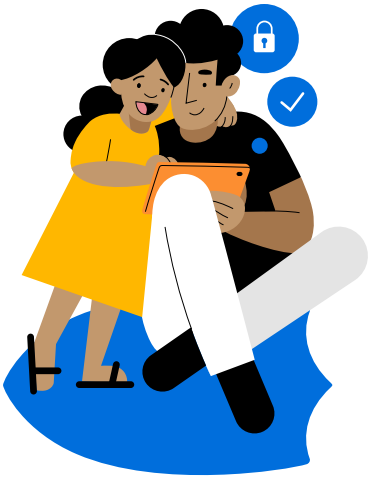


Bâtir un écosystème fiable pour des millions d'apps

Le rôle essentiel des mesures de protection intégrées à l'App Store

Juin 2021

2007

« Nous essayons de faire deux choses diamétralement opposées en même temps : offrir une plateforme ouverte de pointe aux équipes de développement, tout en protégeant iPhone des virus, logiciels malveillants et autres attaques qui portent atteinte à la vie privée. Ce n'est pas une tâche facile. »

Steve Jobs, 2007[1]

2016

« Optez toujours pour les marchés d'apps officiels. Afin de réduire le risque d'installer des applications malveillantes, évitez de vous tourner vers des sources tierces. Et n'ayez pas recours au téléchargement hors boutique pour obtenir des apps peu fiables qui n'ont pas été authentifiées. »

Agence de l'Union européenne pour la cybersécurité (ENISA), 2016[2]

2017

« Les pratiques à privilégier pour atténuer les menaces liées aux apps vulnérables s'appliquent aussi aux apps malveillantes et à celles qui portent atteinte à la vie privée. Les gens devraient également éviter le téléchargement d'apps hors boutique et les achats sur des plateformes non autorisées. Les entreprises, elles, devraient interdire ces façons de faire sur leurs appareils. »

Rapport du département de la Sécurité intérieure des États-Unis, 2017[3]

De nos jours, les téléphones sont bien plus que de simples outils de communication; ils renferment certaines des informations les plus confidentielles sur notre vie personnelle et professionnelle. On s'en sert partout et pour tout : appeler les gens qu'on aime et leur envoyer des textos, prendre et stocker des photos de nos enfants, obtenir un itinéraire quand on se perd, faire le suivi de nos pas quotidiens ou transférer de l'argent à nos proches. On compte sur eux dans les meilleurs comme dans les pires moments.

C'est dans cette optique que nous avons conçu iPhone. Nous avons créé l'App Store pour donner aux équipes de développement du monde entier un endroit où proposer des apps novatrices à une communauté croissante et florissante de plus d'un milliard de personnes. Près de deux millions d'apps sont présentement offertes sur l'App Store, et des milliers d'autres s'ajoutent chaque semaine. Compte tenu de l'ampleur de la plateforme, il était extrêmement important pour nous de garantir la sécurité et la sûreté d'iPhone dès le départ. Les chercheurs et chercheuses du domaine de la sécurité s'entendent pour dire qu'iPhone est l'appareil mobile le plus sûr qui soit. Notre clientèle peut donc y stocker ses données les plus confidentielles en toute confiance. Nous avons intégré à iPhone des fonctionnalités de sécurité des plus sophistiquées et avons créé l'App Store, un espace fiable où il est possible de découvrir et télécharger des apps sans danger. Les apps de l'App Store sont développées par des entreprises reconnues qui ont accepté de suivre nos lignes directrices et sont distribuées de façon sécuritaire, sans aucune interférence de tiers. Nous vérifions chacune des apps et des mises à jour pour déterminer si elles répondent à nos normes élevées. Ce processus, que nous cherchons constamment à améliorer, est conçu pour protéger les gens en gardant l'App Store à l'abri des logiciels malveillants, de la cybercriminalité et des tentatives d'hameçonnage. Pour garantir la sécurité des enfants, les apps qui leur sont destinées doivent respecter des directives strictes en matière de collecte et de données et de sécurité, en plus d'être étroitement intégrées aux fonctions de contrôle parental d'iOS.

La confidentialité n'est pas quelque chose que nous prenons à la légère – c'est un droit humain fondamental que nous défendons avec vigueur. Ce principe guide les normes élevées auxquelles nous soumettons nos produits : nous recueillons uniquement les données personnelles indispensables à l'offre de nos produits et services, donnons le plein contrôle aux utilisateurs et aux utilisatrices en sollicitant leur permission avant qu'une app puisse accéder à leurs données confidentielles, et informons clairement ces derniers lorsque des apps doivent accéder à certaines

Le saviez-vous?

Apple vérifie toutes les apps et mises à jour de l'App Store pour intercepter celles qui pourraient nuire aux utilisateurs et aux utilisatrices. Il peut s'agir d'apps qui proposent des contenus inappropriés, portent atteinte à la vie privée ou contiennent des logiciels malveillants connus, c'est-à-dire des logiciels utilisés à des fins dommageables ou dangereuses.

Une étude a démontré que les appareils qui fonctionnent sous Android sont la proie de 15 fois plus d'infections par des logiciels malveillants qu'iPhone. Pourquoi? Alors que les apps pour iPhone ne peuvent être téléchargées que d'un seul et même endroit, l'App Store, les apps Android « peuvent l'être à partir d'à peu près n'importe quelle source »[4].

fonctionnalités sensibles, comme le microphone, la caméra et la géolocalisation. Dans le cadre de notre engagement continu envers la protection de la vie privée, deux de nos plus récentes fonctionnalités – les étiquettes de confidentialité dans l'App Store et la transparence du suivi par les apps – donnent à notre clientèle un contrôle sans précédent sur leur vie privée, avec une transparence accrue et de l'information pour les aider à faire des choix éclairés. Grâce à ces mesures de protection, les gens peuvent télécharger n'importe quelle app de l'App Store en toute quiétude. Une tranquillité d'esprit dont profitent également les équipes de développement, qui peuvent rejoindre un vaste auditoire confiant au moment de télécharger leurs apps.

