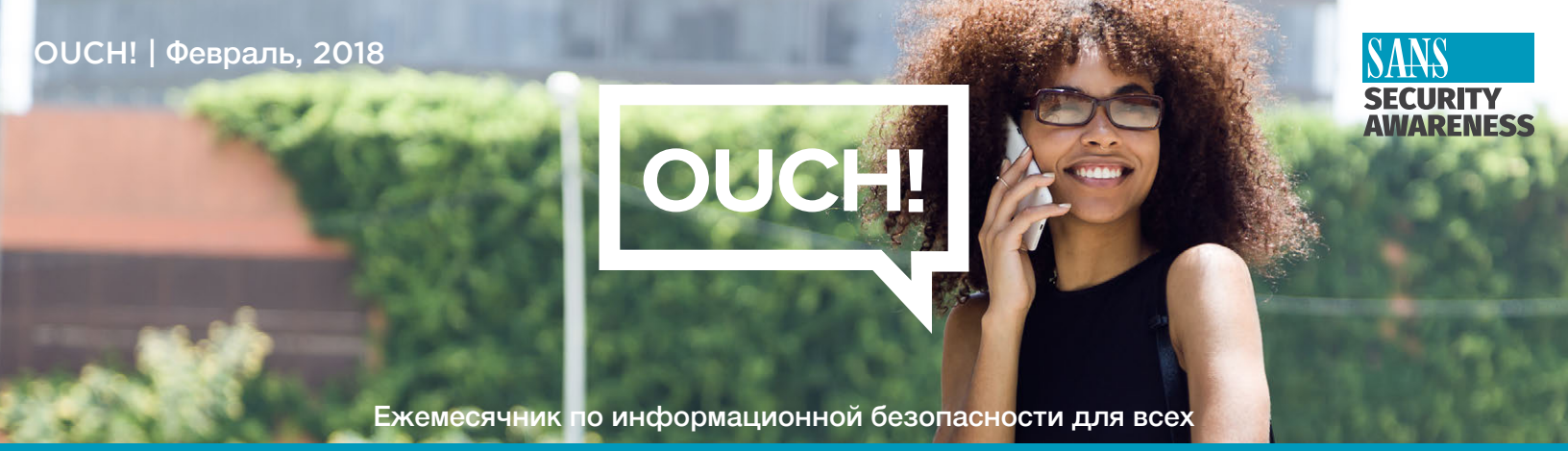

Ежемесячник по информационной безопасности для всех

Безопасность ваших мобильных устройств

Обзор

Ваши мобильные устройства предоставляют удивительные возможности для общения с друзьями, совершения покупок и проведения банковских операций через интернет, просмотра фильмов и бесконечного множества других занятий. Поскольку эти устройства занимают такое важное место в вашей жизни, мы познакомим вас с некоторыми простыми шагами, которые позволят вам обезопасить ваши мобильные устройства.

Как обезопасить ваши мобильные устройства

Вы можете удивиться, узнав что наибольший риск вашим мобильным устройствам исходит не от хакеров, а от вас самих. Вероятность того, что вы потеряете или оставите где-нибудь ваше мобильное устройство значительно выше вероятности его взлома злоумышленниками. Прежде всего, чтобы защитить ваше устройство, вы должны включить автоматическую блокировку экрана. Это означает, что всякий раз, когда вы хотите использовать своё устройство, вы должны разблокировать экран, например, с помощью парольного кода или отпечатка вашего пальца. Это гарантия того, что в случае кражи или потери вашего устройства, никто не сможет воспользоваться им. Ещё несколько советов, которые помогут вам защитить свои устройства:

Обновления

Включите функцию автоматического обновления на всех своих мобильных устройствах, так чтобы они всегда использовали новейшую версию операционной системы и приложений. Злоумышленники всё время ищут новые уязвимости в программном обеспечении, а производители постоянно выпускают новые версии и обновления для устранения этих уязвимостей. Используя новейшие версии операционной системы и мобильных приложений, вы значительно осложняете задачу взлома ваших устройств.

Отслеживание

Установите или включите программу, позволяющую дистанционно отслеживать местоположение вашего устройства через интернет. В случае кражи или потери вашего устройства, вы можете подключиться к нему через интернет и найти, где оно находится, или, в крайнем случае, удалённо стереть всю свою информацию с этого устройства.

Заслуживающие доверия приложения

Загружайте и устанавливайте только приложения, которые действительно вам нужны и только из заслуживающих доверия источников. Для устройств iPad и iPhone это означает загрузку приложений только

из Apple App Store. Для устройств системы Android загружайте приложения с Google Play. Планшеты Amazon обновляйте через Amazon App Store. У вас есть возможность загружать приложения с других сайтов, но эти приложения не проходят проверку на безопасность и, вполне вероятно, могут быть заражены. Кроме того, перед загрузкой приложения, проверьте что у него большое число положительных отзывов и что приложение активно обновляется разработчиком. Остерегайтесь совершенно новых приложений, приложений, имеющих мало отзывов или редко обновляемых. И, наконец, независимо от того, где вы приобрели ваше приложение, мы рекомендуем удалить его с вашего устройства, как только оно вам более не нужно или вы его не используете.

Настройки конфиденциальности

При установке новых приложений, обращайте внимание на настройки конфиденциальности. Например, действительно ли программа, которую вы только что загрузили, нуждается в доступе ко всей информации о ваших контактах и друзьях? Мы рекомендуем вам запретить функцию отслеживания местоположения устройства для всех программ и затем разрешить её использование только теми приложениями, которым она действительна нужна, по вашему мнению. Если вас не устраивают требования прав доступа приложения, найдите другое приложение, которое вас устраивает. Периодически проверяйте права доступа, чтобы удостовериться, что они не изменились.

Резервное копирование

Всегда делайте резервную копию ваших данных. Резервные копии большого количества данных с ваших мобильных устройств делаются автоматически, например ваши снимки или сообщения. Однако, резервные копии также хранят конфигурацию настроек вашего устройства, приложения и другую информацию, значительно облегчая задачу восстановления данных с потерянного устройства или перехода на использование нового устройства.

На работе

Когда вы на работе, будьте предельно осторожны и никогда не делайте фото или видео съёмку, так как вы можете случайно запечатлеть конфиденциальную информацию, например снимки информации на стираемой доске или на экране компьютера.

Ваши мобильные устройства - мощные инструменты, которые помогают вам работать и развлекаться.
Следуя нашим рекомендациям, вы сможете обезопасить себя и свои устройства.

Ресурсы

Парольные фразы:	https://www.sans.org/u/A3E
Резервное копирование:	https://www.sans.org/u/A3z
Утилизация мобильных устройств:	https://www.sans.org/u/A3u
Безопасное использование мобильных приложений:	https://www.sans.org/u/A3p
Ежедневные советы Института SANS:	https://www.sans.org/tip_of_the_day.php

Лицензия

Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова