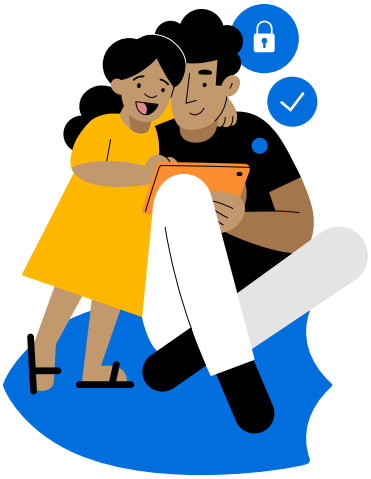


Construimos un ecosistema confiable para millones de apps

El importante papel de las protecciones del App Store

Junio de 2021

2007

"Estamos tratando de hacer dos cosas diametralmente opuestas a la vez: brindar una plataforma abierta y avanzada a los desarrolladores y, al mismo tiempo, proteger a los usuarios de iPhone de virus, malware y ataques a la privacidad, entre otras amenazas. No es una tarea simple".

Steve Jobs, 2007[1]

2016

"Utiliza únicamente la plataforma oficial de aplicaciones. Para reducir el riesgo de instalar apps maliciosas, los usuarios... no deben [descargar aplicaciones] de terceros. Los usuarios no deben hacer sideloading de aplicaciones (instalarlas de fuentes externas) si no provienen de una fuente legítima y auténtica".

Agencia de la Unión Europea para la Ciberseguridad (ENISA), 2016[2]

2017

"Las mejores prácticas identificadas para mitigar las amenazas de apps vulnerables son pertinentes para las aplicaciones maliciosas que invaden la privacidad. Además, los usuarios deben evitar (y las empresas deben prohibir en sus dispositivos) el sideloading de aplicaciones y el uso de tiendas de apps no autorizadas".

Informe del Departamento de Seguridad Nacional de Estados Unidos, 2017[3]

Hoy en día, nuestros teléfonos no son sólo teléfonos; almacenan parte de la información más confidencial sobre nuestra vida personal y profesional. Los llevamos con nosotros a todas partes y los usamos para comunicarnos con nuestros seres queridos, tomar y guardar fotos de nuestros hijos, consultar cómo llegar a un destino cuando estamos perdidos, contar nuestros pasos y enviar dinero a nuestras amistades. Nos acompañan cuando estamos felices y cuando estamos en dificultades.

Pensamos en esto al diseñar el iPhone. Creamos el App Store para ofrecer a los desarrolladores de todo el mundo un lugar donde crear apps innovadoras que puedan llegar a una comunidad global creciente y próspera de más mil millones de usuarios. Hay casi dos millones de apps en el App Store que los usuarios pueden descargar y cada semana se agregan miles. Dado el gran tamaño de la plataforma del App Store, garantizar la seguridad del iPhone fue de vital importancia para nosotros desde el principio. Los investigadores en seguridad coinciden en que el iPhone es el dispositivo móvil más seguro. Por eso nuestros usuarios pueden confiar en sus dispositivos para guardar sus datos más confidenciales. Integramos protecciones de seguridad líderes en la industria en el dispositivo y creamos el App Store, un lugar confiable donde los usuarios pueden descubrir y descargar apps de forma segura. En el App Store, las apps provienen de desarrolladores conocidos que han acordado seguir nuestros lineamientos y se distribuyen de forma segura a los usuarios, sin interferencias de terceros. Revisamos cada app y cada actualización para evaluar si cumplen con nuestros altos estándares. Este proceso, en el que trabajamos constantemente para mejorar, está diseñado para proteger a nuestros usuarios, ya que mantiene el malware, los ciberdelincuentes y los estafadores fuera del App Store. Las apps infantiles deben seguir estrictos lineamientos en relación con la recopilación de datos y la seguridad, diseñados para proteger a los niños. Además, deben estar estrechamente integradas con las funcionalidades de control parental de iOS.

En cuanto a la privacidad, no sólo creemos que es importante: la consideramos un derecho humano fundamental. Ese principio guía los altos estándares de privacidad que incluimos en nuestros productos. Recopilamos sólo los datos personales estrictamente necesarios para ofrecer un producto o servicio, le damos el control al usuario para otorgar permiso a las apps antes de que accedan a información confidencial y brindamos indicaciones claras cuando estas usan determinadas funcionalidades sensibles como el micrófono, la cámara o la ubicación del usuario. Como parte de nuestro compromiso continuo con la privacidad del usuario, dos de nuestras funcionalidades de privacidad más recientes (la información de privacidad en el App Store y la transparencia del rastreo en apps) ofrecen a nuestros usuarios un control sin precedentes sobre su privacidad, con mayor transparencia e información para permitirles tomar decisiones bien sustentadas. Gracias a todas estas protecciones, los usuarios pueden descargar cualquier app en el App Store con tranquilidad. Esta tranquilidad también beneficia a los desarrolladores, ya que pueden llegar a una amplia cantidad de usuarios que se sienten seguros al descargar sus apps.