Jusqu'ici, notre approche en matière de sécurité et de confidentialité s'est avérée très efficace. Il est aujourd'hui extrêmement rare de voir un logiciel malveillant apparaître sur iPhone[5]. Certaines personnes croient qu'Apple devrait offrir aux équipes de développement un moyen de distribuer leurs apps en dehors de l'App Store, soit par l'entremise de sites web ou de plateformes de ventes d'apps opérées par des tiers, une pratique qu'on appelle le « téléchargement hors boutique ». Or, autoriser le téléchargement hors boutique entraînerait une détérioration de la sécurité de la plateforme iOS et exposerait les appareils à de graves risques, non seulement dans les magasins d'apps de tiers, mais aussi dans l'App Store. Étant donné la taille considérable du bassin de personnes qui utilisent iPhone, et des données sensibles qu'elles stockent sur leur appareil (photos, données de localisation, informations médicales et financières), permettre le téléchargement hors boutique donnerait lieu à un afflux de nouveaux investissements visant à attaquer la plateforme. Des organisations mal intentionnées pourraient saisir cette occasion et consacrer plus de ressources à la mise au point d'attaques sophistiquées ciblant les appareils iOS, dans le but de multiplier les assauts hostiles et d'exploiter les failles de sécurité – un ensemble de ruses communément appelé « modèle de menace », contre lequel tout le monde doit être protégé. Ce risque accru d'attaques par des logiciels malveillants pourrait compromettre la sécurité de tous les utilisateurs et utilisatrices, même celles et ceux qui téléchargent uniquement des apps de l'App Store. Même les gens qui s'en tiennent à l'App Store pourraient être forcés d'utiliser une plateforme de tiers pour télécharger une app essentielle à leur travail ou à leurs études si elle n'est pas offerte dans l'App Store. Ou encore, ils pourraient télécharger une app à leur insu depuis une boutique de tiers qui tente de se faire passer pour l'App Store.

Des études ont révélé que les boutiques de tiers où les apps ne sont pas soumises à des vérifications sont beaucoup plus risquées et susceptibles de renfermer des logiciels malveillants que les plateformes officielles[6]. C'est pourquoi les spécialistes du domaine de la sécurité déconseillent au public de faire affaire avec ces magasins tiers, qu'ils jugent peu sécuritaires[3, 7]. Autoriser le téléchargement hors boutique ouvrirait la voie à un monde qui ne nous donnerait pas le choix d'accepter ces risques, puisque certaines apps pourraient ne plus être disponibles sur l'App Store. Des pros de l'arnaque pourraient alors usurper l'identité de l'App Store et nous leurrer en nous faisant croire à tort qu'on peut télécharger ces apps en toute sécurité. Le téléchargement hors boutique exposerait le public à des pirates capables d'exploiter des apps à des fins frauduleuses, d'attaquer les fonctions de sécurité d'iPhone et de porter atteinte à la vie privée. Il deviendrait aussi plus difficile de compter sur Demander d'acheter, une fonction de contrôle parental qui permet aux parents de gérer les téléchargements d'apps et les achats intégrés faits par leurs enfants, ainsi que sur Temps d'écran, une fonction de gestion du temps passé devant les écrans. Ces deux fonctionnalités seraient en outre moins efficaces, puisque les cyberescrocs auraient la possibilité d'induire les enfants et les parents en erreur en dissimulant la vraie nature de leurs apps.

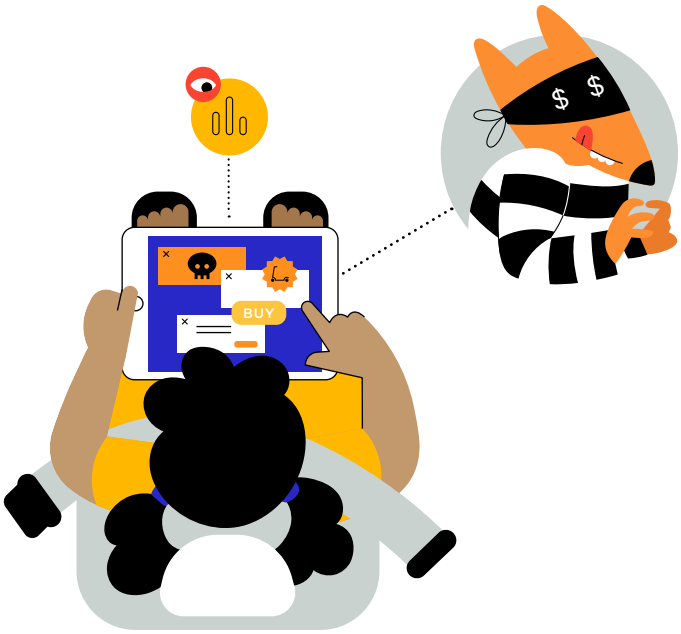
Les utilisateurs et les utilisatrices se devraient d'être continuellement à l'affût des arnaques, ne sachant jamais à qui ou à quoi se fier. Par conséquent, les gens téléchargeraient un nombre limité d'apps, auprès d'une poignée d'équipes de développement. Les entreprises de développement deviendraient elles-mêmes plus vulnérables aux menaces d'entités malintentionnées, qui pourraient leur proposer des outils de développement infectés contenant et propageant des logiciels dangereux. Elles seraient également plus exposées au piratage, ce qui réduirait leur capacité à se faire payer pour leur travail.

