur la collecte et l'utilisation de vos données par les apps, lisez **Une journée avec vos données** et consultez **apple.com/fr/privacy/control.**



Une app téléchargée par sideloading porte atteinte à la vie privée de Nicolas

Nicolas a entendu parler d'une nouvelle app de suivi du sommeil qu'il aimerait essayer, mais qui n'est pas disponible sur l'App Store. Il la télécharge depuis un magasin d'apps tiers, s'identifie à l'aide de son adresse e-mail et commence à l'utiliser pour surveiller la qualité de son sommeil. L'app prétend assurer la confidentialité des données de santé et d'usage des personnes qui l'utilisent et ne pas associer celles-ci à des données externes ni les communiquer à des tiers. Cette affirmation se révèle néanmoins complètement mensongère. Comme l'app était disponible par sideloading, l'entité de développement était libre d'agir à sa guise : l'app a donc suivi Nicolas à l'aide de son adresse e-mail sans lui demander son autorisation. Cela a permis à l'entité de développement d'associer ses données à des informations recueillies auprès d'autres apps et de vendre ses données de santé à des courtiers en données, sans son autorisation et sans craindre d'en être empêchée.



L'iPhone est utilisé chaque jour par plus d'un milliard de personnes pour effectuer des opérations bancaires, gérer leurs données de santé et prendre des photos de leurs proches. Cette vaste base d'utilisateurs et utilisatrices constituerait une cible attrayante et lucrative pour la cybercriminalité et les escrocs en ligne, et l'autorisation du sideloading déclencherait un déluge de nouveaux investissements dans les attaques visant l'iPhone, d'une ampleur bien supérieure à celle des attaques visant d'autres plateformes comme le Mac. Les escrocs se sentiraient pousser des ailes et développeraient des outils et une expertise pour attaquer la sécurité des iPhone. L'App Store est conçu pour détecter et déjouer les attaques actuelles, mais un changement du modèle de menace pourrait permettre de contourner ces protections. La cybercriminalité utiliserait ensuite les outils et l'expertise ainsi réunis pour cibler les magasins d'apps tiers ainsi que l'App Store, ce qui constituerait un risque plus important pour l'ensemble des utilisateurs et utilisatrices, même celles et ceux qui téléchargent des apps uniquement depuis l'App Store. Les canaux de distribution supplémentaires introduits par le sideloading offrent aux personnes et entreprises malveillantes de nouvelles possibilités d'exploiter les vulnérabilités du système, incitant les responsables d'attaques à développer et disséminer un nombre accru de logiciels malveillants.

Cela signifie que les personnes comme Nicolas, qui en était venu à considérer comme acquises la sécurité et la protection qu'offrent l'iPhone et l'App Store, devraient être constamment sur leurs gardes pour détecter les astuces en perpétuelle évolution de la cybercriminalité et des escrocs, sans jamais savoir à qui ni à quoi se fier. Dans certains cas, Nicolas n'aurait guère d'autre choix que de prendre un risque en téléchargeant depuis un magasin d'apps tiers une app non disponible sur l'App Store, ou bien il serait trompé et incité à faire du sideloading sans le savoir. Dans les cas les plus graves, les apps téléchargées par sideloading se faisant passer pour ce qu'elles ne sont pas (par exemple, pour une mise à jour de logiciel Apple) ou maquillant leur page de téléchargement pour la faire ressembler à l'App Store, pourraient tenter de briser les protections intégrées à l'iPhone pour accéder à des données protégées telles que les messages, les photos et la localisation de la personne. À la lueur de tous ces risques et arnaques, Nicolas serait beaucoup plus précautionneux dans son choix d'apps à télécharger. En fin de compte, il en téléchargerait moins et se cantonnerait à celles qui proviennent de quelques entités de développement fiables, ce qui compromettrait l'émergence de nouvelles entités plus petites proposant des apps innovantes. Il n'aurait pas la tranquillité d'esprit que procure la certitude que les apps de son iPhone sont les options les plus sûres pour lui et pour sa fille.

Le saviez-vous ?

Les personnes inquiètes pour leur sécurité et pour le respect de leur vie privée sont plus susceptibles de télécharger moins d'apps et d'en supprimer de leurs appareils[26,27,28]. Un écosystème moins sûr, où le téléchargement d'apps peut sembler aventureux, pourrait dissuader d'essayer de nouvelles apps innovantes ou de se risquer sur des apps provenant d'entités de développement plus récentes ou moins connues. Cela pourrait freiner la croissance de l'économie des apps et serait préjudiciable pour toutes les parties prenantes, côté utilisation comme côté développement.

Les strates de sécurité d'Apple et la procédure App Review protègent Nicolas, Emma et leurs appareils

Pour protéger les personnes utilisant iOS des apps malveillantes et assurer la meilleure sécurité possible pour la plateforme, nous adoptons une approche pluridimensionnelle, avec de multiples strates de protection. iOS pose des défis de sécurité sans équivalent parce que les personnes qui l'utilisent téléchargent en permanence de nouvelles apps sur leurs appareils, et que les appareils iOS doivent être assez sécurisés pour être utilisés par des enfants sans surveillance. Cela signifie que nous choisissons une approche renforcée de la sécurité de l'iPhone par rapport au Mac afin de tenir compte des différences d'usages, de comportements et d'attentes.

- **Comme sur le Mac, nous utilisons des logiciels automatisés pour parcourir les apps à la recherche de logiciels malveillants connus, empêchant ces derniers de se frayer un chemin sur l'App Store et d'atteindre la communauté utilisatrice ou de lui nuire.**
- **Par ailleurs, les entités de développement d'apps sont tenues de fournir une description de leur app et de ses fonctionnalités.** Ces informations sont examinées par une équipe de spécialistes qui en vérifient l'exactitude au cours de la procédure App Review, puis elles sont présentées au public, qui peut ainsi mieux évaluer l'intérêt de télécharger telle ou telle app. Cette procédure érige une barrière efficace contre les arnaques les plus couramment utilisées pour diffuser des logiciels malveillants : le fait de présenter un logiciel malveillant sous les traits d'une app populaire, ou encore la prétention à offrir des fonctionnalités attrayantes qui ne sont en réalité jamais fournies.
- En plus de vérifier si les fonctionnalités de l'app sont conformes à la description et si la page de l'App Store dédiée à l'app fournit des informations exactes, **ces spécialistes vérifient manuellement que l'app ne demande pas un accès aux données sensibles sans raison valable, et s'assurent que les apps ciblant les enfants respectent des règles très strictes en matière de collecte des données et de sûreté.**
- **Lorsqu'une app est admise sur l'App Store, mais qu'il apparaît ensuite qu'elle ne respecte pas nos directives, nous nous rapprochons de l'équipe de développement afin de résoudre le problème au plus vite.** Dans les cas dangereux, impliquant une escroquerie et une activité malveillante, l'app est immédiatement retirée de l'App Store – et les personnes l'ayant téléchargée peuvent être averties de son comportement néfaste.
- **En cas de problème avec une app téléchargée depuis l'App Store, l'AppleCare peut fournir une assistance et proposer un éventuel remboursement.**

L'objectif de la procédure App Review est de s'assurer que les apps proposées sur l'App Store sont fiables et que les informations fournies sur la page de l'App Store dédiée à une app offrent une représentation fidèle de son fonctionnement et des données auxquelles elle aura accès. Nous améliorons en permanence cette procédure en actualisant et en affûtant continuellement nos outils et notre méthodologie.

Après avoir téléchargé une app par le biais de l'App Store, les personnes peuvent contrôler le fonctionnement de cette app et à quelles données elle peut accéder grâce à des autorisations et à des fonctionnalités telles que la transparence du suivi par les apps. Les parents contrôlent les achats effectués par leurs enfants grâce à la fonctionnalité de demande d'autorisation, le temps passé sur certaines catégories d'apps grâce aux fonctionnalités de Temps d'écran ainsi que le type de données partagées. Les utilisateurs et utilisatrices peuvent également gérer de manière centralisée tous les paiements liés à des apps, mais aussi consulter et annuler facilement les abonnements réglés par le biais des Paiements intégrés. Ces mécanismes de contrôle ne pourraient pas être pleinement mis en œuvre sur des apps téléchargées par sideloading.

Outre les protections fournies par la procédure App Review, nous concevons le matériel et les logiciels de nos appareils de façon à assurer une dernière ligne de défense en cas de téléchargement sur l'appareil d'une app nuisible. Par exemple, les apps téléchargées sur iPhone depuis l'App Store sont placées dans un « bac à sable ». Cela signifie qu'elles ne peuvent pas accéder aux fichiers stockés par d'autres apps, ni apporter des changements à l'appareil, sans avoir obtenu l'autorisation explicite de l'utilisateur ou utilisatrice.

