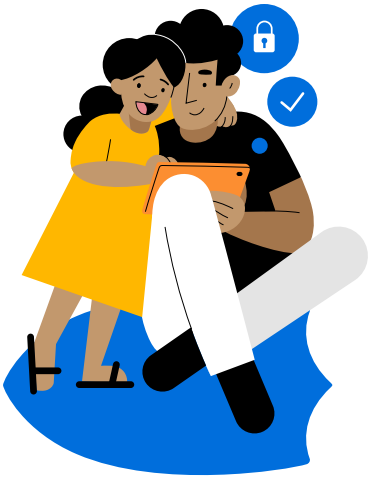


Как построить надёжную экосистему для миллионов приложений

Роль инструментов безопасности, которые использует App Store

Июнь 2021 г.

2007

«Мы пытаемся решить две противоположные задачи: дать разработчикам открытую и современную платформу, одновременно защищая пользователей iPhone от вирусов, вредоносного ПО и так далее. Это очень непросто».

Стив Джобс, 2007 г.[1]

2016

«Используйте только официальные платформы для поиска приложений. Пользователи не должны… [скачивать приложения] из сторонних источников во избежание установки вредоносного ПО. Пользователю не следует скачивать приложения, если нет уверенности в надёжности их источника».

Европейское агентство по кибербезопасности (ENISA), 2016 г.[2]

2017

«Рекомендации по защите от угроз, возникающих при использовании уязвимого ПО, также актуальны для вредоносного ПО и приложений, в которых не соблюдаются требования к защите личных данных. Пользователи не должны скачивать непроверенные приложения и пользоваться сомнительными магазинами приложений, а компании должны запрещать такую практику на корпоративных устройствах».

Отчёт Министерства внутренней безопасности США, 2017 г.[3]

На смартфонах хранится множество конфиденциальных данных о работе и личной жизни пользователей. Телефоны сопровождают нас повсюду. С их помощью мы общаемся с близкими, фотографируем своих детей, находим дорогу, если потерялись, считаем шаги и отправляем деньги друзьям. Смартфоны всегда с нами — и в счастливые моменты, и в грустные.

Мы продумали принципы обеспечения безопасности ещё при разработке iPhone. App Store даёт разработчикам со всего мира платформу для публикации инновационных приложений — такую, где они будут доступны растущему и развивающемуся международному сообществу более чем из миллиарда пользователей. В App Store представлено почти два миллиона приложений, и тысячи новых добавляются каждую неделю. Учитывая такие масштабы, нам с самого начала было чрезвычайно важно позаботиться о безопасности владельцев iPhone. Исследования показывают, что iPhone — одно из самых защищённых мобильных устройств, и наши пользователи могут смело доверить ему свои персональные данные. Мы встроили в устройства передовые средства безопасности, а также создали App Store — надёжную платформу, позволяющую искать и скачивать только проверенные приложения. Публиковать свои приложения в App Store могут только те разработчики, которых мы проверили, — при этом все они согласились соблюдать требования платформы. Все приложения безопасны и предоставляются пользователям без участия третьих сторон. Мы оцениваем каждое приложение и каждое обновление на предмет соответствия нашим стандартам. Эта процедура постоянно совершенствуется и помогает защитить пользователей, не допуская появления вредоносного ПО, киберпреступников и других мошенников в App Store. В приложениях для детей должны соблюдаться особо строгие правила сбора данных и усиленные меры безопасности. Кроме того, такие приложения должны тесно взаимодействовать со средствами родительского контроля, встроенными в iOS.

Для нас конфиденциальность не просто важна — мы считаем её одним из основных прав человека. Поэтому мы с таким вниманием относимся к средствам защиты конфиденциальности в наших продуктах. Мы собираем только те данные, которые необходимы для работы наших устройств и сервисов. Мы даём пользователю возможность выбирать, что разрешить приложению, а что — нет. Если приложение использует микрофон, камеру или службы геолокации, это сразу отображается на экране устройства.

Знаете ли вы?

Apple проверяет все приложения и их обновления перед публикацией в App Store. Это помогает изолировать ПО, способное навредить пользователям. В частности, мы запрещаем публиковать приложения, которые содержат неприемлемый контент, нарушают правила конфиденциальности или содержат известное вредоносное ПО — то есть программный код, который используется для достижения незаконных или опасных целей.