Exemples réels d'attaques sur des plateformes qui autorisent le téléchargement hors boutique

On a découvert que des apps Android destinées aux enfants avaient recours à des pratiques en matière de collecte de données qui portaient atteinte à la vie privée des jeunes. Ces apps continuent de circuler et de cibler les propriétaires d'appareils Android sur des boutiques d'apps tierces, et ce, même si elles ont été supprimées du Google Play Store[8].

Des entités malveillantes ont intégré des publicités inappropriées ou obscènes à des apps qui s'adressent aux enfants[9].

Voyons la différence que le téléchargement hors boutique pourrait faire dans le quotidien d'une famille qui utilise iPhone. Nous allons suivre Jean et Emma, sa fille de 7 ans, lors d'une journée comme une autre dans ce monde des plus incertains.



Un jeu téléchargé hors boutique contourne le contrôle parental

Emma demande à son père si elle peut jouer à un jeu dont elle a entendu parler à l'école. Jean cherche le jeu dans l'App Store, mais il peut uniquement être téléchargé depuis des magasins d'apps tiers. Même s'il n'est pas tout à fait à l'aise, Jean télécharge le jeu puisque Emma y tient vraiment et que la boutique tierce garantit qu'il convient aux enfants. Plus tard, en route vers le parc, alors qu'Emma joue à son nouveau jeu sur le siège arrière de la voiture, l'app se met à la bombarder de publicités ciblées et de liens vers des sites web externes. Au moment d'installer le jeu, Jean a saisi ses renseignements de carte de crédit pour acheter une trousse de départ à Emma, sans penser que le contrôle parental Demander d'acheter ne serait pas compatible avec l'application téléchargée hors boutique. Pendant qu'elle joue, Emma achète plusieurs parties supplémentaires 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, même si le jeu est destiné aux enfants.

Exemples réels d'attaques sur des plateformes qui autorisent le téléchargement hors boutique

Les apps téléchargées hors boutique sous Android sont connues pour exécuter des logiciels de rançon qui attaquent les appareils en les verrouillant. Si elles sont installées, ces apps malveillantes bloquent l'accès de la personne à son téléphone ou s'empare de ses photos, à moins qu'elle n'accepte de payer une rançon[10, 11].

Des propriétaires d'appareils Android ont été amenés, par la ruse, à utiliser des méthodes non sécurisées pour télécharger de fausses versions d'apps comme Netflix et Candy Crush. En obtenant un simple accès ou en exploitant les vulnérabilités de la plateforme, ces apps contrefaites sont capables d'espionner les utilisateurs et utilisatrices d'Android par l'entremise du micro de l'appareil, de prendre des captures d'écran, d'afficher la localisation, les messages texte et les contacts, de voler les identifiants de connexion et de modifier les réglages du téléphone[12, 13, 14]. D'autres apps ont quant à elles servi à voler les informations bancaires de certaines personnes et à prendre le contrôle de leur compte[15, 16, 17, 18].

Une récente arnaque au rançongiciel tire parti d'une app Android qui se fait passer pour une app de traçage de la COVID-19.

Au parc, la fausse app de filtres que Jean a téléchargée hors boutique menace de supprimer toutes ses photos s'il ne paie pas de rançon

Alors qu'il se trouve au parc avec Emma, Jean voit la publicité d'une app de filtres pour selfies développée par une entreprise bien connue et se dit qu'il serait amusant de l'utiliser avec sa fille. L'annonce le mène à une page de téléchargement qui ressemble à la page de l'entreprise sur l'App Store. Comme il se croit protégé, Jean ne réalise pas qu'il télécharge en fait une imitation sur une boutique d'apps de tiers. Et parce qu'il croit avoir affaire à une entreprise de développement fiable et reconnue, il donne à l'app l'autorisation d'accéder à ses photos. Dès qu'il lance l'app, Jean s'aperçoit qu'il a fait une erreur : l'app menace de supprimer toutes les photos de sa photothèque, à moins qu'il entre les données de sa carte de crédit et paie une rançon. Les mesures de protection intégrées à iPhone permettent à Jean de décider à quelles apps il donne accès à ses photos, mais celle-ci l'a piégé et l'a incité à donner accès à sa photothèque en se faisant passer pour une app de filtres pour selfies.

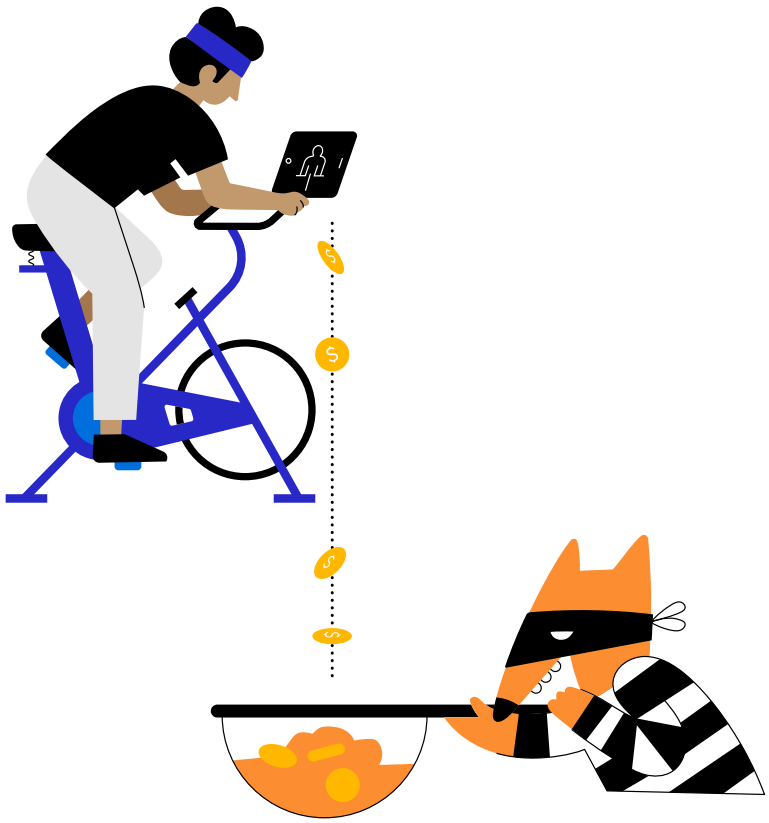
Une fois installée, l'app chiffre tous les renseignements personnels stockés sur l'appareil, puis laisse au propriétaire une adresse courriel à laquelle écrire pour récupérer ses données[19].

