Безопасность Apple ID

Что такое Apple ID?

Apple ID – универсальное средство доступа к мультимедийным сервисам компании Apple. Фактически, Apple ID предназначен для идентификации одного пользователя, который может получить с его помощью доступ ко всем необходимым сервисам компании, включая, iTunes, App Store и iCloud.

Для входа в аккаунт Apple используется аутентификация на основе пароля. Таким образом, пара адрес_электронной_почты/пароль служит для входа в учетную запись Apple ID. С использованием Apple ID вы можете получить доступ к необходимым вам сервисам через веб-интерфейс (соответствующие веб-сервисы) либо через приложения для iOS, OS X и Windows.

Почему необходимо заботиться о безопасности Apple ID?

Ваш аккаунт Apple, который идентифицируется через Apple ID, хранит личную информацию, указанную при его создании. К такой информации может относиться ваш фактический адрес, номер телефона и информация о кредитной карте, с которой совершаются покупки в AppStore и iTunes.

Если злоумышленники получат доступ к паре логин/пароль от Apple ID, они смогут использовать информацию из вашего аккаунта в своих целях.

Какие рекомендации вы можете дать по защите Apple ID?

Для того чтобы обеспечить должный уровень безопасности iDevice и Apple ID, воспользуйтесь следующими советами.

- Используйте на своем устройстве пароль для разблокировки. Это обезопасит ваше устройство в том случае, если оно попало в руки третьих лиц. Кроме этого, если злоумышленники скомпрометируют ваш Apple ID и попытаются удаленно заблокировать устройство (см. ниже), вы можете использовать свой код для его разблокировки.
- Не реагируйте на фишинговые сообщения от якобы компании Apple, которые призывают отправить в ответном сообщении логин/пароль от своего аккаунта, либо иную информацию об аккаунте, например, контрольные вопросы.
- Регулярно обновляйте iOS и десктопные приложения OS X & Windows, которые работают с Apple ID. Apple своевременно закрывает security-уязвимости, которые могут компрометировать устройство.
- Не используйте сервисы типа «Аренды Apple ID». Вы не можете гарантировать «безопасность» такого Apple ID, который получен из стороннего источника. Используйте только свой Apple ID, который принадлежит вам и безопасность которого обеспечиваете именно вы.
- Проверьте, включена ли у вас функция «Найти iDevice». В случае пропажи устройства вы можете воспользоваться iCloud для его блокировки, либо удаления с устройства своих данных.

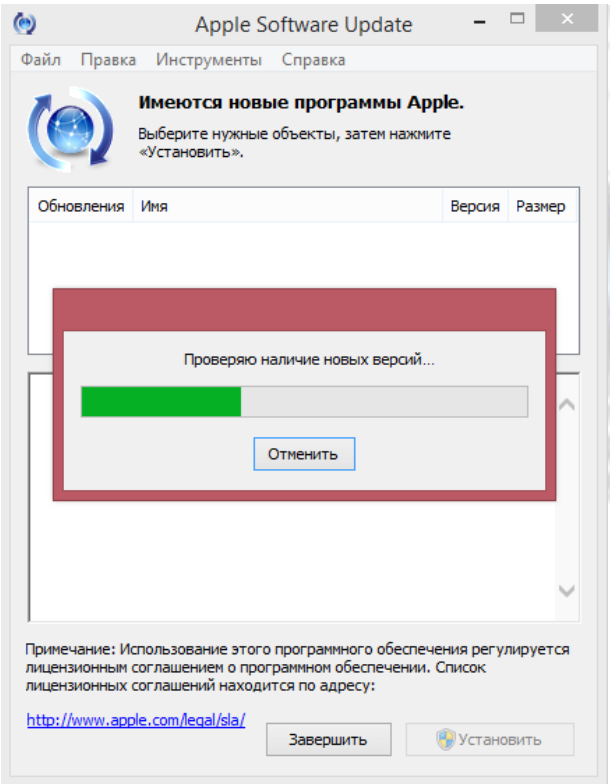

Рис. Интерфейс программы Apple Software Updater для Windows. С ее помощью всегда можно поддерживать программы iTunes, iCloud и QuickTime в актуальном состоянии.