Исследование показало, что устройства Android в 15 раз чаще подвергаются заражению вредоносным ПО, чем iPhone. Главная причина состоит в том, что приложения для Android «можно скачать практически откуда угодно», тогда как рядовые пользователи iPhone могут скачивать приложения только из App Store.[4]

Мы постоянно совершенствуем средства защиты конфиденциальности. Две наши новые функции — информация о конфиденциальности приложения, которая теперь размещается в App Store, и запросы на отслеживание данных в приложениях — дают пользователям беспрецедентный уровень контроля и помогают делать осознанный выбор. Благодаря этому наши пользователи могут без опасений скачивать приложения из App Store. Это является преимуществом и для разработчиков: они получают доступ к широкой аудитории, которая не боится скачивать их приложения.

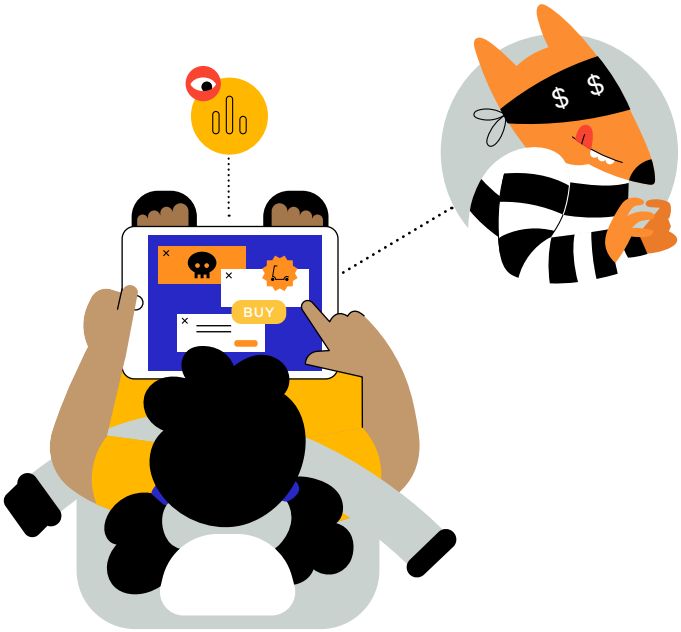
Такой подход к безопасности и конфиденциальности доказал свою высокую эффективность. Сейчас пользователи iPhone крайне редко сталкиваются с вредоносным ПО.[5] Существует мнение, что мы должны позволить разработчикам распространять свои приложения за пределами App Store — через сайты или сторонние магазины приложений. Но такая практика снизит безопасность платформы iOS и поставит под угрозу не только тех, кто будет пользоваться сторонними магазинами, но и тех, кто скачивает приложения из App Store. Устройствами iPhone пользуются очень многие, и на них хранятся конфиденциальные данные, например фотографии, сведения о местоположении, здоровье, финансах пользователя. Разрешив использование сторонних магазинов приложений, мы спровоцируем новую волну финансирования атак на наши платформы. Злоумышленники постараются воспользоваться появившейся возможностью, вложат ещё больше ресурсов в разработку новых схем взлома устройств iOS и тем самым расширят круг уязвимостей, от которых нужно защищать всех наших пользователей. Такой риск внедрения вредоносного ПО ставит под угрозу всех пользователей, в том числе тех, кто скачивает приложения только из App Store. И даже тех, кто предпочитает использовать App Store, можно вынудить скачать необходимое приложение со стороннего ресурса: достаточно просто сделать его недоступным на нашей платформе. Или обмануть: сделать сторонний магазин похожим на App Store.

Исследования показали, что сторонние магазины приложений для Android, в которых приложения не проходят проверку, связаны с более высокими рисками и чаще приводят к заражению вредоносным ПО — по сравнению с официальными магазинами.[6] Эксперты по безопасности не рекомендуют пользоваться сторонними магазинами.[3,7] Разрешив размещать приложения для iOS в них, мы можем поставить своих пользователей в такое положение, когда они будут вынуждены брать на себя риск, потому что нужного приложения просто нет в App Store.

А у злоумышленников появится возможность подделать App Store и убедить пользователей, что они находятся в защищённом магазине. Сторонние платформы откроют дорогу для мошенников, которые смогут пользоваться уязвимостями в приложениях, обманывать пользователей, осуществлять атаки на системы безопасности iPhone и красть личные данные пользователей. Кроме того, будет сложнее пользоваться теми средствами родительского контроля, которые ограничивают скачивание приложений и покупки в них. Сложнее будет следить за соблюдением правил Экранного времени. У мошенников будет возможность ввести детей и их родителей в заблуждение, скрыв происхождение скачанного приложения, и сделать функции защиты детей менее эффективными.