Une autre app offerte sur des boutiques tierces d'apps Android trompe les gens en prétendant être une mise à jour système. Après avoir été installée sur l'appareil, une notification de type « Recherche de mise à jour » s'affiche à l'écran pendant que l'app accède aux données personnelles – messages, contacts, photos, etc. – pour les voler[20, 21].

Exemples réels d'attaques sur des plateformes qui autorisent le téléchargement hors boutique

Des études montrent que les apps piratées publiées sur les magasins d'apps tiers font perdre chaque année des milliards de dollars en revenus aux entreprises de développement[22].

Les apps piratées et autrement illicites sont très répandues sous Android. Parmi celles-ci figurent les apps de jeu qui permettent de tricher (p. ex., une version piratée de Pokémon Go capable de simuler la position d'une personne), les apps modifiées qui fournissent un accès piraté à certaines fonctionnalités ou à des contenus exclusifs, ainsi que les apps de jeux clandestins et de contenus réservés aux adultes[23, 24, 25].

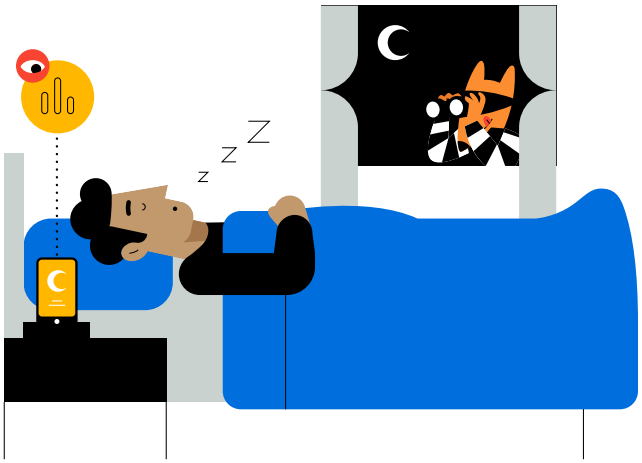


Jean télécharge sans le savoir une app piratée à partir d'une boutique de tiers

Une amie de Jean utilise une app de mise en forme qu'elle adore. Elle lui envoie un lien pour qu'il en fasse l'essai. Mais pour que le lien fonctionne, Jean doit télécharger l'app à partir d'un magasin de tiers plutôt que via l'App Store. Il télécharge l'app et s'inscrit à l'abonnement mensuel. Toutefois, ni lui ni son amie ne remarque que l'app a été piratée. La somme que Jean paie chaque mois pour son abonnement n'est donc pas versée au groupe qui a conçu et développé l'app, mais bien aux personnes qui l'ont volée. Jean est convaincu de soutenir l'équipe derrière une app formidable. Il contribue plutôt à enrichir des escrocs et encourage, à son insu, un système frauduleux qui prive les entreprises de développement de leurs revenus.

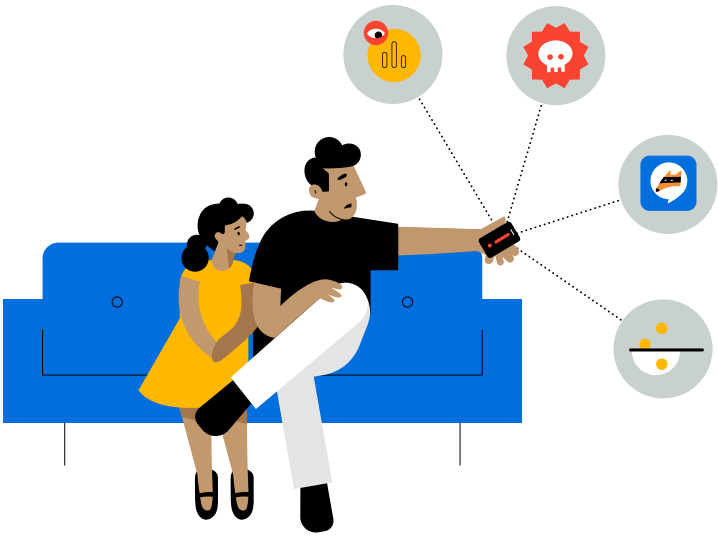
En savoir plus sur les mesures de protection de la confidentialité mises en place par Apple

Voyez comment la transparence du suivi par les apps et les étiquettes de confidentialité dans l'App Store vous offrent un plus haut niveau de transparence et de contrôle sur la façon dont les apps collectent et utilisent vos données. Prenez connaissance du document **Une journée dans la vie de vos données** et visitez **apple.com/ca/fr/privacy/control/.**



