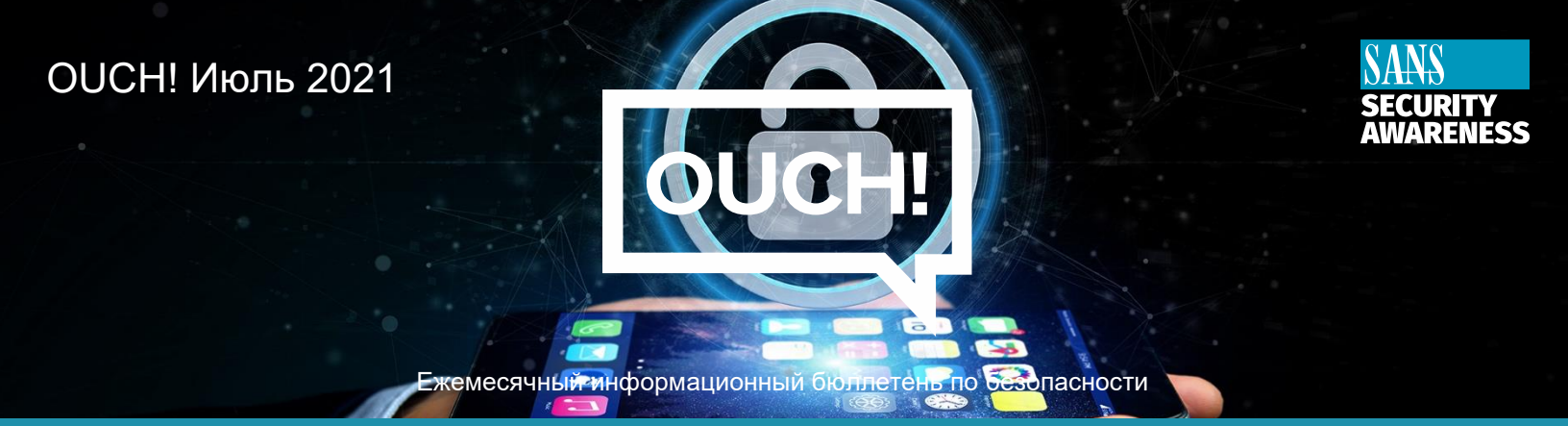


Ежемесячный информационный бюллетень по безопасности

Безопасность ваших мобильных устройств

Обзор

Мобильные устройства - это прекрасный и простой способ общения с друзьями, делать покупки или банковские операции в Интернете, смотреть фильмы, играть в игры и выполнять множество других действий. Поскольку эти устройства являются такой важной частью вашей жизни, важно обеспечить безопасность вас и ваших устройств.

Безопасность ваших устройств

Вы можете удивиться, узнав, что наибольшую опасность для вашего мобильного устройства, скорее всего, представляют не киберпреступники, а вы. У вас гораздо больше шансов потерять или забыть мобильное устройство, чем подвергнуться взлому. Первое, что вы должны сделать для защиты своего устройства, когда оно находится в режиме ожидания - это включить автоматическую блокировку экрана. Это означает, что для использования устройства вам необходимо разблокировать экран с помощью надежного пароля, лица или отпечатка пальца. Это помогает гарантировать, что кому-либо будет намного сложнее получить доступ к вашей информации, если устройство потеряно или украдено. В качестве бонуса для большинства мобильных устройств включение блокировки экрана также включает шифрование, помогая защитить данные, хранящиеся на устройстве.

Вот еще несколько советов, которые помогут защитить ваши устройства:

1. **Обновление**: включите автоматическое обновление на своих устройствах, чтобы на них всегда была установлена последняя версия операционной системы и приложений. Злоумышленники всегда ищут новые слабые места в программном обеспечении, а поставщики постоянно выпускают обновления и патчи для их исправления. Своевременное обновление устройств усложняет их взлом. Выбирая новое устройство Android, обратите внимание на обязательства поставщика по обновлению устройства. Устройства Apple iOS обновляются самой компанией, в то время как мобильные устройства Android обновляются поставщиком, который продал вам устройство, и не все поставщики активно обновляют свои устройства. Если вы используете старое устройство, которое больше не поддерживается или не может быть обновлено, подумайте о покупке нового устройства.

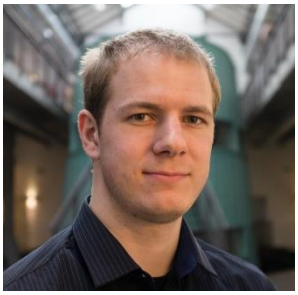
2. **Отслеживание**: установите или включите надежное программное обеспечение для удаленного отслеживания вашего мобильного устройства через Интернет. Таким образом, если устройство потеряно или украдено вы можете подключиться к нему через Интернет и узнать его местоположение, в худшем случае, удаленно стереть всю вашу информацию.

3. **Надежные мобильные приложения**: Устанавливайте только нужные приложения и пользуйтесь надежными источниками. Для устройств Apple iOS, таких как iPad или iPhone, это означает Apple App Store. Для устройств Android используйте Google Play; для планшетов Amazon используйте Amazon App Store. Хотя вы можете устанавливать приложения с других сайтов, они не проходят проверку и с гораздо большей вероятностью могут быть заражены или вредоносны, что может поставить под угрозу вашу конфиденциальность. Кроме того, перед загрузкой убедитесь, что приложение имеет много положительных отзывов и активно обновляется поставщиком. Держитесь подальше от новых приложений, с небольшим количеством отзывов или приложений, которые редко обновляются.

4. **Параметры конфиденциальности**: мобильные устройства собирают обширную информацию о вас, тем более, когда оно находится с вами. Тщательно проверьте настройки конфиденциальности своего устройства, включая отслеживание местоположения, и убедитесь, что конфиденциальные уведомления (например, коды подтверждения) не появляются на экране, когда устройство заблокировано.
5. **Работа**: убедитесь, что любое мобильное устройство, которое вы используете для работы, разрешено для использования в работе. На работе будьте особенно осторожны и никогда не снимайте фото или видео, которые могут случайно содержать конфиденциальную информацию, например, изображения досок или экранов компьютеров.

Ваши мобильные устройства - это мощный инструмент, которым мы хотим, чтобы вы использовали безопасно и с удовольствием. Простое выполнение этих нескольких простых шагов может иметь большое значение для обеспечения безопасности вас и ваших устройств.

Приглашенный редактор



Джерун Бекерс - эксперт по мобильной безопасности в NVISO, соавтор OWASP MASVS и MSTG, инструктор института SANS и автор SEC575: Курс по безопасности мобильных устройств и этичному взлому. Вы можете найти Джеруна через LinkedIn на https://www.linkedin.com/in/beckersjeroen/.

Ресурсы

Сила обновления: https://www.sans.org/newsletters/ouch/the-power-of-updating
Безопасное использование мобильных приложений: https://www.sans.org/newsletters/ouch/securely-using-mobile-apps/
Текстовые сообщения /SMS фишинг: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks
Создание простых паролей: https://www.sans.org/newsletters/ouch/making-passwords-simple
Вишинг - атаки на телефонные звонки и мошенничество: https://www.sans.org/newsletters/ouch/vishing

Роман Полаков