Nuestro enfoque en la seguridad y la privacidad ha sido muy eficaz. Hoy en día, es sumamente inusual que un usuario encuentre malware en su iPhone.[5] Algunas

¿Sabías esto?

Apple revisa todas las apps y actualizaciones en el App Store para interceptar aquellas que podrían perjudicar a los usuarios. Esto incluye apps que tienen contenido inapropiado, invaden la privacidad de los usuarios o contienen malware conocido, es decir, software que se usa con propósitos maliciosos o peligrosos.

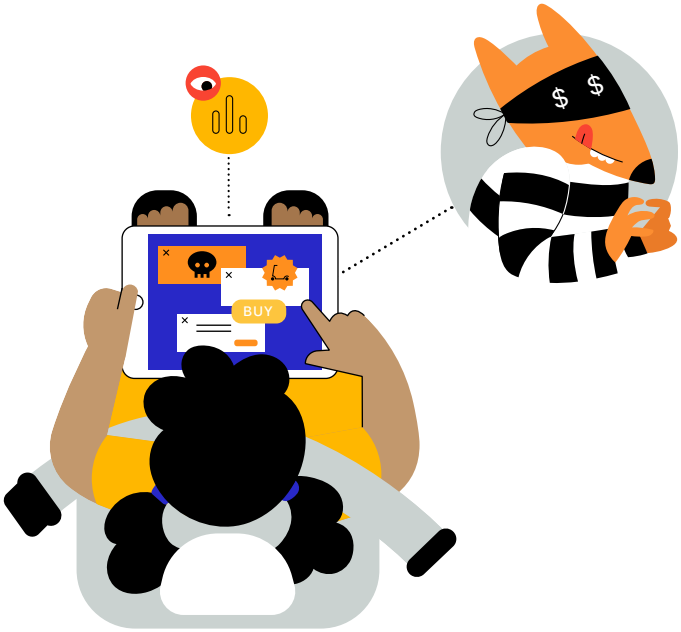
Un estudio determinó que los dispositivos con Android tenían 15 veces más infecciones de software malicioso que los iPhone. El motivo principal es que las apps de Android "se pueden descargar prácticamente desde cualquier lugar", mientras que los usuarios de iPhone sólo pueden descargar apps desde una fuente: el App Store.[4]

personas sugieren que deberíamos crear opciones para que los desarrolladores distribuyan sus apps fuera del App Store, a través de sitios web o tiendas de apps de terceros, un proceso que en inglés se denomina sideloading. Permitir este tipo de proceso degradaría la seguridad de la plataforma iOS y expondría a los usuarios a graves riesgos de seguridad, no sólo en tiendas de apps de terceros, sino también en el App Store. Debido al gran tamaño de la base de usuarios de iPhone y los datos confidenciales almacenados en sus teléfonos (fotos, datos de ubicación, información financiera y de salud), permitir el sideloading generaría una avalancha de nuevos esfuerzos centrados en atacar la plataforma. Actores malintencionados aprovecharían esta oportunidad para dedicar más recursos al desarrollo de ataques sofisticados dirigidos a usuarios de iOS. Esto ampliaría el conjunto de vulnerabilidades de seguridad y ataques, también conocido como "modelado de amenazas", contra los que todos los usuarios deben protegerse. Este mayor riesgo de ataques de malware compromete aún más la seguridad de todos los usuarios, incluso la de aquellos que sólo descargan apps del App Store. Además, incluso los usuarios que prefieren descargar únicamente del App Store podrían verse obligados a descargar una app que necesitan para el trabajo o la escuela desde tiendas de terceros si no está disponible en nuestra plataforma. También podrían ser víctimas de engaños para que descarguen apps de tiendas de terceros que se hagan pasar por el App Store.

Los estudios muestran que las tiendas de terceros para dispositivos Android, en las que las apps no están sujetas a revisión, son mucho más riesgosas y tienen más probabilidades de contener malware en comparación con las tiendas de apps oficiales.[6] Por consiguiente, los expertos en seguridad aconsejan a los consumidores que no usen tiendas de apps de terceros ya que son inseguras.[3,7] Permitir el sideloading abriría la puerta a un mundo donde los usuarios podrían verse obligados a aceptar estos riesgos porque algunas apps no están disponibles en el App Store, y los estafadores podrían engañar a los usuarios haciéndoles creer que están descargando apps del App Store de manera segura cuando no es así. El sideloading pondría en peligro a los usuarios frente a los estafadores, que aprovecharían las vulnerabilidades de las apps para engañarlos, atacar las funcionalidades de seguridad del iPhone y violar su privacidad. Además, sería más difícil para los usuarios confiar en Pedir la Compra, una funcionalidad de control parental que permite a los padres controlar las descargas de apps y compras que hacen sus hijos dentro de las apps, así como Tiempo en Pantalla, una funcionalidad que administra el tiempo que pasan ellos y sus hijos con los dispositivos. Los estafadores tendrían la oportunidad de engañar a los niños y sus padres al ocultar la naturaleza de sus apps, lo que haría que ambas funcionalidades sean menos efectivas.