Une app téléchargée hors boutique viole la vie privée de Jean

Jean a entendu parler d'une app de suivi du sommeil. Il aimerait l'essayer, mais elle n'est pas offerte sur l'App Store. Il la télécharge donc à partir d'un magasin d'apps tiers. Il crée un compte avec son adresse courriel, puis commence à utiliser l'app pour évaluer la qualité de son sommeil. L'équipe de développement qui a conçu l'app affirme protéger la confidentialité des données de santé et d'utilisation des personnes abonnées. Elle prétend également ne pas associer les renseignements des utilisatrices et des utilisateurs à des données externes ni les partager avec des tiers. Malheureusement, ces déclarations se révèlent complètement fausses. Comme l'app a été téléchargée hors boutique, l'entreprise derrière a pu agir sans contraintes. L'app a donc pu suivre Jean à l'aide de son courriel, sans jamais lui demander son autorisation. L'entreprise a été en mesure d'associer les données de Jean aux renseignements recueillis par d'autres apps et de vendre ses données de santé à des courtiers, sans demander de permission et sans craindre qu'on l'en empêche.



Plus d’un milliard de personnes utilisent iPhone chaque jour pour effectuer des opérations bancaires, gérer leurs données de santé et prendre des photos de leurs proches. Ce vaste bassin représente une cible lucrative et attrayante pour le milieu de la cybercriminalité et de la fraude. L’autorisation du téléchargement hors boutique entraînerait un afflux de nouveaux investissements dans les attaques sur iPhone, d’une ampleur bien plus importante encore que celles ciblant les autres plateformes comme Mac. Les escrocs auraient le champ libre pour mettre au point des outils et développer une expertise visant à compromettre la sécurité des appareils iPhone. L’App Store est conçu pour détecter et contrecarrer les attaques de l’heure. Mais une transformation du modèle de menace pourrait permettre de contourner les mesures de protection actuellement en place. Les responsables d’activités frauduleuses mettraient à profit l’expertise et les outils nouvellement acquis pour cibler les magasins d’apps de tiers et l’App Store, exposant ainsi l’ensemble de notre clientèle, y compris les gens qui téléchargent uniquement à partir de l’App Store, à un risque considérable. Les canaux de distribution supplémentaires que procure le téléchargement hors boutique offriraient aux entités malintentionnées de nouvelles possibilités d’exploiter les vulnérabilités du système, en plus de les inciter à concevoir et disséminer un nombre accru de logiciels malveillants.

Il faudrait désormais que les personnes comme Jean, qui tiennent pour acquises la sécurité et la protection d’iPhone et de l’App Store, demeurent continuellement à l’affût des ruses en constante évolution des groupes misant sur la fraude et la cybercriminalité, sans jamais savoir à qui ou à quoi elles peuvent se fier. Dans certaines situations, Jean n’aurait pas d’autre choix que de prendre le risque de télécharger une app non disponible sur l’App Store à partir d’un magasin de tiers – ou il pourrait être poussé à le faire à son insu. Dans les cas les plus graves, les apps téléchargées hors boutique – qui tentent de se faire passer pour ce qu’elles ne sont pas (comme une mise à jour logicielle d’Apple) ou dont la page de téléchargement est déguisée pour ressembler à celle de l’App Store – pourraient essayer de contourner les mesures de protection intégrées à iPhone pour accéder à des données protégées, notamment les messages, les photos et la localisation. Sachant cela, Jean ferait certainement preuve d’une plus grande prudence au moment de choisir des apps. Il en téléchargerait probablement moins et s’en tiendrait à celles qui sont conçues par quelques entreprises en qui il a confiance. À long terme, cette approche nuirait à l’émergence des petites équipes de développement qui souhaitent faire leur place auprès du public en offrant des apps novatrices. Jean n’aurait pas la tranquillité d’esprit de savoir que les apps qu’il installe sur son iPhone sont les options les plus sécuritaires pour lui et pour sa fille.

Le saviez-vous?

Les personnes préoccupées par leur sécurité et la confidentialité de leurs données ont tendance à télécharger moins d'apps et sont plus susceptibles d'en supprimer de leurs appareils[26, 27, 28]. Un écosystème moins sûr où les gens ne se sentent pas en confiance quand ils téléchargent des apps pourrait les dissuader d'essayer de nouveaux produits ou de prendre le risque d'installer de nouvelles apps développées par des entreprises émergentes ou moins connues. Un tel climat pourrait entraver la croissance de l'économie des apps, au détriment du public et des équipes de développement.

Les couches de sécurité et le processus de vérification des apps App Review d'Apple protègent Jean, Emma et leurs appareils

Pour protéger les appareils iOS des apps malveillantes et offrir le meilleur niveau de sécurité sur la plateforme, nous privilégions une approche à plusieurs volets, comprenant de multiples couches de protection. iOS pose des défis uniques en matière de sécurité, entre autres parce que les personnes qui y ont recours téléchargent continuellement de nouvelles apps sur leurs appareils, et que les appareils iOS doivent être suffisamment sûrs pour que les enfants puissent s'en servir sans surveillance. Nos méthodes sur iPhone sont plus strictes que sur Mac, puisque les gens qui utilisent ces appareils, de même que leurs attentes et comportements, sont différents.