La meilleure défense repose sur l'association de toutes les strates : la solide procédure App Review pour éviter l'installation d'apps malveillantes et les solides protections de la plateforme pour limiter les dégâts que peuvent infliger les apps malveillantes. La sécurité intégrée à iOS fournit de puissants mécanismes de protection qui sont les meilleurs qu'on puisse trouver sur un appareil grand public. Mais ces mécanismes ne sont pas conçus pour protéger contre les choix qu'une personne peut être incitée à faire par des moyens fallacieux. La procédure App Review renforce les règles de l'App Store conçues pour protéger les utilisateurs et utilisatrices des apps qui tenteraient de leur nuire ou de les amener, par divers subterfuges, à accorder l'accès à des données sensibles. Et dans les cas très graves où des apps malveillantes tenteraient de contourner les mécanismes de protection intégrés à l'appareil, la procédure App Review leur rend l'accès aux appareils plus difficile dès le départ.

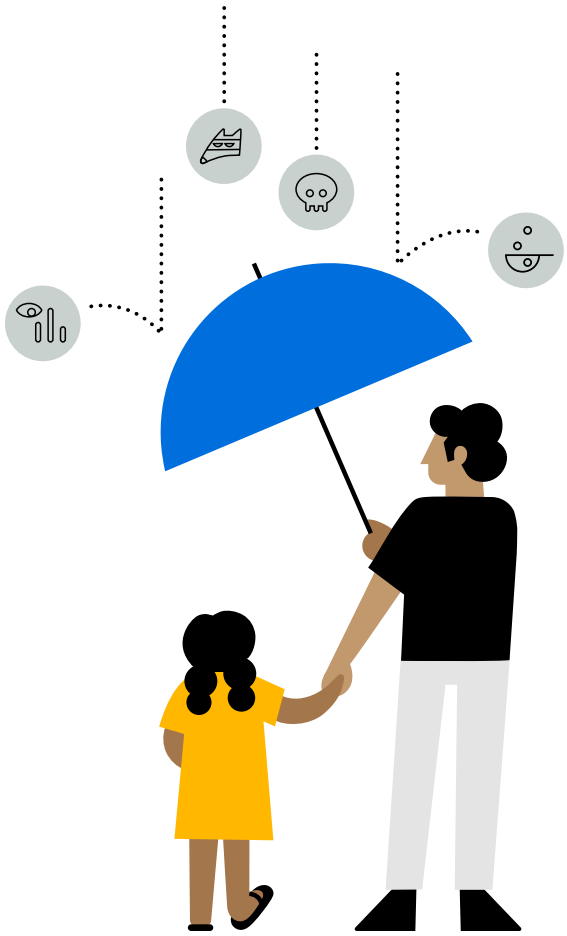
Le résultat de toutes ces mesures, c'est que les spécialistes de la sécurité s'accordent à dire que l'iPhone est l'appareil mobile le plus sûr et le plus sécurisé. Les multiples strates de sécurité fournies par Apple assurent un niveau inégalé de protection face aux logiciels malveillants, offrant ainsi une parfaite tranquillité d'esprit.

Procédure App Review

La procédure App Review nous permet de nous assurer que les apps proviennent de sources vérifiées et qu'elles sont exemptes de composants malveillants connus. Nous vérifions également que les apps ne cherchent pas à vous piéger en vous amenant à faire des achats non désirés ou à accorder l'accès à vos données personnelles. Côté développement et côté utilisation, tout le monde passe au crible, et les personnes qui se comportent mal sont exclues. La procédure App Review n'empêche pas la diffusion de chacune des apps de mauvaise qualité, mais nous n'avons de cesse d'innover et d'en améliorer les technologies, les pratiques et les processus.

Coup d'œil sur les mesures de protection des apps mises en œuvre par Apple en 2020