В итоге пользователи будут во всём подозревать мошенничество. Они не будут уверены в том, кому можно доверять, а значит, будут скачивать приложения реже и у меньшего числа разработчиков. Сами разработчики также станут более уязвимыми перед лицом угроз, потому что у злоумышленников будет возможность заразить их инструменты вредоносным ПО, которое они непреднамеренно станут распространять дальше. При этом вырастут объёмы пиратского скачивания, и разработчики начнут терять доходы.

Давайте посмотрим, как изменится повседневная жизнь простой семьи, если мы разрешим скачивать приложения для iPhone со сторонних ресурсов. Мы проведём один день с Андреем и его 7-летней дочкой Катей, чтобы посмотреть, насколько уверенно они будут себя чувствовать.



Игра, скачанная со стороннего ресурса, обходит средства родительского контроля

Катя спрашивает папу, можно ли ей скачать игру, о которой рассказывали её школьные друзья. Андрей пытается найти игру в App Store, но выясняется, что разработчик разместил её только на сторонних ресурсах. Это кажется Андрею подозрительным, но он всё же скачивает игру: Катя очень её просила, а в описании указано, что это приложение для детей. По дороге в парк Катя включает игру, сидя на заднем сиденье автомобиля. Приложение атакует её ссылками на внешние веб-сайты и таргетированной рекламой. Покупая стартовый пакет игры, Андрей указал данные своей кредитной карты, однако он не предполагал, что средства родительского контроля, ограничивающие дополнительные покупки, не сработают, потому что игра скачана из стороннего магазина. Во время игры Катя покупает много дополнительных ходов и других игровых элементов. Она не понимает, что совершает реальные покупки и что её папа не давал на них разрешение. Кроме того, в эту игру встроены трекеры, которые собирают и анализируют данные Кати, чтобы затем продать их брокерам, — несмотря на то, что приложение было помечено как детское.

Реальные атаки на платформы, позволяющие скачивать приложения со сторонних ресурсов

Как оказалось, некоторые детские приложения для Android собирают и обрабатывают данные, нарушая конфиденциальность ребёнка. Эти приложения остаются доступны через сторонние ресурсы, и пользователи Android продолжают их скачивать даже несмотря на то, что нарушителей удалили из Google Play.[8]

Нарушители размещали неподходящую и даже недопустимую рекламу в приложениях, предназначенных для детей.[9]

Реальные атаки на платформы, позволяющие скачивать приложения со сторонних ресурсов

Известно, что приложения для Android, скачанные со сторонних ресурсов, могут содержать программы-вымогатели. Это вредоносное ПО, которое блокирует устройство или грозится распространить личные фото пользователя, если тот не заплатит выкуп.[10,11]

Пользователей Android обманом убеждают скачать поддельные версии известных приложений, таких как Netflix или Candy Crush. Эти приложения получают доступ от самого пользователя либо используют уязвимости и крадут данные: подключаются к микрофону, делают снимки экрана, следят за местоположением, просматривают текстовые сообщения и контакты, перехватывают учётные данные, вносят изменения в настройки устройства.[12,13,14] Есть также приложения, которые крадут банковские данные пользователей и получают доступ к их банковским счетам.[15,16,17,18]

В одной из недавних атак на Android использовалось приложение, напоминающее инструмент для отслеживания контактов с носителями COVID-19. При установке оно шифровало персональные данные пользователя и оставляло адрес электронной почты, на который нужно написать, чтобы восстановить доступ.[19]

В парке приложение-клон, которое Андрей скачал со стороннего ресурса, угрожает удалить все фотографии, если он не заплатит выкуп