- **Comme sur Mac, nous faisons appel à des logiciels automatisés pour rechercher dans les apps des logiciels malveillants connus et ainsi éviter qu'ils se retrouvent dans l'App Store et nuisent à notre clientèle.**
- **Les équipes de développement sont également tenues de fournir une description de leur app et de ses caractéristiques.** Ces renseignements sont passés en revue par une équipe de spécialistes durant le processus de vérification App Review, puis présentés aux utilisateurs et aux utilisatrices pour les aider à faire des choix éclairés. La vérification des apps crée une barrière efficace contre les arnaques les plus couramment utilisées pour distribuer des logiciels malveillants : déguiser un logiciel malveillant en app populaire, ou prétendre offrir des fonctionnalités intéressantes alors que ce n'est pas réellement le cas.
- En plus de vérifier si l'app fonctionne comme décrit et si les renseignements qui figurent sur la page de l'App Store sont exacts, **ces spécialistes s'assurent manuellement que l'app ne demande pas inutilement d'accès aux données confidentielles. Par ailleurs, ces personnes veillent à ce que les apps destinées aux enfants respectent des règles rigoureuses en matière de sécurité et de collecte de données.**

- **Si une app est admise dans l'App Store, mais qu'on découvre plus tard qu'elle ne respecte pas les lignes directrices en vigueur, nous travaillons avec l'équipe de développement visée pour résoudre le problème rapidement.** Dans les cas dangereux qui impliquent une fraude ou une activité malveillante, l'app est immédiatement retirée de l'App Store, et les personnes qui l'ont téléchargée peuvent être mises au courant de la situation.
- **Et dans l'éventualité d'un problème avec une app téléchargée depuis l'App Store, le service AppleCare peut fournir une assistance et émettre un remboursement.**

L'objectif du processus de vérification App Review est de garantir que les apps de l'App Store sont fiables et que les renseignements qui figurent sur la page de l'App Store d'une app décrivent avec justesse son fonctionnement et les données auxquelles elle aura accès. Nous améliorons continuellement nos façons de faire en mettant à jour et en perfectionnant nos méthodes et outils.

Après avoir téléchargé une app par l'entremise de l'App Store, les utilisateurs et les utilisatrices peuvent contrôler son fonctionnement et les données auxquelles elle peut accéder au moyen de fonctionnalités comme la transparence du suivi par les apps et les permissions. Les parents peuvent aussi surveiller ce que leurs enfants achètent avec la fonction Demander d'acheter. Et grâce à Temps d'écran, il leur est possible de faire le suivi des données partagées et du temps passé dans certaines catégories d'apps. Enfin, les gens peuvent gérer tous leurs paiements à un seul et même endroit, en plus de consulter et d'annuler en toute simplicité les abonnements payés via le paiement dans les apps. Il serait difficile d'assurer la mise en œuvre de tels protocoles dans les apps téléchargées hors boutique.

En plus de la protection que confère le processus de vérification App Review, nous concevons le matériel et les logiciels de nos appareils de manière à offrir une dernière ligne de défense en cas de téléchargement d'une app nuisible. Par exemple, les apps téléchargées sur iPhone à partir de l'App Store sont placées en « bac à sable »; elles ne peuvent donc pas accéder aux fichiers stockés par d'autres apps ni apporter de modifications à l'appareil sans avoir obtenu l'autorisation explicite de l'utilisateur ou de l'utilisatrice.

La meilleure couverture repose sur une combinaison de couches : le processus rigoureux de vérification des apps, qui permet d'éviter l'installation d'apps malveillantes, et les mesures de protection robustes de la plateforme, qui limitent les dégâts que ces apps peuvent causer. La sécurité intégrée à iOS assure une puissante protection – la meilleure de tous les appareils grand public. Elle n'est toutefois pas conçue pour préserver les gens des mauvais choix qu'ils pourraient être poussés à faire. Le processus de vérification App Review renforce les politiques de l'App Store qui visent à protéger les utilisateurs et utilisatrices contre les apps qui

pourraient tenter de leur nuire ou les amener de façon malhonnête à faciliter l'accès à leurs données sensibles. Et dans l'éventualité plus grave où une app essaie de contourner les mesures de protection intégrées à l'appareil, App Review intervient dès le départ pour compliquer l'accès.

Les spécialistes de la sécurité sont unanimes : iPhone est l'appareil mobile le plus sûr qui soit. Les nombreuses couches de sécurité d'Apple procurent à notre clientèle un niveau inégalé de protection contre les logiciels malveillants et une tranquillité d'esprit sans pareil.

- **l'équipe de développement visée pour résoudre le problème rapidement.** Dans les cas dangereux qui impliquent une fraude ou une activité malveillante, l'app est immédiatement retirée de l'App Store, et les personnes qui l'ont téléchargée peuvent être mises au courant de la situation.
- **Et dans l'éventualité d'un problème avec une app téléchargée depuis l'App Store, le service AppleCare peut fournir une assistance et émettre un remboursement.**

L'objectif du processus de vérification App Review est de garantir que les apps de l'App Store sont fiables et que les renseignements qui figurent sur la page de l'App Store d'une app décrivent avec justesse son fonctionnement et les données auxquelles elle aura accès. Nous améliorons continuellement nos façons de faire en mettant à jour et en perfectionnant nos méthodes et outils.

Après avoir téléchargé une app par l'entremise de l'App Store, les utilisateurs et les utilisatrices peuvent contrôler son fonctionnement et les données auxquelles elle peut accéder au moyen de fonctionnalités comme la transparence du suivi par les apps et les permissions. Les parents peuvent aussi surveiller ce que leurs enfants achètent avec la fonction Demander d'acheter. Et grâce à Temps d'écran, il leur est possible de faire le suivi des données partagées et du temps passé dans certaines catégories d'apps. Enfin, les gens peuvent gérer tous leurs paiements à un seul et même endroit, en plus de consulter et d'annuler en toute simplicité les abonnements payés via le paiement dans les apps. Il serait difficile d'assurer la mise en œuvre de tels protocoles dans les apps téléchargées hors boutique.

En plus de la protection que confère le processus de vérification App Review, nous concevons le matériel et les logiciels de nos appareils de manière à offrir une dernière ligne de défense en cas de téléchargement d'une app nuisible. Par exemple, les apps téléchargées sur iPhone à partir de l'App Store sont placées en « bac à sable »; elles ne peuvent donc pas accéder aux fichiers stockés par d'autres apps ni apporter de modifications à l'appareil sans avoir obtenu l'autorisation explicite de l'utilisateur ou de l'utilisatrice.

La meilleure couverture repose sur une combinaison de couches : le processus rigoureux de vérification des apps, qui permet d'éviter l'installation d'apps malveillantes, et les mesures de protection robustes de la plateforme, qui limitent les dégâts que ces apps peuvent causer. La sécurité intégrée à iOS assure une puissante protection – la meilleure de tous les appareils grand public. Elle n'est toutefois pas conçue pour préserver les gens des mauvais choix qu'ils pourraient être poussés à faire. Le processus de vérification App Review renforce les politiques de l'App Store qui visent à protéger les utilisateurs et utilisatrices contre les apps qui pourraient tenter de leur nuire ou les amener de façon malhonnête à faciliter l'accès à leurs données sensibles. Et dans l'éventualité plus grave où une app essaie de contourner les mesures de protection intégrées à l'appareil, App Review intervient dès le départ pour compliquer l'accès.

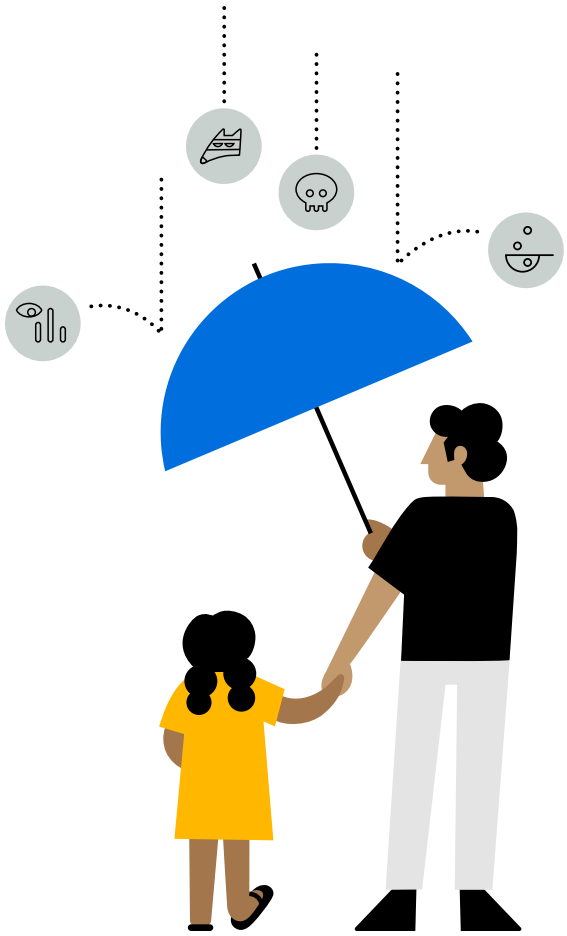
Les spécialistes de la sécurité sont unanimes : iPhone est l'appareil mobile le plus sûr qui soit. Les nombreuses couches de sécurité d'Apple procurent à notre clientèle un niveau inégalé de protection contre les logiciels malveillants et une tranquillité d'esprit sans pareil.

Le processus de vérification App Review

Par l'entremise du processus de vérification App Review, nous nous assurons que les apps proviennent de sources vérifiées et sont exemptes de composants malveillants connus. Nous veillons aussi à ce que les apps ne tentent pas de vous piéger en vous incitant à faire des achats non désirés ou à leur donner accès à vos données personnelles. Et nous passons tout le monde au crible, équipes de développement, utilisatrices et utilisateurs compris, expulsant systématiquement quiconque adopte un comportement inapproprié. Si le processus de vérification App Review n'empêche pas la distribution d'apps de mauvaise qualité, nous continuons sans cesse d'innover et d'améliorer les technologies, pratiques et procédés connexes.

Les mesures de protection des apps déployées par Apple en 2020

- **En moyenne, 100 000 nouvelles apps et mises à jour sont vérifiées chaque semaine** par une équipe de plus de 500 spécialistes qui examinent les apps dans différentes langues.
- **Près d'un million de nouvelles apps problématiques et un nombre similaire de mises à jour ont été rejetées ou supprimées :**
  - Plus de 150 000 étaient des apps indésirables ou des imitations, ou visaient à tromper le public
  - Plus de 215 000 contrevenaient aux directives en matière de respect de la vie privée
  - Plus de 48 000 comportaient des fonctionnalités cachées ou non documentées
  - Près de 95 000 étaient frauduleuses, principalement parce qu'elles intégraient des fonctionnalités de publicité-leurres visant à poser des gestes criminels ou autrement illicites
- **Apple a stoppé des transactions potentiellement frauduleuses représentant plus de 1,5 milliard de dollars.**
- **Apple a expulsé 470 000 équipes du programme Apple Developer pour des raisons liées à la fraude.** L'entreprise a aussi rejeté près de 205 000 tentatives d'inscription d'équipes de développement pour des questions de fraude.
- **Apple a désactivé 244 millions de comptes clients en raison d'activités frauduleuses et abusives, comme la publication de faux avis sur les produits.** Elle a également rejeté 424 millions de tentatives de création de comptes en raison de schémas de fraude et d'abus.



Le processus de vérification App Review permet à Jean d’avoir l’esprit tranquille quand il télécharge des apps

Les fonctionnalités de sécurité et de confidentialité de l’App Store offrent à Jean paix et tranquillité d’esprit quand il télécharge des apps pour lui ou pour sa fille. Il sait qu’Apple filtre 100 % des apps de l’App Store pour détecter les logiciels malveillants connus et que, par rapport aux autres appareils, il est extrêmement rare d’en retrouver sur iPhone.