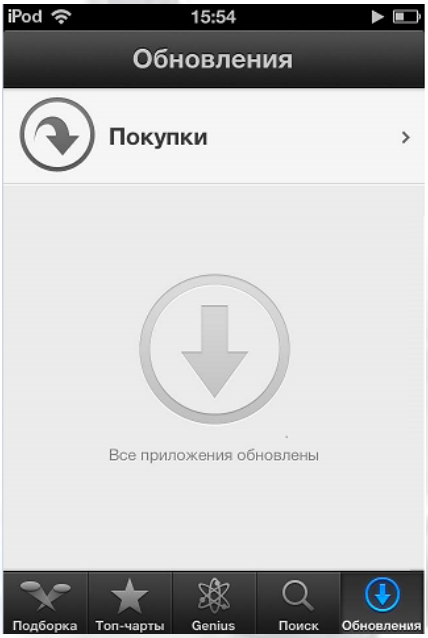

Рис. Раздел с обновлениями приложений в приложении App Store. Отсюда можно следить за актуальностью установленных приложений в iOS.

Почему следует обновлять ПО, которое работает с моим Apple ID (iOS, OS X, Windows) (поддерживать ПО в актуальном состоянии)?

Для таких приложений и ОС (iOS, OS X) компания Apple может закрывать (закрывала) опасные уязвимости, которые могут использоваться (использовались) злоумышленниками для кражи Apple ID. Например, для кражи информации на уязвимых версиях ОС может быть использована атака Man-in-the-Middle (SSL bug).

Я слышал, что злоумышленники могут удаленно заблокировать мой iPod Touch, iPhone или iPad с использованием iCloud. Это действительно так?

Для удобства пользователей вышеупомянутых устройств, компания Apple ввела специальную функцию, которая называется Lost Mode (Режим пропажи). Этот режим доступен через сервис iCloud (https://www.icloud.com/) и позволяет пользователю удаленно заблокировать устройство под управлением iOS6+ в случае его пропажи. При этом само устройство должно иметь выход в интернет, а также иметь активную опцию в iOS, которая называется «Найти iDevice».

Рис. Опция «Найти iPod» на iPod Touch под управлением iOS 6.1.6. Активна по умолчанию.

При блокировании устройства, пользователю предоставляется возможность вывести на экран предупредительное сообщение о том, что найденное устройство должно быть возвращено его законному владельцу.

Рис. Интерфейс сервиса iCloud, который используется для нахождения iDevice на карте, а также позволяет включать режим пропажи для удаленного блокирования устройства.

Если злоумышленникам удалось скомпрометировать (украсть) ваш Apple ID, т. е. получить к нему доступ, они могут воспользоваться сервисом блокировки устройства (Режим пропажи) от вашего имени и удаленно заблокировать устройство. В таком случае

возможно два варианта развития событий. В первом случае ваше устройство уже защищено паролем, который вы установили для его разблокировки. Таким образом для его разблокировки нужно просто ввести необходимый пароль, чтобы обратно восстановить доступ к устройству. Во втором случае устройство не было защищено паролем для разблокировки и тогда вам следует обращаться в техническую поддержку компании, либо воспользоваться методом его восстановления из резервной копии iTunes. Кроме этого, вам нужно сменить пароль на Apple ID, воспользовавшись сервисом https://appleid.apple.com/ru/.

