Ежемесячный журнал по вопросам компьютерной безопасности

OUCH!

В ЭТОМ ВЫПУСКЕ…

Как защитить новый планшет

Ваш новый планшет

Поздравляем с приобретением нового планшета; современные технологии предоставляют возможность общения, онлайн покупок, чтения, прослушивания музыки, игр и множество других развлечений. С того дня, как новое устройство стало важной частью вашей жизни, вы должны предпринять несколько простых шагов для его защиты и обеспечить безопасность.

Об авторе

Чад Тилбури – автор нашего выпуска. У Чада богатый опыт расследования компьютерных преступлений. Он является соавтором курсов FOR408 Windows Forensics, FOR508 Advanced Forensics и читает курс Расследование инцидентов в Институте SANS. В Twitter Чад ведёт записи как **@chadtilbury** и у него есть блог **http://forensicmethods.com**.

Защита нового планшета

Первым шагом является установка пароля или другой блокировки экрана. Планшет легко брать с собой куда угодно, его также легко потерять или его могут украсть. Чтобы ваша личная информация не попала в чужие руки, убедитесь, что защитили экран сложным PIN, паролем или установили блокировку движением. В некоторых моделях может быть установлена система биометрической аутентификации, например, сканером отпечатков пальцев. Используйте самые надежные способы защиты планшета, которые он поддерживает, и убедитесь, что включен режим автоматической блокировки через короткое время при бездействии.

Следующим шагом является обновление операционной системы планшета до самой последней. Плохие парни постоянно находят слабые места в системе, вендоры постоянно выпускают обновления и патчи, чтобы их исправить. Если вы используете последнюю версию программного обеспечения, ваш планшет взломать сложней.

Уделите особое внимание первичной настройке планшета. Самыми важными конфигурациями являются настройки конфиденциальности и функции облака. Настройки конфиденциальности помогут сохранить вашу личную информацию. Одним из самых важных вопросов безопасности является возможность отслеживать ваше местоположение через планшет. Мы рекомендуем отключить в настройках приватности функцию отслеживания местоположения для всех приложений и подключить эту функцию только для конкретных. Некоторым приложениям

Как защитить новый планшет

данная функция необходима (например, для навигатора или приложения для поиска ресторана поблизости), но большинству приложений функция отслеживания местоположения в реальном времени не нужна.

лучший способ защиты планшета - использование блокировки монитора или пароля, последней версии операционной системы, осторожность с облачными сервисами и постоянный контроль конфиденциальности.

Другой важной функцией является возможность хранения данных на облаке. Облачные сервисы, как Apple's iCloud, Microsoft's Skydrive, Dropbox или Google Drive позволяют хранить данные на серверах с доступом через Интернет. У большинства планшетов есть встроенная функция хранения практически всех данных на облаке, включая все документы, фотографии и видео. Поэтому определитесь с конфиденциальностью данных перед тем, как хранить их на облаке. Убедитесь, что вы поняли, как информация будет защищена (например, с помощью пароля) и кто получит к ней доступ. Вы же не хотите, чтобы ваши фото были опубликованы в сети вместе с вашими координатами без вашего ведома.

Имейте в виду, что большинство планшетов синхронизируют работу с другими устройствами, например, компьютерами или ноутбуками. Это типично для приложений подобных Google Chrome, широко используется в Windows 8 и является одной из популярных функций сервиса Icloud. Функция синхронизации довольно удобная в некоторых случаях, но не удивляйтесь, если увидите список посещённых вами сайтов и вкладок с планшета в браузере рабочего компьютера.

Используйте планшет безопасно

Если вы однажды настроили защиту планшета, то следует убедиться, что он остается защищенным. Вот некоторые шаги, которые помогут правильно использовать планшет.

- Используйте только последнюю версию программного обеспечения и приложений и регулярно их обновляйте. Большинство планшетов автоматически обновляют приложения; необходимо включить данную функцию.
- Не ломайте защиту вашего планшета, это приведет в негодность многие настройки безопасности и сделает ваш планшет очень уязвимым.

Как защитить новый планшет

- Загружайте только те приложения, которые вам нужны и делайте это из достоверных источников. Для IPad все просто: загружайте все приложения с ITunes. Компания Apple тщательно проверяет их перед тем, как опубликовать. Для пользователей Google рекомендуем ограничиться Google Play. Также вы можете скачивать приложения и с других сайтов, но обычно они не проверяются и могут содержать вирусы. Наконец, не важно, из каких источников вы загрузили приложение, удалите его сразу, как перестали активно использовать и оно больше не нужно.
- При установке нового приложения пересмотрите настройки безопасности, как вы делали изначально при настройке нового планшета. Будьте осторожны с информацией, к которой открываете доступ или разрешаете приложению определённые действия с ней. Действительно ли новому приложению необходим доступ ко всем вашим контактам?
- Убедитесь, что установили и настроили программу, которая позволяет удалённо отслеживать, блокировать и удалять данные с планшета в случае его кражи или потери.

Узнайте Больше

Подпишитесь на OUCH! – ежемесячный журнал по информационной безопасности, получите доступ к архивам OUCH! и узнайте больше о решениях SANS в вопросах информационной безопасности на нашем сайте http://www.securingthehuman.org.

Дополнительная информация

Синхронизация Chrome
http://www.techrepublic.com/blog/google-in-the-enterprise/chrome-sync-configure-once-work-everywhere/
Опасности облаков:
http://www.businessnewsdaily.com/5215-dangers-cloud-computing.html
Термины информационной безопасности:
http://www.securingthehuman.org/resources/security-terms
Ежедневные советы Института SANS:
https://www.sans.org/tip_of_the_day.php

Редакция: Билл Уайман, Уолт Скривенс, Фил Хоффман, Боб Рудис
Русский перевод: Александр Котков, Ирина Коткова