En definitiva, los usuarios tendrían que estar constantemente atentos a las estafas, sin saber en quién o qué confiar y, por lo tanto, muchos usuarios descargarían menos apps de menos desarrolladores. Incluso estos últimos se volverían más vulnerables a amenazas de actores malintencionados, quienes podrían proporcionarles herramientas de desarrollo infectadas que contengan y propaguen malware. Los desarrolladores serían también más vulnerables a la piratería, lo que socavaría su capacidad de recibir pagos por su trabajo.

Veamos cómo la experiencia cotidiana de una familia que usa el iPhone cambiaría con el sideloading. Acompañaremos a Juan y su hija de siete años, Emma, mientras exploran este mundo más incierto.



Un juego instalado mediante sideloading elude los controles parentales

Emma le pregunta a Juan si puede usar un juego que le recomendaron sus amigas de la escuela. Juan lo busca en el App Store, pero sólo se puede descargar desde tiendas de apps de terceros. Esto preocupa a Juan, pero descarga el juego porque Emma tiene muchas ganas de probarlo y la tienda de apps de terceros afirma que es apropiado para niños. Más tarde, camino al parque, cuando Emma está jugando en el asiento trasero del auto, la app la bombardea con enlaces a sitios web externos y anuncios personalizados. Juan había agregado la información de su tarjeta de crédito para comprarle a Emma un kit inicial cuando descargó el juego, pero no se dio cuenta de que los controles parentales de Pedir la Compra no funcionarían con esta app. Mientras juega, Emma compra muchas vidas extra y objetos especiales, sin darse cuenta de que su papá no había aprobado esas compras. La app también tiene rastreadores de terceros integrados, que recopilan, analizan y venden los datos de Emma a empresas revendedoras de datos, aunque la app está orientada a niños.

Ataques reales a plataformas que permiten el sideloading

Se descubrió que apps de Android para niños participaban en prácticas de recopilación de datos que violaban su privacidad. Estas apps se siguen propagando y se dirigen a usuarios de Android en tiendas de apps de terceros, a pesar de que se eliminaron de Google Play.[8]

Actores malintencionados han ubicado anuncios inapropiados u obscenos en apps para niños.[9]

Ataques reales en plataformas que permiten sideloading

Se sabe que las apps instaladas mediante sideloading en Android realizan ataques de ransomware con bloqueo. Si estas apps maliciosas se instalan, bloquean el acceso de los usuarios a sus teléfonos o apuntan a sus fotos, a menos que estos acepten pagar un rescate.[10,11]

Se ha engañado a los usuarios de Android para que descarguen con métodos inseguros versiones falsas de apps como Netflix y Candy Crush. Tanto cuando se les da acceso como al explotar las vulnerabilidades de la plataforma, estas apps falsas pueden espiar a los usuarios de Android a través del micrófono; tomar capturas de pantalla de sus dispositivos; ver la ubicación, mensajes de texto y contactos; robar sus credenciales de inicio de sesión y hacer cambios en sus teléfonos.[12,13,14] También se las ha utilizado para robar credenciales bancarias y apropiarse de las cuentas bancarias de los usuarios.[15,16,17,18]

Una reciente estafa de ransomware consiste en una app para Android que se hace pasar por una aplicación de rastreo de contactos con COVID-19. Si se instala, encripta toda la información personal y deja un email de contacto para que el usuario pueda recuperar sus datos.[19]

Una app que se encuentra en tiendas de apps de Android de terceros engaña a los usuarios al hacerse pasar por una actualización del sistema. Una vez instalada, la app muestra la notificación "Buscando actualizaciones", mientras obtiene acceso y roba la información personal del usuario, como sus mensajes, contactos y fotos.[20,21]