En savoir plus sur les mesures de protection d'Apple

Pour en savoir plus sur la façon dont Apple assure votre sécurité et préserve votre confidentialité dans l'App Store, consultez **apple.com/ca/fr/app-store.**

Pour en savoir plus sur la façon dont Apple protège vos données de localisation, consultez le document **Location Services Privacy Overview (en anglais).**

Pour en savoir plus sur le contrôle parental sous iOS visitez **apple.com/ca/fr/families.**

Foire aux questions

Qu'est-ce que le téléchargement hors boutique?

Le téléchargement hors boutique est un processus qui consiste à télécharger et à installer une app sur un appareil mobile à partir d'une source autre que l'App Store officiel, comme un site web ou un magasin d'apps tiers. Afin d'assurer la sécurité et de protéger la confidentialité des propriétaires d'iPhone, nous avons dès le départ conçu l'appareil de façon à ne pas permettre ce type de téléchargement.

Qu'est-ce qu'un modèle de menace?

On appelle « modèle de menace » l'ensemble des attaques et des vulnérabilités contre lesquelles le public doit être protégé. Tous les appareils, personnes et environnements présentent des modèles de menace différents, et la sécurité doit être intégrée en tenant compte de cette réalité. L'App Store est une composante essentielle de la protection contre le modèle de menace d'iPhone. C'est une plateforme sûre qui permet de télécharger des apps vérifiées par Apple et développées par des entreprises connues qui sont tenues de respecter nos lignes directrices.

Autoriser le téléchargement hors boutique sur iPhone à partir de sites web et de magasins d'apps tiers pourrait-il nuire aux personnes qui téléchargent uniquement des apps depuis l'App Store?

Oui. En offrant des canaux de distribution supplémentaires, modifiant le modèle de menace et multipliant le nombre d'attaques potentielles, le téléchargement hors boutique sur iPhone mettrait tout le monde en danger – y compris ceux et celles qui font l'effort volontaire de se protéger en téléchargeant des apps via l'App Store seulement. L'autorisation du téléchargement hors boutique entraînerait un afflux de nouveaux investissements dans les attaques visant iPhone et inciterait les entités malveillantes à développer outils et expertise pour compromettre la sécurité d'iPhone à une échelle sans précédent. Cette expertise pour mener des attaques toujours plus sophistiquées permettrait aux entités malveillantes de cibler des magasins tiers (et l'App Store), faisant ainsi courir un risque accru à tout le monde. Par ailleurs, même les personnes qui préfèrent s'en tenir à l'App Store pour télécharger leurs apps pourraient être forcées d'utiliser une plateforme de tiers pour installer une app essentielle à leur emploi ou à leurs études si elle n'est pas offerte sur l'App Store. Ou encore, elles pourraient télécharger à leur insu une app sur une boutique de tiers qui tente de se faire passer pour l'App Store.

Qu’est-ce que le processus de vérification App Review d’Apple?

Nous combinons technologies poussées et expertise humaine pour examiner soigneusement chaque app et mise à jour afin d’évaluer si elles respectent les directives strictes de l’App Store en matière de confidentialité et de sécurité. Nous comptons sur le savoir-faire d’une équipe professionnelle dans les cas où la vérification automatisée n’est pas suffisante pour détecter des problèmes donnés (la violation de la vie privée ou les apps destinées aux enfants qui ne sont pas conformes, par exemple). Nos lignes directrices ont évolué au fil du temps en fonction des nouveaux défis et menaces, mais l’objectif est toujours demeuré le même : protéger les utilisateurs et les utilisatrices, et leur offrir la meilleure expérience possible sur l’App Store. En moyenne, 100 000 nouvelles apps et mises à jour sont vérifiées chaque semaine dans le monde entier par plus de 500 spécialistes.

Qu’est-ce qui est vérifié?

Toutes les apps et mises à jour qui souhaitent intégrer l’App Store sont soumises au processus de vérification App Review.

Quels contrôles parentaux sont offerts sur les appareils Apple?

Nous concevons des fonctionnalités qui permettent aux parents de contrôler la façon dont les enfants utilisent les appareils. Temps d’écran aide les parents à mieux comprendre le temps que leurs enfants passent dans les apps, sur le web et sur les appareils en général. Elle leur permet aussi d’établir une limite d’utilisation quotidienne par catégorie d’apps et de sites web. Et grâce à Demander d’acheter, les parents peuvent approuver ou refuser chacun des achats et des téléchargements initiés par leurs enfants directement à partir de leur appareil. La fonction empêche également tout achat subséquent pendant un délai de quinze minutes.

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

Ces nouvelles fonctionnalités offrent aux utilisateurs et aux utilisatrices un plus grand contrôle sur leurs données et leur vie privée. La transparence du suivi par les apps impose qu’une autorisation soit accordée à l’app avant qu’elle puisse effectuer un suivi des données dans les apps et sur les sites web d’entreprises tierces. Et avec les étiquettes de confidentialité de l’App Store, chaque app doit fournir aux utilisatrices et aux utilisateurs un résumé clair des pratiques de sécurité de l’équipe de développement, en offrant des renseignements clés sur la façon dont elle utilise leurs données.

Sources

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

2. ENISA. « Vulnerabilities - Separating Reality from Hype », *Agence de l'Union européenne pour la cybersécurité*, 24 août 2016.

3. GRIFFIN, Robert Jr. « Study on Mobile Device Security », *Département de la Sécurité intérieure des États-Unis*, 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.