- **En moyenne, 100 000 nouvelles apps et mises à jour sont examinées chaque semaine** par une équipe dédiée de plus de 500 spécialistes qui évaluent les apps dans différentes langues.
- **Près d'un million de nouvelles apps posant un problème ainsi qu'un nombre équivalent de mises à jour ont été rejetées ou supprimées :**
  - Plus de 150 000 parce qu'elles étaient des éléments indésirables ou des imitations, ou parce qu'elles trompaient le public
  - Plus de 215 000 parce qu'elles violaient les directives en matière de respect de la vie privée
  - Plus de 48 000 parce qu'elles contenaient des fonctionnalités cachées ou non documentées
  - Quelque 95 000 parce qu'elles constituaient des infractions, essentiellement par l'intégration de fonctionnalités leurres (de type « prix d'appel ») pour commettre des actions illégales, voire criminelles
- **Apple a suspendu des transactions potentiellement frauduleuses pour un montant total de plus de 1,5 milliard de dollars.**
- **Apple a expulsé 470 000 équipes du programme Apple Developer pour cause de fraude.** Apple a aussi rejeté près de 205 000 tentatives d'inscription au programme pour des suspicions de fraude.
- **Apple a désactivé 244 millions de comptes clients en raison de fraudes ou d'abus, notamment de faux avis.** Apple a également rejeté 424 millions de tentatives de création de comptes reposant sur des schémas frauduleux et abusifs.



La procédure App Review procure à Nicolas une parfaite tranquillité d’esprit lorsqu’il télécharge des apps

Les fonctionnalités de sécurité et de respect de la vie privée de l’App Store procurent à Nicolas une parfaite tranquillité d’esprit lorsqu’il télécharge des apps pour lui-même ou pour sa fille. Il sait qu’Apple passe au crible 100 % des apps de l’App Store à la recherche de logiciels malveillants connus et que, par rapport aux autres appareils, il est extrêmement rare de faire face à des logiciels malveillants sur un iPhone.

En savoir plus sur les mesures de protection mises en œuvre par Apple

Pour en savoir plus sur la façon dont Apple protège votre sécurité et votre vie privée sur l'App Store, consultez **apple.com/fr/app-store.**

Pour en savoir plus sur la façon dont Apple protège vos données de localisation, lisez le **Livre blanc sur le service de localisation.**

Pour en savoir plus sur le contrôle parental sur iOS, consultez **apple.com/fr/families.**

Questions et réponses

Qu'est-ce que le « sideloading » ?

Le « sideloading » est le processus de téléchargement et d'installation d'apps sur un appareil mobile depuis une source autre que l'App Store officiel, comme un site web ou un magasin d'apps tiers. Pour protéger la sécurité et la vie privée, nous avons, dès le départ, conçu l'iPhone de sorte que le sideloading ne soit pas autorisé dans le cadre d'une utilisation quotidienne.

Qu'est-ce qu'un « modèle de menace » ?

Un « modèle de menace » est l'ensemble des attaques et vulnérabilités contre lesquelles il est nécessaire de se prémunir. Selon les appareils, les personnes et les environnements, les modèles de menace diffèrent, et la sécurité doit être conçue avec une vigilance particulière à cet égard. L'App Store est un élément clé dans la protection contre le modèle de menace visant l'iPhone. C'est un lieu fiable qui permet de télécharger des apps vérifiées par Apple provenant d'entités de développement connues qui sont tenues de respecter les consignes d'Apple.

L'autorisation du sideloading d'apps depuis des sites web et des magasins d'apps tiers sur iPhone pourrait-elle constituer une menace pour les personnes qui ne téléchargent des apps que depuis l'App Store ?

Oui. En fournissant des canaux de distribution supplémentaires, en modifiant le modèle de menace et en élargissant le champ des attaques potentielles, le sideloading sur iPhone exposerait tout le monde à un risque – y compris celles et ceux qui font volontairement la démarche de ne télécharger des apps que par le biais de l'App Store pour se protéger. L'autorisation du sideloading déclencherait un déluge de nouveaux investissements dans les attaques visant l'iPhone, en incitant les personnes et entités mal intentionnées à développer des outils et une expertise pour attaquer la sécurité des iPhone à une échelle sans précédent. Ces personnes et entités mal intentionnées pourraient se servir de l'expertise ainsi développée pour lancer des attaques de plus en plus sophistiquées, visant des fournisseurs d'apps tiers ainsi que l'App Store, ce qui présenterait un risque accru pour tout le monde. En outre, même les personnes qui préfèrent ne télécharger des apps que depuis l'App Store peuvent être contraintes de télécharger une app indispensable à leur activité professionnelle, scolaire ou universitaire depuis un magasin d'apps tiers si l'app en question n'est pas mise à disposition sur l'App Store. Elles peuvent aussi être trompées et amenées à télécharger des apps depuis des magasins d'apps tiers se présentant sous les traits de l'App Store.

Que recouvre la procédure App Review d'Apple ?

