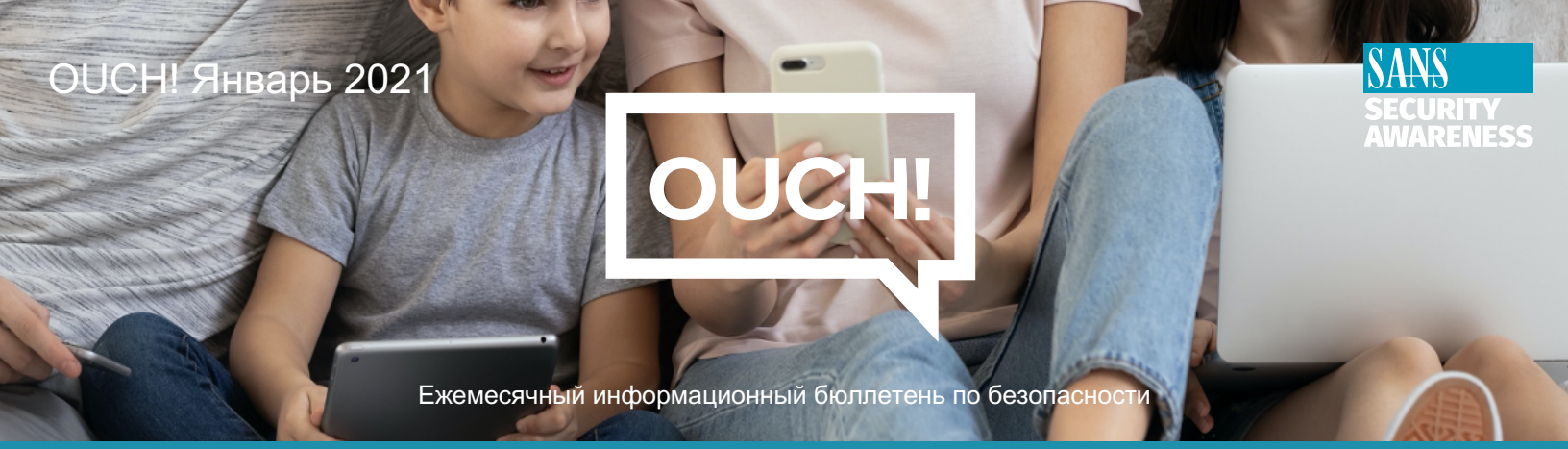
OUCH! Январь 2021



Ежемесячный информационный бюллетень по безопасности

Обеспечение безопасности Wi-Fi дома

Обзор

Чтобы создать безопасную домашнюю сеть, вам нужно начать с защиты точки доступа Wi-Fi (иногда называемой маршрутизатором Wi-Fi). Это устройство, которое контролирует, кто и что может подключаться к вашей домашней сети. Вот пять простых шагов по обеспечению безопасности вашего домашнего Wi-Fi, чтобы создать гораздо более безопасную домашнюю сеть для вас и вашей семьи.

Сосредоточьтесь на основах

Часто самый простой способ подключиться к устройству Wi-Fi и настроить его - это когда он подключен к домашней сети. Укажите в веб-браузере конкретный IP-адрес, указанный в руководстве к вашему устройству (например, https://192.168.1.1), или воспользуйтесь служебной программой или мобильным приложением, предоставленным поставщиком вашего устройства Wi-Fi.

1. **Изменить пароль администратора**: Ваша точка доступа Wi-Fi, скорее всего, была отправлена с паролем по умолчанию для учетной записи администратора, который позволяет вам изменять конфигурацию устройства. Часто эти пароли по умолчанию являются общедоступными, возможно, даже размещенными в Интернете. Обязательно измените пароль администратора на уникальный надежный пароль, чтобы только вы имели к нему доступ. Если устройство позволяет, также измените имя пользователя администратора.
2. **Используйте сетевой пароль**: Настройте свою сеть Wi-Fi так, чтобы у нее был уникальный надежный пароль (убедитесь, что он отличается от пароля администратора вашего устройства). Таким образом, только люди и устройства, которым вы доверяете, смогут присоединиться к вашей домашней сети. Подумайте об использовании менеджера паролей, чтобы выбрать надежный пароль и отслеживать все ваши пароли за вас.
3. **Обновление микропрограммного обеспечения**: Включите автоматическое обновление операционной системы точки доступа Wi-Fi, которое часто называется микропрограммное обеспечение. Таким образом вы обеспечите максимальную безопасность своего устройства с помощью новейших опций безопасности. Если автоматическое обновление недоступно

для вашей точки доступа Wi-Fi, периодически входите в систему и проверяйте свое устройство, чтобы узнать, доступны ли какие-либо обновления. Если ваше устройство больше не поддерживается поставщиком, подумайте о покупке нового устройства, которое вы можете обновить, чтобы получить последние функции безопасности.

4. **Использовать гостевую сеть**: Гостевая сеть- это отдельная виртуальная сеть, которую может создать ваша точка доступа Wi-Fi. Это означает, что ваша точка доступа Wi-Fi фактически имеет две сети. *Первичная сеть* - это та, к которой подключаются ваши доверенные устройства, например компьютер, смартфон или планшет. *Гостевая сеть*- это то, к чему подключаются ненадежные устройства, например, гости, посещающие ваш дом, или, возможно, некоторые из ваших личных устройств умного дома. Когда что-то подключается к вашей гостевой сети, оно не может видеть или связываться с какими-либо из ваших доверенных личных устройств, подключенных к вашей основной сети.
5. **Используйте безопасную фильтрацию DNS:** DNS - это интернет-сервис, который преобразует имена веб-сайтов в числовые адреса. Это то, что помогает обеспечить подключение вашего компьютера к веб-сайту, когда вы вводите его название. Точки доступа Wi-Fi обычно используют DNS-сервер по умолчанию, предоставленный вашим интернет-провайдером, но более безопасные альтернативы доступны бесплатно в таких службах, как OpenDNS, CloudFlare for Families, or Quad9 которые могут обеспечить дополнительную безопасность, блокируя вредоносные или другие нежелательные веб-сайты. Войдите в свою точку доступа Wi-Fi и измените адрес DNS-сервера на более безопасный.

Защита вашей домашней точки доступа Wi-Fi - это первый и один из самых важных шагов в создании безопасной домашней сети. Дополнительные сведения о защите точки доступа Wi-Fi смотрите в руководстве к устройству. Если ваше устройство Wi-Fi предоставил поставщик услуг Интернета, обратитесь к нему за дополнительной информацией о функциях безопасности.

Приглашенный редактор

Джошуа Райт (Twitter @ joswr1ght) - старший директор Counter Hack Challenges, LLC, руководящий координацией и разработкой киберзадач для NetWars и Holiday Hack Challenge. Найдите Джоша в LinkedIn здесь:https://linkedin.com/in/joswr1ght.

Ресурсы

Создание простых паролей: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Менеджер паролей: https://www.sans.org/security-awareness-training/resources/password-managers-0
Обновление: https://www.sans.org/security-awareness-training/resources/power-updating
Руководство по установке OpenDNS: https://www.opendns.com/setupguide/#familyshield

Переведено для сообщества: Роман Поляков