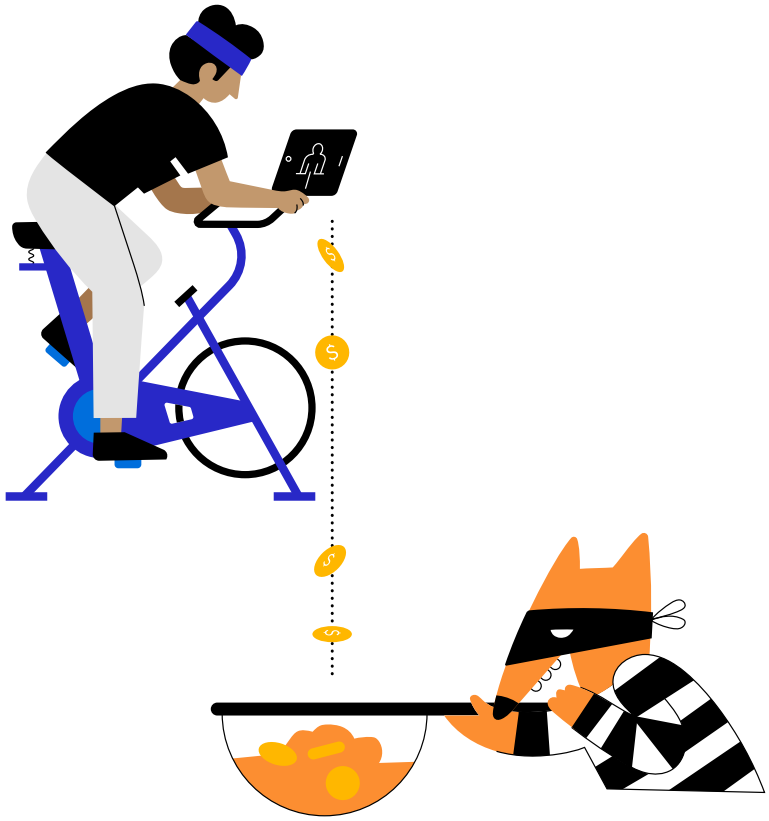
En el parque, la app de filtros falsa que Juan instaló mediante sideloading amenaza con borrar todas sus fotos a menos que pague el rescate

Cuando Emma y Juan están en el parque, este ve el anuncio de una app de filtros para selfies de un conocido desarrollador de apps y piensa que sería divertido usarla con su hija. El anuncio lo lleva a una página para descargar la app que se ve igual a la del desarrollador en el App Store, así que Juan cree que está protegido. No se da cuenta de que, en realidad, está descargando una versión falsa de la app desde una tienda de apps de terceros. Como Juan piensa que la app de filtros proviene de un desarrollador conocido y confiable, le da permiso para acceder a sus fotos. Sin embargo, cuando la aplicación comienza a ejecutarse, se da cuenta del error: la app amenaza con borrar todas las fotos de su rollo fotográfico a menos que introduzca la información de su tarjeta de crédito y pague un rescate. Gracias a las protecciones integradas del iPhone, Juan puede decidir qué apps tienen permiso para acceder a sus fotos, pero en este caso, la aplicación instalada mediante sideloading se hizo pasar por una app de filtros para selfies y lo engañó para obtener acceso a sus fotos.

Ataques reales en plataformas que permiten sideloading

Según algunos estudios, las apps pirateadas publicadas en tiendas de apps de terceros generan una pérdida de ingresos de miles de millones al año para los desarrolladores.[22]

Las apps pirateadas o ilegítimas están muy extendidas en Android. Estas incluyen apps de juegos que permiten hacer trampa (como una versión pirateada de Pokémon Go que puede simular la ubicación del usuario), apps modificadas para dar acceso pirateado a contenido o funciones premium, y apps con contenido para adultos o de apuestas ilegales.[23,24,25]

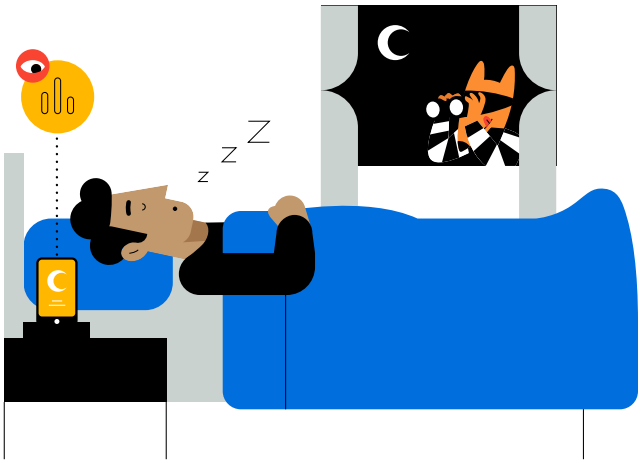


Sin saberlo, Juan descarga una app pirateada de una tienda de terceros

A una amiga de Juan le encanta una app de fitness que ha estado usando y le envía una invitación para que la pruebe, pero sólo funciona si la descarga a través de una tienda de terceros y no desde el App Store. Juan descarga la app y se registra para una suscripción mensual. Sin embargo, lo que ninguno de los dos sabe es que esa app estaba pirateada. Esto significa que el dinero que Juan paga cada mes no va al desarrollador que la diseñó y creó, sino a los estafadores que la robaron. Juan creyó que estaba haciendo lo correcto: apoyar al desarrollador de esa increíble app de fitness. En cambio, estaba llenando los bolsillos de los estafadores y, sin saberlo, apoyando un fraude que priva a los desarrolladores de sus ganancias.