Nous associons des technologies sophistiquées à une expertise humaine pour examiner attentivement chaque app et chaque mise à jour afin de déterminer si elles respectent les consignes strictes de l'App Store en matière de respect de la vie privée, de sécurité et de sûreté. Nous comptons sur l'expertise humaine lorsque l'examen automatisé ne suffit pas à détecter des problèmes spécifiques, comme des violations de la vie privée ou des apps destinées aux enfants qui ne respectent pas nos consignes strictes. Ces consignes ont évolué au fil du temps pour répondre à de nouvelles menaces et à de nouveaux défis, dans le but de protéger les utilisateurs et utilisatrices et de leur offrir la meilleure expérience possible sur l'App Store. En moyenne, 100 000 nouvelles apps et mises à jour sont examinées chaque semaine par une équipe dédiée de plus de 500 spécialistes dans le monde entier.

Qu'est-ce qui est évalué ?

Toutes les apps et mises à jour proposées à l'App Store sont soumises à la procédure App Review.

Quels sont les contrôles parentaux disponibles sur les appareils Apple ?

Nous concevons des fonctionnalités qui permettent aux parents de contrôler la façon dont les enfants utilisent leurs appareils. Temps d'écran offre aux parents une meilleure compréhension du temps que passent leurs enfants à utiliser les apps, à consulter des sites web et à se servir de leurs appareils. Cette fonctionnalité leur permet également de fixer la durée que leurs enfants peuvent consacrer chaque jour à certaines catégories d'apps et de sites web. Par ailleurs, la fonctionnalité Demander l'autorisation d'achat permet aux parents d'approuver ou de refuser, directement depuis leur appareil, les achats et téléchargements d'apps par leurs enfants. Cette fonctionnalité dispose d'un délai de quinze minutes pour empêcher tout achat ultérieur.

Que sont la transparence du suivi par les apps et les étiquettes de confidentialité de l'App Store ?

Ces nouvelles fonctionnalités offrent aux utilisateurs et utilisatrices un plus grand contrôle sur leurs données et leur vie privée. La transparence du suivi par les apps exige que les apps obtiennent l'autorisation de la personne utilisatrice avant d'en suivre les données sur des apps ou des sites web détenus par d'autres entreprises. Avec les étiquettes de confidentialité de l'App Store, nous exigeons que chaque app de l'App Store fournisse un résumé clair des pratiques de sécurité mises en œuvre par l'entité de développement, ce qui livre des informations essentielles sur la façon dont une app utilise les données.

Sources

1. Jobs, Steve, « Third Party Applications on the iPhone », 17 octobre 2007, accessible sur tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, « Vulnerabilities - Separating Reality from Hype », *European Union Agency for Cybersecurity*, 24 août 2016.

3. Griffin, Robert Jr., « Study on Mobile Device Security », *U.S. Department of Homeland Security*, avril 2017.

4. Nokia, « Threat Intelligence Report 2020 », *Nokia*, 2020.

5. Johnson, Dave, « Can iPhones get viruses? Here's what you need to know », *Business Insider*, 4 mars 2019.

6. Symantec, « Internet Security Threat Report, Volume 23 », avril 2018.

7. Golovin, Igor, « Malware in Minecraft mods: story continues », *Kaspersky*, 9 juin 2021.

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

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

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

11. Seals, Tara, « Emerging Ransomware Targets Photos, Videos on Android Devices », *ThreatPost*, 24 juin 2020.

12. Owaida, Amer, « Beware Android trojan posing as Clubhouse app », *WeLiveSecurity by ESET*, 18 mars 2021.

13. Desai, Shivang, « SpyNote RAT posing as Netflix app », *Zscaler*, 23 janvier 2017.

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

15. Palmer, Danny, « This Android trojan malware is using fake apps to infect smartphones, steal bank details », *ZDNet*, 1er juin 2021.

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

17. Stefanko, Lukas, « Android Trojan steals money from PayPal accounts even with 2FA on », *WeLiveSecurity* by ESET, 11 décembre 2018.

18. Cybereason Nocturnus Team, « FakeSpy Masquerades as Postal Service Apps Around the World », *Cybereason*, 1er juillet 2020.

19. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, 24 juin 2020.

20. Yaswant, Aazim, « New Advanced Android Malware Posing as "System Update" », *Zimperium*, 26 mars 2021.

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

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

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

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

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

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

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

28. Gikas, Mike, « How to Protect Your Privacy on Your Smartphone », *Consumer Reports*, 1er février 2017.