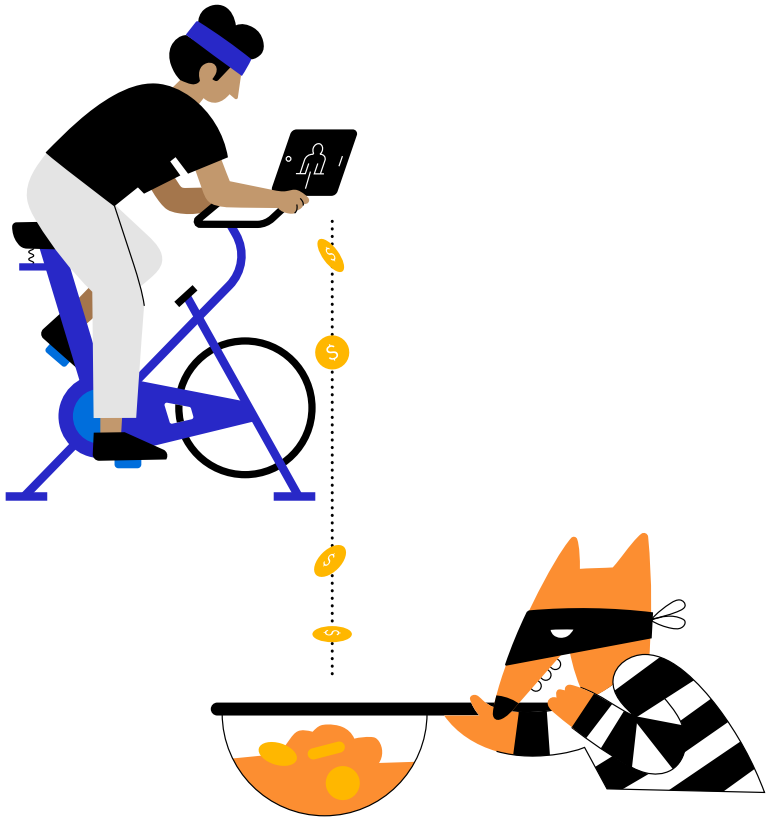
Пока Андрей с дочкой отдыхал в парке, он увидел рекламу фильтра для селфи. Это было приложение от известного разработчика, и Андрей подумал, что будет забавно попробовать его в деле. Коснувшись объявления, он перешёл на страницу, очень похожую на страницу разработчика в App Store — Андрей не понял, что на самом деле скачивает приложение-клон из стороннего магазина приложений. Поскольку Андрей решил, что фильтр скачан из официального магазина и сделан известным разработчиком, он предоставил приложению доступ к своим фотографиям. Когда приложение открылось, Андрей понял, что совершил ошибку. На экране появилось сообщение с угрозой удалить все фото, если он не введёт данные кредитной карты и не заплатит выкуп. Инструменты, встроенные в iPhone, позволяют Андрею самому решать, у каких приложений будет доступ к фотографиям, но в данном случае мошенники обманом получили этот доступ, убедив пользователя, что перед ним обычный фильтр для селфи.

Реальные атаки на платформы, позволяющие скачивать приложения со сторонних ресурсов

Одно из приложений, размещённых на сторонних ресурсах, было похоже на обновление системы. После его установки появлялось сообщение: «Идёт поиск обновлений». При этом приложение получало доступ к личным данным пользователя, в том числе к сообщениям, контактам и фотографиям.[20,21]

Исследование показало, что из-за пиратских копий приложений, публикуемых на сторонних ресурсах, разработчики ежегодно теряют миллиарды долларов дохода.[22]

Пиратские копии и другое незаконное ПО для Android встречается часто. Среди таких приложений есть игры, изменённые мошенниками (например, пиратская версия Pokémon Go способна моделировать местоположение пользователя), приложения, дающие незаконный доступ к премиум-контенту и расширенным функциям, запрещённые азартные игры и приложения, содержащие контент для взрослых.[23,24,25]

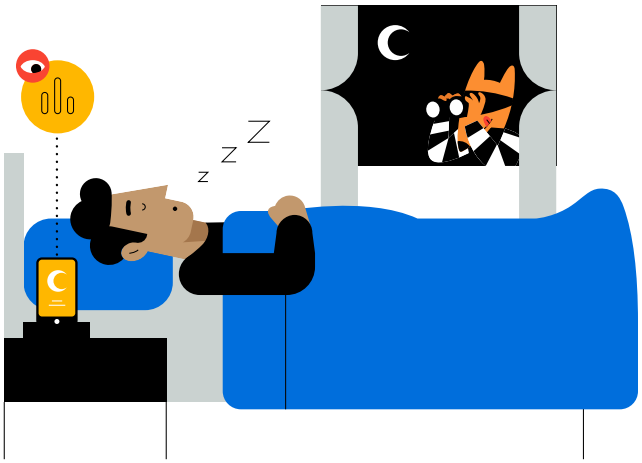


Андрей случайно скачал пиратское приложение со стороннего ресурса

Коллега Андрея посоветовала ему приложение для фитнеса, которым она пользуется. Подруга прислала Андрею реферальную ссылку на приложение. Но ссылка ведёт на сторонний ресурс, а не на App Store. Андрей скачал приложение и оформил подписку на месяц. Ни он, ни его знакомая не знали, что на самом деле приложение было пиратским. То есть ежемесячные платежи пользователей уходят не разработчику, а мошенникам, которые украли это приложение. Андрей считал, что поступает правильно, — поддерживает разработчика, создавшего отличное приложение для фитнеса, а на самом деле перечислял свои средства злоумышленникам, которые посредством незаконной схемы лишают разработчика доходов.