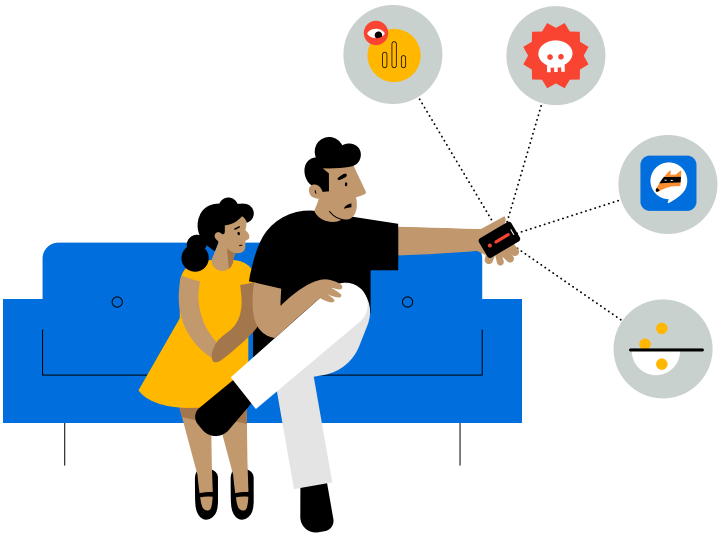
Más información sobre las protecciones de privacidad de Apple

Para obtener más información sobre cómo la transparencia del rastreo en apps y la información de privacidad en el App Store te dan control y transparencia sobre el uso y la recopilación de datos que hacen las apps, lee **Un día en la vida de tus datos** y visita **apple.com/mx/privacy/control.**



Una app instalada mediante sideloading viola la privacidad de Juan

Juan se enteró de una nueva app de seguimiento del sueño que le gustaría probar, pero no está disponible en el App Store. La descarga de una tienda de apps de terceros se registra con su dirección de email y comienza a usarla para monitorear la calidad de su sueño. La app afirma que mantiene los datos de uso y salud de los usuarios completamente privados y que no los vincula con información externa ni los comparte con terceros. Sin embargo, esta afirmación resulta ser absolutamente falsa. Como la app se instaló mediante sideloading, el desarrollador podía hacer lo que quisiera, así que la aplicación rastreó a Juan con su dirección de email sin pedirle permiso. De esta manera, el desarrollador pudo vincular los datos de Juan con información recopilada por otras apps y vender sus datos de salud a empresas revendedoras de datos, sin el permiso del usuario y sin preocuparse de que se lo impidieran.



Más de mil millones de personas usan el iPhone todos los días para realizar operaciones bancarias, administrar sus datos de salud y tomar fotos de sus familias. Esta gran base de usuarios sería un objetivo atractivo y lucrativo para ciberdelincuentes y estafadores. Si se permite el sideloading, se generaría una avalancha de nuevos esfuerzos centrados en atacar el iPhone, en una escala mucho mayor que en otras plataformas como la Mac. Los estafadores se verían motivados a desarrollar herramientas y conocimientos para atacar la seguridad de los dispositivos iPhone. El App Store está diseñado para detectar y bloquear los ataques que existen hoy en día, pero al cambiar el modelado de amenazas se eludirían estas protecciones. Los estafadores usarían entonces sus nuevas herramientas y conocimientos para atacar a tiendas de terceros y al App Store, lo que implicaría un mayor riesgo para todos los usuarios, incluso para quienes sólo descargan apps en nuestra plataforma. Los canales de distribución adicionales introducidos por el sideloading brindan a actores malintencionados mayores oportunidades de explotar las vulnerabilidades del sistema, lo que incentiva a los atacantes a desarrollar y diseminar más malware.

Esto significa que usuarios como Juan, que se habían acostumbrado a confiar en la seguridad y la protección del iPhone y el App Store, tendrían que estar constantemente atentos a los distintos engaños de los ciberdelincuentes y estafadores, sin saber en quién o qué confiar. En algunos casos, es posible que Juan no tuviera más remedio que arriesgarse a instalar mediante sideloading una app que no está disponible en el App Store desde una tienda de terceros o lo podrían engañar para hacerlo. En los casos más graves, las apps instaladas mediante sideloading que simulan ser algo que no son (por ejemplo, que afirman ser una actualización de software de Apple o disfrazan su página de descarga para que se vea como el App Store) podrían intentar romper las protecciones en el dispositivo del iPhone para obtener acceso a datos protegidos como los mensajes, las fotos y la ubicación. En vista de estos riesgos y estafas, Juan sería mucho más cauteloso a la hora de descargar apps. Al final, descargaría menos apps y se quedaría con las de un puñado de desarrolladores de confianza, lo que dificultaría que desarrolladores nuevos y más pequeños lleguen a los usuarios con apps novedosas e innovadoras. Ya no tendría la tranquilidad de saber que las apps de su iPhone son las opciones más seguras para él y su hija.

¿Sabías esto?

Es más probable que los usuarios que están preocupados por su seguridad y privacidad descarguen menos apps y las eliminen de sus dispositivos.[26,27,28] Un ecosistema menos seguro, en el que los usuarios no se sienten protegidos al descargar apps, puede hacer que sean menos propensos a probar apps nuevas e innovadoras, o bien a arriesgarse con apps de desarrolladores nuevos o poco conocidos. Esto podría frenar el crecimiento de la economía de las apps, perjudicando tanto a usuarios como a desarrolladores.