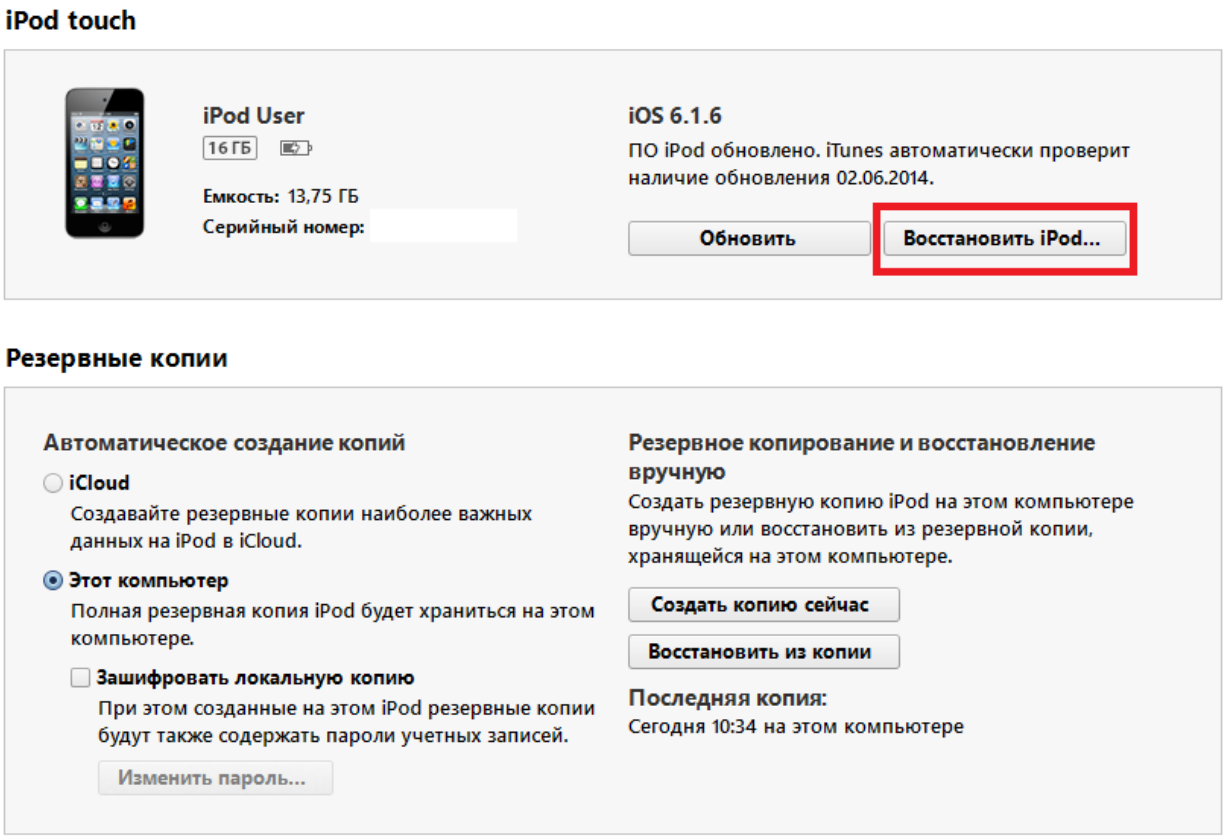

Рис. iTunes представляет собой основное средство управление iDevice и может использоваться как инструмент восстановления устройства в случае его блокировки (непреднамеренной или намеренной). Подробнее см. здесь.

Если злоумышленники узнали мои логин/пароль Apple ID, они получают полный доступ к моему аккаунту?

Можно сказать, что они получают ограниченный доступ, поскольку для выполнения некоторых критических операций понадобятся ответы на секретные контрольные вопросы.

Как мне отличить настоящие электронные сообщения компании Apple от тех, которые рассылаются злоумышленниками?

Настоящие электронные письма от компании рассылаются только с электронного адреса с доменом верхнего уровня apple.com. Например, адрес *appleid@id.apple.com* используется для извещения пользователя об операциях, которые были выполнены над его аккаунтом Apple ID. Фишинговые сообщения злоумышленников могут «напоминать» такой адрес, но в домене будет содержаться ошибка, которую можно сразу заметить, если внимательно на него посмотреть.

Фишинговые сообщения от злоумышленников могут напоминать по содержанию аналогичные от компании Apple. Но в таких фишинговых сообщениях может находиться информация, которая предлагает пользователю раскрыть его Apple ID, т. е. отправить его в ответном сообщении. Такая ситуация невозможна с официальными письмами компании Apple, которые также не будут содержать внутри текста сообщения гиперссылки на сторонние сайты.

Я использую двухфакторную аутентификацию (2FA) для своих аккаунтов Google и Microsoft Live ID. Могу ли я подключить 2FA и для Apple ID?

К сожалению, Россия пока не относится к тем регионам, где Apple поддерживает 2FA для Apple ID. Список таких стран см. здесь.

Как связаны между собой функции Найти iDevice и Activation Lock?

Activation Lock (Блокировка активации) представляет собой новую функцию iOS7, которая включается автоматически при активации функции «Найти iDevice». Она вводит дополнительный уровень безопасности (запрос пароля Apple ID) для следующих критичных операций (которые могут использоваться для повторной активации устройства без ведома пользователя).

- Выключение функции «Найти iDevice» на устройстве.
- Выход из сервиса iCloud на устройстве.
- Уничтожение данных на устройстве и его повторная активация.

Могу ли я получать уведомления от компании Apple о закрываемых ею уязвимостях и выпускаемых обновлениях, чтобы быть в курсе информации о безопасности интересующих меня продуктов?

Apple предоставляет такую возможность через специальные списки рассылок по электронной почте. Эти списки перечислены здесь https://lists.apple.com/mailman/listinfo. Для того, чтобы получать информацию об обновлениях безопасности, вам нужно подписаться на рассылку *Security-announce*, которая находится здесь https://lists.apple.com/mailman/listinfo/security-announce.