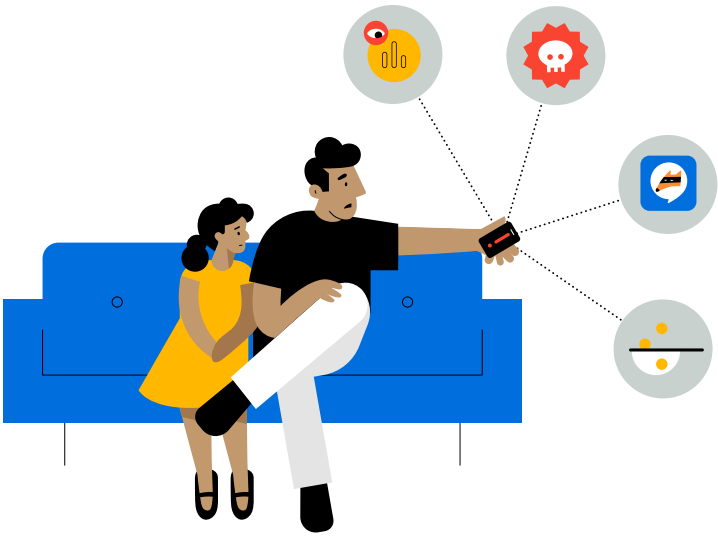
Подробнее о средствах защиты конфиденциальности в продуктах Apple

Чтобы больше узнать о том, как Прозрачность отслеживания и информация о конфиденциальности приложения, добавленная в App Store, помогают сохранять контроль над личными данными, посмотрите документ **«Один день из жизни ваших данных»** и изучите сведения на странице **apple.com/ru/privacy/control**.



Приложение, скачанное со стороннего ресурса, незаконно использует личные данные

Андрей услышал о новом приложении для оценки качества сна, решил его попробовать, но не нашёл в App Store. Он скачал приложение со стороннего ресурса, зарегистрировал учётную запись на свой адрес электронной почты и начал следить за тем, как спит по ночам. Андрей прочитал, что данные о здоровье и об использовании приложения полностью защищены, не привязываются к другим данным и не передаются третьим лицам. Но оказалось, что это неправда. Поскольку приложение было размещено на стороннем ресурсе, разработчик решил не соблюдать требования к конфиденциальности и стал отслеживать действия Андрея по адресу электронной почты, не спросив разрешения. Разработчик смог связать полученную информацию с данными из других приложений и продать медицинские сведения брокерам, не заботясь о согласии пользователя и не боясь, что кто-то его остановит.



Более миллиарда людей во всём мире ежедневно используют iPhone. Они оплачивают покупки и переводят денежные средства, хранят на устройстве данные о своём здоровье и фотографии близких. Завладеть такой огромной базой пользователей — цель для киберпреступников и мошенников. Поэтому, если мы разрешим скачивать приложения со сторонних ресурсов, то спровоцируем поток инвестиций в атаки на iPhone, и эти средства будут гораздо больше, чем то, что тратится сейчас для подготовки атак на другие платформы, в том числе на Mac. У злоумышленников будет стимул разрабатывать инструменты и набираться опыта в области взлома систем безопасности iPhone. В App Store есть средства, помогающие блокировать и предотвращать известные виды атак, но если мошенники изменят свои модели угроз, эффективность защиты может снизиться. Далее преступники начнут применять новые средства против сторонних магазинов, и это создаст дополнительные риски для всех наших пользователей — в том числе для тех, кто скачивает приложения только из App Store. Чем больше каналов распространения приложений появляется, тем больше у злоумышленников возможностей воспользоваться какой-нибудь уязвимостью — и тем сильнее их желание создавать вредоносное ПО.

Такие пользователи, как Андрей, привыкшие полагаться на безопасность iPhone, и сама платформа App Store, будут вынуждены постоянно следить за новыми угрозами со стороны киберпреступников и перестанут доверять разработчикам. Возможно, однажды у Андрея не будет выбора, и ему придётся скачать приложение со стороннего ресурса, или его убедят сделать это обманом. В самых опасных случаях, поддельное приложение, похожее на обновление для iPhone или скачанное со страницы, напоминающей App Store, получит доступ к конфиденциальным данным: сообщениям, фотографиям, сведениям о местоположении пользователя.

Зная обо всех этих рисках, Андрей станет гораздо осторожнее. Он будет пользоваться только приложениями нескольких избранных разработчиков, которым доверяет. В результате молодым программистам будет сложнее добиться успеха и предложить пользователям инновационные решения. Андрей уже не сможет быть уверенным в том, что приложения на его iPhone — самые безопасные для него и его дочери.