Las capas de seguridad de Apple y la revisión de apps protegen a Juan, Emma y sus dispositivos

Para proteger a los usuarios de iOS de apps maliciosas y brindar la mejor seguridad de plataformas del mundo, adoptamos un enfoque múltiple, con muchas capas de protección. iOS plantea desafíos de seguridad únicos porque los usuarios descargan apps nuevas constantemente en sus dispositivos y porque los dispositivos iOS tienen que ser lo suficientemente seguros como para que los niños los usen sin supervisión. Esto significa que adoptamos un enfoque más estricto para la seguridad en el iPhone en comparación con la Mac, ya que los usuarios, así como sus comportamientos y expectativas, son diferentes.

- **Al igual que en la Mac, usamos software automatizado para escanear apps en busca de malware conocido. De esta manera, evitamos que lleguen al App Store y perjudiquen a los usuarios.**
- **Además, los desarrolladores de apps deben enviar una descripción de la app y sus funcionalidades.** Un equipo de expertos revisa esta información para verificar su precisión durante el proceso de revisión de apps y se presenta a los usuarios cuando estos evalúan si quieren descargar o no una app. Este proceso crea una importante barrera contra las estafas más comunes que se usan para distribuir malware, cuando simula que es una app conocida o afirma que ofrece funcionalidades atractivas que en realidad no proporciona.
- Además de verificar si las funcionalidades de la app cumplen con lo descrito y si la página en el App Store es correcta, **los expertos también verifican manualmente que la app no solicite acceso innecesario a datos confidenciales y evalúan que las apps infantiles cumplan con estrictas normas de seguridad y recopilación de datos.**
- **En los casos en que una app llega al App Store, pero luego se descubre que viola nuestros lineamientos, trabajamos con el desarrollador para resolver rápidamente el problema.** En casos peligrosos que involucran fraude y actividad malintencionada, la app se elimina inmediatamente del App Store, y se puede notificar a los usuarios que la descargaron sobre el comportamiento malicioso de la app.
- **Si un usuario tiene un problema con una app descargada del App Store, AppleCare está disponible para brindar soporte y emitir reembolsos.**

El objetivo de la revisión de apps es garantizar que las apps del App Store sean confiables y que la información proporcionada en la página de una app

en el App Store represente con exactitud cómo funciona y a qué datos tendrá acceso. Mejoramos constantemente este proceso, de manera que actualizamos y perfeccionamos nuestras herramientas y metodología de forma continua.

Una vez que los usuarios descargan una app a través del App Store, pueden controlar cómo funciona y los datos a los que tiene acceso, gracias a funcionalidades como la transparencia del rastreo en apps y los permisos. Los padres pueden controlar aún más lo que sus hijos compran con la funcionalidad Pedir la Compra, el tiempo que pasan en ciertas categorías de apps con Tiempo en Pantalla y los datos que comparten. Los usuarios también pueden administrar de forma centralizada todos los pagos relacionados con la app, así como consultar y cancelar fácilmente suscripciones que se pagan dentro de la app. Estos controles no se podrían aplicar en su totalidad en apps instaladas mediante sideloading.

Además de las protecciones proporcionadas por la revisión de apps, diseñamos el hardware y software de nuestros dispositivos para brindar una última línea de defensa en caso de que una aplicación dañina se descargue en el dispositivo. Por ejemplo, las apps descargadas en el iPhone desde el App Store están en una zona protegida, lo que significa que no pueden acceder a archivos almacenados por otras apps o hacer cambios en el dispositivo a menos que el usuario lo permita explícitamente.

La mejor defensa se basa en una combinación de todas las capas: una revisión de apps sólida, que ayuda a prevenir la instalación de aplicaciones maliciosas, y protecciones fuertes para la plataforma, que limitan los daños que estas apps pueden infligir. La seguridad integrada en iOS brinda a los usuarios protecciones poderosas, que son las mejores de cualquier dispositivo, pero no están diseñadas para proteger al usuario contra decisiones que podría tomar mediante engaños. La revisión de apps refuerza las políticas del App Store diseñadas para proteger a los usuarios de aplicaciones que podrían intentar perjudicarlos o engañarlos para obtener acceso a información confidencial. Además, en los casos más graves de aplicaciones maliciosas que intentan eludir las protecciones del dispositivo, la revisión de apps les dificulta aún más el acceso a los dispositivos de los usuarios en primer lugar.

