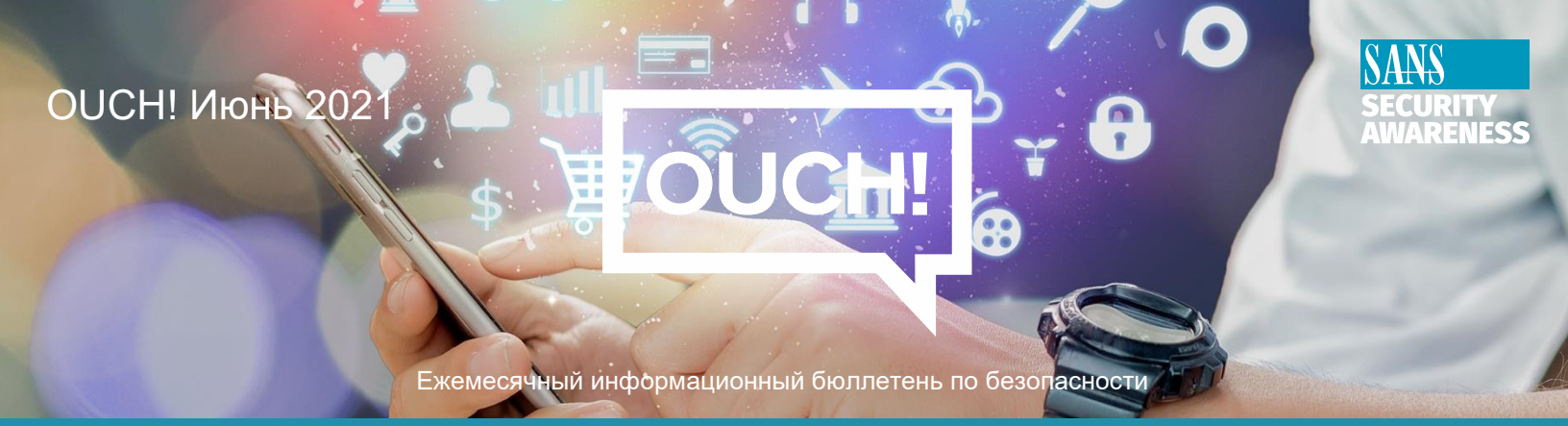
OUCH! Июнь 2021



Ежемесячный информационный бюллетень по безопасности

Безопасное использование мобильных приложений

Обзор

Мобильные устройства, такие как планшеты, смартфоны и умные часы, стали одной из основных технологий, которые мы используем как в личной, так и в профессиональной жизни. Что делает эти устройства такими популярными, так это тысячи приложений, из которых мы можем выбирать. Приложения позволяют нам быть более продуктивными, общаться и делиться с другими, обучаться, тренироваться или просто получать удовольствия. Вот шаги, которые вы можете предпринять для безопасного использования современных мобильных приложений.

Получение безопасных мобильных приложений

Киберпреступники овладели навыками создания и распространения вредоносных приложений, которые кажутся законными. Если вы установите одно из таких приложений, злоумышленники смогут получить полный контроль над вашим мобильным устройством или данными. Вот почему вы хотите убедиться, что загружаете только безопасные мобильные приложения из надежных источников. Вы можете не осознавать, что марка мобильного устройства, которое вы используете, определяет ваши варианты загрузки приложений.

Для устройств Apple загружайте только мобильные приложения из Apple App Store. Преимущество здесь в том, что Apple выполняет проверку безопасности всех мобильных приложений, прежде чем они станут доступными для клиентов. Хотя Apple не может обнаружить все вредоносные приложения, эта управляемая среда значительно снижает риск загрузки такого. Кроме того, если сотрудники Apple обнаружат приложение, которое, по их мнению, является вредоносным, они быстро его удалят.

Для устройств Android загружайте только мобильные приложения из Google Play, который поддерживается Google. Подобно Apple, Google проверяет безопасность всех приложений, прежде чем они станут доступными для клиентов. Разница с устройствами Android заключается в том, что вы также можете включить определенные параметры, которые позволяют загружать мобильные приложения из других источников. Мы настоятельно не рекомендуем этого делать, поскольку любой, включая киберпреступников, может легко создавать и распространять вредоносные мобильные приложения и вынуждать вас заразить ваше мобильное устройство. Независимо от того, какой бренд вы используете, изучите приложение перед его загрузкой. Посмотрите, как долго было доступно мобильное приложение, сколько людей им пользовалось и кто его продавец.

Чем дольше приложение было общедоступным, тем больше людей использовали и оставили положительные комментарии о нем, и чем чаще поставщики приложений обновляли его, тем больше вероятность, что приложению можно доверять. Кроме того, устанавливайте только те приложения, которые вам нужны и которыми вы пользуетесь. Спросите себя: «Действительно ли мне нужно это приложение?» Каждое приложение потенциально несет не только новые уязвимости, но и новые проблемы с конфиденциальностью. Если вы перестали использовать приложение или больше не находите его полезным, удалите его со своего мобильного устройства (вы всегда можете добавить его позже, если обнаружите, что оно вам действительно нужно).

Конфиденциальность и разрешения доступа

После установки убедитесь, что приложение защищает вашу конфиденциальность. Действительно ли мобильному приложению нужен доступ к вашему местоположению, микрофону и контактам? Когда вы включаете разрешения, вы позволяете создателю приложения отслеживать вас, делиться или продавать вашу информацию другим. Если вы не хотите предоставлять эти разрешения, просто отклоните запрос, предоставьте разрешение приложению только тогда, когда оно активно используется, или найдите другое приложение, отвечающее вашим требованиям. Помните, у вас есть много вариантов.

Обновление приложений

Мобильные приложения, как и ваш компьютер и операционная система мобильного устройства, должны быть обновлены. Преступники постоянно ищут и находят новые слабые места в приложениях и разрабатывают способы их использования. Разработчики приложения создают и выпускают обновления, чтобы исправить эти недостатки и защитить ваши устройства. Чем чаще вы проверяете и устанавливаете обновления, тем лучше. Большинство устройств позволяют настроить систему для автоматического обновления мобильных приложений. Мы настоятельно рекомендуем включить этот параметр.

Мобильные приложения - ключ к максимально эффективному использованию ваших устройств. Просто будьте осторожны с теми, которые вы выбираете, и убедитесь, что вы используете их безопасно и надежно.

Приглашенный редактор

Доменика Крогнале - инженер по обеспечению качества и сертифицированный инструктор Института SANS. Она является соавтором книги «FOR585: Подробный анализ смартфона». Свяжитесь с Доменикой в Твиттере @domenicacrognal.

Ресурсы

Сила обновления : https://www.sans.org/security-awareness-training/resources/power-updating
Конфиденциальность : https://www.sans.org/newsletters/ouch/privacy/
Роман Полаков