Знаете ли вы?

Пользователи, которые боятся за свою безопасность и конфиденциальность данных, склонны скачивать меньше приложений и чаще удалять их с устройств.[26,27,28] Плохо защищённая экосистема, в которой нельзя скачать приложение, не переживая за безопасность, приводит к тому, что пользователи не пробуют новое и не доверяют продуктами малоизвестных разработчиков. Это может подавлять рост рынка приложений, что принесёт вред и пользователям, и разработчикам.

Средства защиты безопасности в продуктах Apple и процедура проверки приложений защищают Андрея, Катю и их устройства

Мы применяем многоуровневый подход к защите пользователей iOS от вредоносных приложений и обеспечению безопасности наших платформ. Защита в iOS — непростая задача, потому что пользователи постоянно скачивают новые приложения и потому что наши мобильные устройства должны быть достаточно безопасными, чтобы дети могли пользоваться ими без присмотра. Это значит, что для iPhone мы должны применять более мощные средства защиты, чем для Mac: у них разные аудитории пользователей, с разным поведением и разными ожиданиями.

- **В случае с Mac мы используем автоматические системы, которые проверяют приложения на наличие известного вредоносного ПО. Они не дают ему попасть ни в App Store, ни к пользователям.**
- **Кроме того, разработчик обязан предоставлять описание приложения и всех его функций.** Наши специалисты оценивают точность этой информации в рамках процедуры проверки приложения. Пользователи могут с ней ознакомиться, чтобы решить, скачивать приложение или нет. Такой подход создаёт надёжные барьеры против основных видов мошенничества, используемых для распространения вредоносного ПО, например: подделка популярных приложений или рассказы об интересных функциях, которые на самом деле не работают.
- Убедившись, что функции соответствуют заявленному описанию и что на странице в App Store указана точная информация, **наши специалисты вручную проверяют, не требует ли приложение чрезмерно широкого доступа к конфиденциальным данным и соблюдаются ли правила сбора данных и безопасности в приложениях, предназначенных для детей.**

- **Если приложение было опубликовано в App Store, а позднее выяснилось, что правила были нарушены, мы связываемся с разработчиком, чтобы как можно быстрее устранить возникшую проблему.** Если речь идёт о чём-то особенно серьёзном, например о мошенничестве или вредоносных действиях, мы сразу же удаляем приложение из App Store и по возможности предупреждаем о происшествии тех, кто успел его скачать.
- **Если пользователь пострадал от приложения, скачанного из App Store, то он может получить помощь и даже компенсацию по программе AppleCare.**

Цель процедуры проверки — гарантировать, что приложениям в App Store можно доверять и что на страницах приложений в App Store указана точная информация о функциях и о том, какие данные будут использоваться. Мы постоянно совершенствуем эту процедуру, обновляя инструменты и методы проверки.

Скачав приложение из App Store, пользователь всегда знает, как оно работает и к каким данным получает доступ. В этом помогают такие функции, как «Прозрачность отслеживания» и запросы на предоставление доступа. Родители могут контролировать покупки детей (функция «Попросить купить»), время, которое они проводят, используя те или иные категории приложений, и данные, которыми они делятся. Кроме того, у пользователей есть возможность централизованно управлять платежами, связанными с приложениями, легко проверять и отменять подписки, оформленные внутри приложения. Всё это перестанет действовать так же эффективно, если приложения будут скачиваться со сторонних ресурсов.

В дополнение к процедуре проверки приложений мы оснащаем устройства надёжными средствами защиты на случай, если вредоносное приложение всё-таки будет скачано. Так, например, на iPhone все скачанные приложения работают в «песочнице». Это значит, что они не могут получить доступ к файлам других приложений, или изменить данные, которые хранятся на устройстве, пока пользователь явным образом не даст разрешение на такие действия.

Надёжная защита складывается из нескольких частей: проверка приложений помогает предотвратить установку вредоносного ПО, а средства обеспечения безопасности на устройствах ограничивают ущерб, который может быть нанесён, если приложение всё-таки будет скачано. Средства безопасности, встроенные в iOS, обеспечивают пользователю высокий уровень защиты — выше, чем на многих других потребительских устройствах — но они не способны удержать пользователя от неверного выбора. Процедура проверки приложений делает эффективными правила App Store, созданные для защиты от приложений, которые будут пытаться повредить устройство пользователя или убедить его предоставить доступ к конфиденциальным данным. Самые опасные из вредоносных приложений — те, которые пытаются обойти средства защиты на устройствах, и процедура проверки мешает им попасть на устройства наших пользователей.