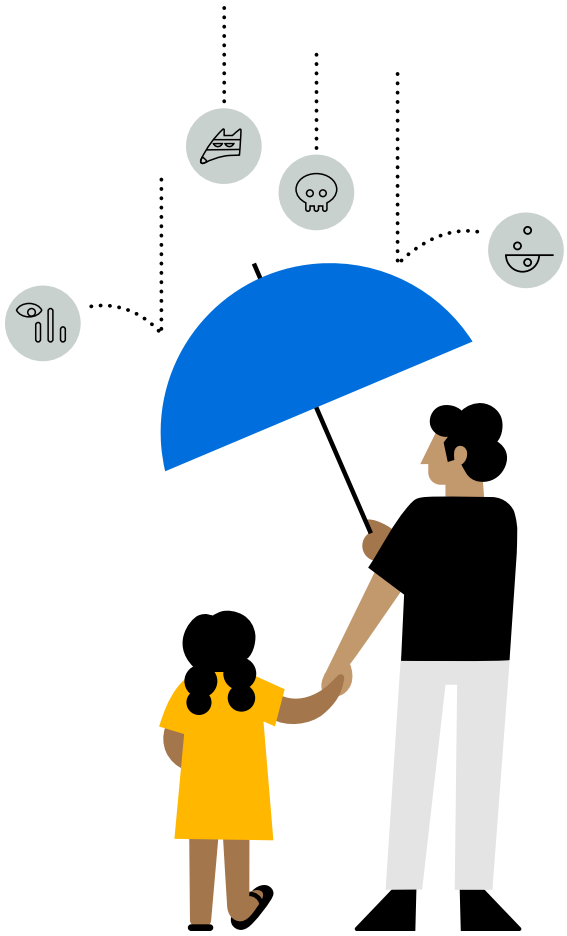
En conclusión, los expertos en seguridad coinciden en que el iPhone es el dispositivo móvil más seguro. Las múltiples capas de seguridad de Apple brindan a los usuarios un nivel incomparable de protección ante software malicioso, lo que les da mayor tranquilidad.

Revisión de apps

A través del proceso de revisión de apps, trabajamos para asegurarnos de que las apps provengan de fuentes verificadas y estén libres de componentes maliciosos conocidos. También comprobamos que no intenten engañarte para que realices compras no deseadas o les des acceso a tu información personal. Examinamos tanto a desarrolladores como usuarios y expulsamos a los que no actúan apropiadamente. Si bien los procesos de revisión de apps no evitan la distribución de todas las apps de baja calidad, continuamos innovando y mejorando su tecnología, prácticas y procesos.

Las protecciones de apps de Apple en acción en 2020

- **En promedio, un equipo de 500 expertos exclusivos revisa 100,000 nuevas apps y actualizaciones cada semana**, en diferentes idiomas.
- **Casi un millón de nuevas apps problemáticas y una cantidad similar de actualizaciones se rechazaron y eliminaron:**
  - Más de 150,000 por ser falsas o imitaciones, o por engañar a los usuarios
  - Más de 215,000 por violar las normas de privacidad
  - Más de 48,000 por contener funcionalidades ocultas o no registradas
  - Aproximadamente 95,000 por infracciones fraudulentas, principalmente por incluir funcionalidades de tipo "bait and switch" (cebo y cambio) para cometer actos delictivos u otras acciones prohibidas
- **Apple detuvo más de 1,500 millones de dólares en transacciones potencialmente fraudulentas.**
- **Apple expulsó a 470,000 equipos del Apple Developer Program por motivos relacionados con fraudes.** También rechazó casi 205,000 intentos de inscripción de desarrolladores por sospechas de fraude.
- **Apple desactivó 244 millones de cuentas de clientes debido a actividades fraudulentas y abusivas, incluidas reseñas falsas.** También rechazó 424 millones de intentos de creación de cuentas a causa de patrones fraudulentos y abusivos.



La revisión de apps le da tranquilidad a Juan a la hora de descargar apps

Las funcionalidades de privacidad y seguridad del App Store le dan tranquilidad a Juan cuando descarga apps para él y su hija. Sabe que Apple analiza el 100% de las apps en el App Store en busca de malware conocido y que, en comparación con otros dispositivos, es extremadamente raro que los usuarios encuentren malware malicioso en el iPhone.

Más información sobre las protecciones de Apple

Para obtener más información sobre cómo Apple protege tu seguridad y privacidad en el App Store, visita **apple.com/mx/app-store.**

Para obtener más información sobre cómo Apple protege tus datos de ubicación, lee el **informe técnico sobre la privacidad de Localización.**

Para obtener más información sobre el control parental en iOS, visita **apple.com/mx/families.**

Preguntas frecuentes

¿Qué es sideloading?

Sideloading es el proceso de descargar e instalar apps en un dispositivo móvil desde una fuente que no sea el App Store oficial, como un sitio web o una tienda de apps de terceros. Para proteger la seguridad y privacidad de los usuarios, desde el principio diseñamos el iPhone para no permitir que los usuarios hagan sideloading.

¿Qué es un modelado de amenazas?

