Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

- **Безопасность беспроводной сети**
- **Безопасность устройств**

Безопасность домашней сети

Обзор

Несколько лет назад домашние беспроводные сети были довольно просты и состояли, как правило, из точки доступа и пары компьютеров, которыми пользовались для доступа в Интернет, онлайн покупок или игр. Но в наше время домашние сети стали значительно сложнее. Сейчас к домашней сети подключено большое количество устройств, которые используются не только для доступа в Интернет или просмотра средств массовой информации. В этом выпуске мы поговорим о том, как сделать домашнюю сеть безопасной для всех членов семьи.

Об авторе

Черил Конли возглавляет отдел тренинга по информационной безопасности в компании Lockheed Martin. Она использует фирменную методику The I Campaign TM для тренинга 100000 сотрудников компании. Методика активно использует фокус-группы внутри компании и координирует глобальную программу защиты от фишинга. Черил ведет блог **@conleychera**.

Безопасность беспроводной сети

Практически в каждом доме есть беспроводная сеть (или, так называемая сеть Wi-Fi). Эта сеть позволяет подключить любое устройство к Интернету, например, ноутбук, планшет или игровую приставку. Большинство беспроводных сетей управляются роутером - устройством, установленным вашим интернет-провайдером для обеспечения доступа к Интернету. Но в некоторых случаях ваша сеть может контролироваться отдельными системами, так называемыми точками доступа, которые соединены с роутером. Не зависимо от того, с помощью какой системы ваши устройства соединяются с Интернетом, принцип работы этих систем одинаков: передача радиосигналов. Различные устройства могут подключаться к вашей беспроводной сети с помощью этих радиосигналов. Через сеть эти устройства могут подключаться к Интернету и к другим устройствам вашей сети. Это означает, что безопасность вашей домашней сети является одним из основных компонентов защиты вашего дома. Мы советуем выполнять следующие правила для обеспечения безопасности вашей домашней сети:

- Измените пароль администратора, установленный производителем Интернет роутера или точки доступа. Аккаунт администратора позволяет вносить изменения к настройкам сети. Проблема в том, что многие роутеры поставляются со стандартными, хорошо известными паролями и их легко найти

Безопасность домашней сети

в Интернете. Поэтому следует изменить заводской пароль на уникальный и сильный пароль, который будете знать только вы.

- Измените название сети, установленное производителем (его ещё называют SSID). Это имя ваши устройства видят при поиске домашней беспроводной сети. Дайте своей домашней сети уникальное имя, которое легко узнать, но оно не должно содержать личной информации. Конфигурация сети как «невидимой» - малоэффективная форма защиты. Большинство программ сканирования беспроводных сетей и любой опытный хакер может легко обнаружить «невидимые» сети.
- Убедитесь, что к вашей сети могут подключаться только люди, которым вы доверяете, и что это соединение является зашифрованным. Это поможет повысить уровень безопасности. В настоящее время самым безопасным соединением является WPA2. При его использовании пароль запрашивается при подключении к сети, и при этом подключении используется шифрование. Убедитесь, что вы не используете устаревший метод, например, WEP, или не пользуетесь открытой сетью (которая вообще не предоставляет защиты). Открытая сеть позволяет абсолютно всем подключаться к вашей беспроводной сети без аутентификации.
- Убедитесь, что для подключения к вашей сети люди используют сильный пароль, который не совпадает с паролем администратора. Помните, что вам нужно ввести пароль для каждого используемого устройства только однажды, этот пароль устройства могут запоминать и хранить.
- Большинство беспроводных сетей поддерживают, так называемую Гостевую Сеть (Guest Network). Это позволяет гостям выходить в Интернет, но домашняя сеть в этом случае защищена, так как гости не могут соединиться с домашними устройствами вашей сети. Если вы добавляете гостевую сеть, убедитесь, что используете WPA2, и она защищена с помощью уникального и сильного пароля.
- Отключите Wi-Fi Protected Setup или другую настройку, позволяющую подключать новые устройства без ввода пароля и других опций конфигурации.
- Если вам сложно запомнить все пароли, настоятельно рекомендуем использовать менеджер паролей для их хранения.

для защиты вашей домашней сети обеспечьте безопасность беспроводного соединения, регулярно обновляйте прошивки устройств и используйте пароли для всех устройств вашей сети.

Безопасность домашней сети

Есть вопросы по перечисленным пунктам? Задайте их провайдерам Интернета, посмотрите инструкцию к роутеру, точке доступа, или посмотрите веб сайты их производителей.

Безопасность ваших устройств

Следующим шагом является уточнение списка всех подключённых к сети устройств и обеспечение их безопасности. Это было легко сделать раньше, когда к сети было подключено небольшое количество устройств. Но в современном мире практически все устройства могут быть «постоянно подключены» к сети, включая телевизоры, игровые приставки, детские камеры, колонки, обогреватели или даже автомобили. Одним из простых способов обнаружить подключённые устройства является использование сетевого сканера, например, Fing. Это приложение, однажды установленное на компьютер, позволяет обнаружить абсолютно все устройства, подключённые к сети. После того, как вы обнаружите все устройства, следует позаботиться об их безопасности. Лучший способ обеспечить безопасность - регулярно обновлять их операционные системы/прошивки. Если возможно, настройте автоматическое обновление систем. Если есть возможность использовать пароль к каждому устройству, используйте только сильный и надёжный пароль. И, наконец, посетите веб сайт Интернет провайдера для получения информации о бесплатных способах защиты вашей сети.

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.

Ресурсы

Паролевые фразы:	https://securingthehuman.sans.org/ouch/2015#april2015
Менеджеры паролей:	https://securingthehuman.sans.org/ouch/2015#october2015
Безопасность планшета:	https://securingthehuman.sans.org/ouch/2016#january2016
Mapping Your Home Network:	http://l.rud.is/home-network-mapping

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