Мы добились очень важного результата: эксперты признают iPhone одним из самых надёжных мобильных устройств. Многоуровневая система безопасности, созданная Apple, обеспечивает беспрецедентный уровень защиты от вредоносного ПО, а значит, пользователи могут не переживать за свои личные данные.

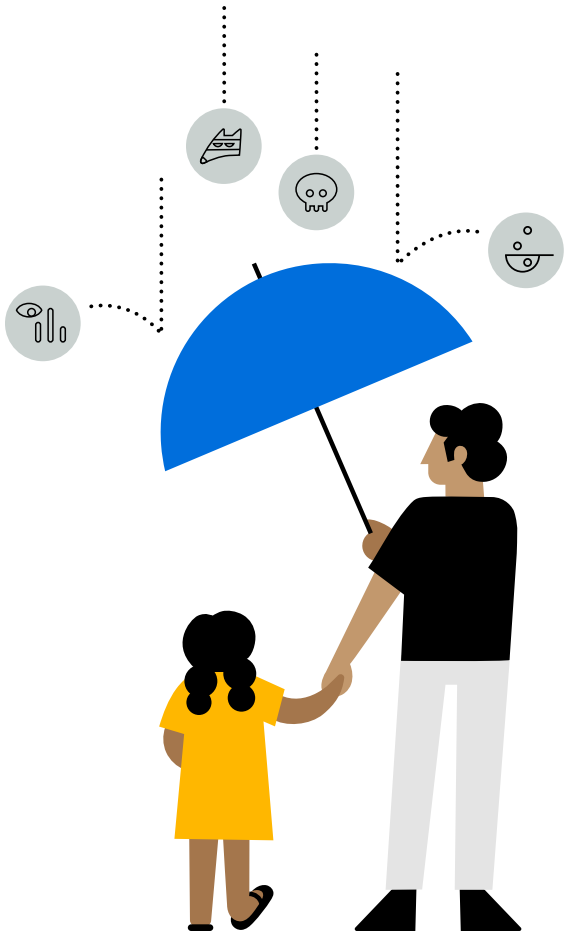
Проверка приложений

Эта процедура позволяет нам убедиться, что приложения поступают из надёжных источников и не содержат вредоносный код. Мы также проверяем приложения на предмет того, чтобы они не пытались обманом убедить пользователя совершить покупку или предоставить доступ к конфиденциальным данным. Мы защищаем разработчиков и пользователей, блокируя тех, кто нарушает правила. Процедура проверки, конечно, не позволяет убрать из App Store абсолютно все приложения низкого качества, но мы продолжаем совершенствовать технологии, процедуры и методы проверки приложений.

Проверка приложений в действии: результаты Apple за 2020 год

- **В среднем 100 000 новых приложений и обновлений каждую неделю проверяются** командой из 500 специалистов. Наши эксперты проверяют приложения на разных языках.
- **Почти миллион проблемных приложений и ещё столько же обновлений было отклонено или удалено:**
  - Более 150 000 — за спам, клонирование официальных приложений или обман пользователей.
  - Более 215 000 — за нарушение правил конфиденциальности.
  - Более 48 000 — за содержание скрытых или не указанных в описании функций.
  - Около 95 000 — за мошенничество, в основном по методу bait and switch, когда рекламодатель заманивает пользователя интересными обещаниями, а затем отвлекает его внимание, чтобы совершать противоправные действия.

- **Apple остановила множество мошеннических транзакций на общую сумму более 1,5 миллиарда долларов США.**
- **Apple исключила 470 000 команд из программы Apple Developer Program за мошенничество или связанные с ним действия.** Также компания отклонила около 205 000 заявок на вступление в программу по причинам, связанным с мошенничеством.
- **Apple заблокировала 244 миллиона учётных записей, связанных с мошеннической деятельностью, в том числе с предоставлением фальшивых отзывов.** Компания предотвратила ещё 424 миллиона попыток создания учётных записей по причине присутствия шаблонов поведения, свидетельствующих о мошенничестве или злоупотреблении доступом.



Благодаря проверке приложений Андрей чувствует себя под защитой

Зная о том, какие средства обеспечения безопасности и конфиденциальности защищают App Store, Андрей скачивает приложения, не переживая за себя и дочку. Он уверен, что Apple проверяет абсолютно все приложения в App Store на предмет наличия известного вредоносного кода и что пользователи iPhone гораздо реже сталкиваются с вредоносным ПО, чем пользователи других устройств.

Часто задаваемые вопросы

Что такое сторонние ресурсы для скачивания приложений?

Это любые другие источники, кроме официального магазина App Store, например веб-сайты или сторонние магазины приложений. Чтобы защитить наших пользователей и их данные, мы с первых этапов разработки iPhone отказались от возможности скачивать приложения со сторонних ресурсов.

Что такое модель угроз?

Это набор атак и уязвимостей, от которых нужно защищать пользователей. Модели угроз различаются в зависимости от устройств, категорий пользователей, среды применения, и всё это нужно учитывать при создании защиты. App Store — важный компонент в защите iPhone от тех опасностей, которые есть в его модели угроз. Это надёжная платформа, с которой можно безопасно скачивать приложения. Apple проверяет приложения, знает, кто их публикует, и следит, чтобы разработчики соблюдали установленные правила.

Если разрешить скачивание приложений со сторонних ресурсов, будет ли это опасно для тех, кто использует только App Store?

Да. Если мы разрешим использовать сторонние ресурсы, то откроем новые пути распространения вирусов, изменим модель угроз и увеличим разнообразие типов возможных атак, тем самым поставив под угрозу всех пользователей, в том числе тех, кто сознательно защищает себя и скачивает приложения только из App Store. Одновременно мы спровоцируем новый поток вложений в подготовку атак на iPhone, у злоумышленников появится стимул создавать новые инструменты и тренироваться проводить масштабные атаки на наши устройства. Набравшись опыта, преступники после App Store обратят свои действия против сторонних магазинов приложений, и под угрозой окажутся все пользователи. Кроме того, даже ответственного пользователя можно вынудить скачать приложение, которое нужно ему для работы или учёбы, со сторонних ресурсов — достаточно просто не публиковать его в App Store. Или обмануть, сделав сторонний магазин похожим на App Store.

Подробнее о средствах защиты, созданных Apple

Чтобы больше узнать о том, как Apple защищает вас и какие средства безопасности и конфиденциальности есть в App Store, зайдите на страницу apple.com/ru/app-store.

Подробная информация о защите сведений о местоположении приведена в Описании служб геолокации.

О средствах родительского контроля в iOS рассказано на странице apple.com/ru/families.

В чём состоит процедура проверки приложений в Apple?

Мы используем сложные технологии и ручную проверку приложений на предмет соблюдения правил App Store в отношении безопасности и конфиденциальности. Там, где автоматической проверки недостаточно, мы полагаемся на опыт наших специалистов. Они выявляют незаконный доступ к данным и проверяют приложения, предназначенные для детей. Порядок проверки со временем меняется, поскольку появляются новые угрозы и новые задачи, а наша цель — делать так, чтобы владельцам наших устройств всегда было удобно и комфортно пользоваться магазином App Store. В среднем 100 000 новых приложений и обновлений еженедельно проверяются командой более чем из 500 специалистов, работающих в разных странах мира.

Какие приложения проходят проверку?

Все приложения и все обновления, поступающие на публикацию в App Store.

Какие средства родительского контроля есть на устройствах Apple?

Мы постоянно разрабатываем функции, позволяющие родителям следить за тем, как дети пользуются устройствами. Функция «Экранное время» даёт возможность понять, сколько времени дети проводят в приложениях, на веб-сайтах и за экраном устройства в общем. С помощью Экранного времени можно также настраивать ограничения для разных категорий приложений и веб-сайтов. Есть также функция «Попросить купить», которая позволяет родителям одобрять или запрещать покупки в приложениях и сами приложения, которые дети хотят скачать на устройство. Период ожидания в ней — 15 минут. Он помогает предотвратить повторные покупки.

Что такое Прозрачность отслеживания и информация о конфиденциальности приложения?

Это новые функции, которые дают пользователю больший контроль над своими данными и больше возможностей защиты конфиденциальности. Согласно правилам прозрачности отслеживания, все приложения должны получать разрешение пользователя, прежде чем начинать отслеживать его данные в приложениях и на веб-сайтах, принадлежащих другим компаниям. Информация о конфиденциальности размещается в App Store: пользователи могут быстро посмотреть, каких правил конфиденциальности придерживается разработчик и как приложение будет использовать личные данные.

Список источников

1. Jobs, Steve, "Third Party Applications on the iPhone," October 17, 2007, accessed via tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

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

3. Griffin, Robert Jr., "Study on Mobile Device Security," *U.S. Department of Homeland Security*, April 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*, March 4, 2019.

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

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

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations," *Tech Crunch*, October 23, 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*, August 13, 2020.

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

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, March 18, 2021.

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

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

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

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

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

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

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

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

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

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

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

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit," *TorrentFreak*, January 8, 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," December 12, 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*, February 1, 2017.