Un modelado de amenazas es el conjunto de ataques y vulnerabilidades contra los que se debe proteger a los usuarios. Diferentes dispositivos, usuarios y entornos tienen diversos modelados de amenazas, por lo que hay que tenerlo en cuenta al desarrollar la seguridad. El App Store es un componente crucial para la protección del iPhone contra el modelado de amenazas. Es un lugar confiable para que los usuarios descarguen de forma segura apps revisadas por Apple, de desarrolladores conocidos que deben cumplir con los lineamientos de Apple.

¿Permitir el sideloading desde sitios web y tiendas de apps de terceros en el iPhone amenazaría a los usuarios que sólo descargan apps del App Store?

Sí. Al proporcionar canales de distribución adicionales, cambiar el modelado de amenazas y ampliar el universo de posibles ataques, el sideloading en el iPhone pondría a todos los usuarios en riesgo, incluso a aquellos que, en un esfuerzo deliberado para protegerse, descargan apps sólo a través del App Store. Permitir el sideloading generaría una avalancha de nuevos esfuerzos centrados en atacar el iPhone, ya que incentivaría a actores malintencionados a desarrollar herramientas y conocimientos para atacar la seguridad de los dispositivos iPhone en una escala sin precedentes. Al adquirir pericia en ataques cada vez más sofisticados, los actores malintencionados apuntarían tanto a tiendas de terceros como al App Store, lo que significaría un enorme riesgo para todos los usuarios. Además, incluso los usuarios que prefieren descargar únicamente del App Store podrían verse obligados a descargar una app que necesitan para el trabajo o la escuela desde tiendas de terceros si no está disponible en nuestra plataforma. También podrían ser víctimas de engaños para que descarguen apps de tiendas de terceros que se hagan pasar por el App Store.

¿Qué es el proceso de revisión de apps de Apple?

Usamos una combinación de tecnología sofisticada y pericia humana para revisar cuidadosamente cada app y cada actualización, con el fin de evaluar si cumplen con los lineamientos estrictos del App Store sobre privacidad y seguridad. Confiamos en la pericia humana cuando la revisión automatizada no es suficiente para detectar problemas específicos, como violaciones de privacidad o apps infantiles que no cumplen con nuestras estrictas normas. Los lineamientos han cambiado con el tiempo para responder a nuevas amenazas y desafíos, con el objetivo de proteger a los usuarios y brindarles la mejor experiencia en el App Store. En promedio, un equipo de 500 expertos exclusivos de todo el mundo revisa 100,000 nuevas apps y actualizaciones cada semana.

¿Qué es lo que se revisa?

Todas las apps y actualizaciones enviadas al App Store están sujetas al proceso de revisión de apps.

¿Qué controles parentales están disponibles en los dispositivos Apple?

Diseñamos funcionalidades que permiten a los padres tener el control sobre el uso que sus hijos hacen de los dispositivos. Tiempo en Pantalla les brinda información precisa sobre el tiempo que los niños pasan en apps y sitios web, y usando los dispositivos en general. Tiempo en Pantalla también permite a los padres establecer el tiempo que sus hijos pueden pasar en determinadas apps y sitios web cada día. Además, con Pedir la Compra, los padres pueden aprobar o rechazar las compras y descargas de apps infantiles directamente desde su dispositivo. Pedir la Compra tiene un tiempo de espera de 15 minutos para impedir compras posteriores.

¿Qué son la transparencia del rastreo en apps y la información de privacidad en el App Store?

Estas nuevas funcionalidades brindan al usuario mayor control sobre sus datos y privacidad. La transparencia del rastreo en apps requiere que las aplicaciones obtengan el permiso del usuario antes de rastrear sus datos en apps o sitios web de otras empresas. Con la información de privacidad en el App Store, exigimos que todas las apps del App Store brinden a los usuarios un resumen simple de las prácticas de privacidad del desarrollador, con información clave sobre el uso que las apps hacen de sus datos.

Referencias

1. Jobs, Steve, "Third Party Applications on the iPhone", 17 de octubre de 2007, consultado a través de tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

2. ENISA, "Vulnerabilities - Separating Reality from Hype", *European Union Agency for Cybersecurity*, 24 de agosto de 2016.

3. Griffin, Robert Jr., "Study on Mobile Device Security", *Departamento de Seguridad Nacional de Estados Unidos*, abril de 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 de marzo de 2019.

6. Symantec, "Internet Security Threat Report, Volume 23", abril de 2018.

7. Golovin, Igor, "Malware in Minecraft mods: story continues", *Kaspersky*, 9 de junio de 2021.

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

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices", *ThreatPost*, 24 de junio de 2020.

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app", *WeLiveSecurity por ESET*, 18 de marzo de 2021.

13. Desai, Shivang, "SpyNote RAT posing as Netflix app", *Zscaler*, 23 de enero de 2017.

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

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

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

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on", *WeLiveSecurity* por ESET, 11 de diciembre de 2018.

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World", *Cybereason*, 1 de julio de 2020.

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

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

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

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

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

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit", *TorrentFreak*, 8 de enero de 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 de diciembre de 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*, 1 de febrero de 2017.