SANS SECURITY AWARENESS

OUCH! | Январь 2018

Ежемесячник по информационной безопасности для всех

OUCH!

В ЭТОМ ВЫПУСКЕ…

- Беспроводная сеть
- Ваши устройства
- Пароли
- Резервные копии

Кибербезопасность Вашего дома

Обзор

Несколько лет назад обеспечение кибербезопасности дома было очень простым; большинство домов имели только беспроводную сеть и несколько компьютеров. В наше время технологии шагнули далеко вперед и стали частью нашей жизни, от мобильных устройств и игровых приставок до домашних термостатов и даже холодильников. Вот некоторые шаги по обеспечению кибербезопасности дома.

Об авторе

Мэтт Бромили – специалист в области реагирования на происшествия информационной безопасности, помогающий своим клиентам, ставшим жертвами кибератак. Матт также является инструктором SANS, он преподает курс FOR508 «Продвинутый курс цифровой форенсики» и курс «Реагирование На Кибератаку». Блог Матта: **@mbromileyDFIR**.

Беспроводная сеть

В большинстве домов есть так называемая беспроводная сеть (Wi-Fi). С её помощью устройства соединяются с интернетом. Большинство беспроводных сетей контролируются роутером, или выделенной точкой доступа в интернет. Принцип работы этих устройств одинаковый: они транслируют беспроводные сигналы; устройства в вашем доме используют эти сигналы для связи. Безопасность вашей беспроводной сети является одним из ключевых компонентов защиты вашего дома. Мы рекомендуем следующие шаги:

- Измените пароль администратора вашего роутера или беспроводной точки доступа в интернет, установленный по умолчанию. Аккаунт администратора позволяет вам сконфигурировать вашу беспроводную сеть.
- Убедитесь, что сетью пользуются только люди, которым вы доверяете. Сконфигурируйте настройки сети, обеспечивающие надёжную защиту. В настоящее время лучшая защита - протокол WPA2. При активизации данной опции, беспроводная сеть будет запрашивать пароль для подключения к сети. После установления соединения, весь обмен данных в сети будет зашифрован.
- Доступ к сети следует защитить сильным и надёжным паролем, который отличается от пароля администратора. Вам следует ввести этот пароль всего один раз, ваши устройства сохранят его и будут подключаться автоматически.
- Большинство беспроводных сетей предоставляет возможность создания выделенной сети для гостей,

Кибербезопасность Вашего дома

к так называемой Гостевой Сети. Данная опция позволяет пользователям подключиться к интернету, но другие устройства, подключенные к вашей домашней сети, им недоступны. При подключении гостя к сети убедитесь, что используется протокол WPA2 и сеть защищена уникальным паролем доступа.

Не знаете, как следовать перечисленным шагам? Уточните у вашего интернет провайдера или изучите информацию на их сайте, ознакомьтесь с инструкцией к роутеру или беспроводной точке доступа или поищите информацию на соответствующих сайтах.

Четыре простых правила безопасности домашней сети: безопасность доступа к сети Wi-Fi, настройка автоматических обновлений, использование уникальных парольных фраз и создание резервных копий.

Ваши устройства

Следующий шаг – определить какие устройства подключены к домашней беспроводной сети и обеспечить их безопасность. Это просто, если вы пользуетесь одним или двумя компьютерами. В наше время практически любое устройство можно подключить к сети, включая смартфоны, телевизоры, игровые приставки, детские камеры, колонки или даже автомобили. Определив все устройства, подключенные к вашей сети, убедитесь что все они безопасны. Лучший способ – настройка автоматического обновления, если это возможно. Кибермошенники постоянно ищут новые уязвимости в различных устройствах и операционных системах. При настройке автоматического обновления компьютера и устройств, вы всегда будете работать с самыми последними версиями программ, которые намного сложней взломать.

Пароли

Следующий шаг – использование сильного и уникального пароля для каждого устройства и онлайн аккаунта. Ключевые слова «сильный» и «уникальный». Естественно, большое количество сложных паролей запомнить практически невозможно, ведь так? Поэтому воспользуйтесь парольными фразами. Это разновидность пароля, состоящая из серии слов, которые легко запомнить, например: «Где мой кофе?» или «Солнечный бублик радостно скрылся». Чем длинней парольная фраза, тем она безопасней. Под уникальным паролем подразумевается использование разных паролей для различных устройств и аккаунтов. В случае взлома одного из них, остальные будут в безопасности. Не можете запомнить уникальный и сильный пароль? Воспользуйтесь менеджером паролей – специальной программой, которая хранит ваши пароли в зашифрованном виртуальном «сейфе».

Кибербезопасность Вашего дома

По возможности, подключите двухступенчатую верификацию. Эта услуга обеспечит наилучшую защиту онлайн аккаунтов. Вам необходим не только пароль, но и второй шаг, например, код, отправленный на смартфон или приложение, которое генерирует уникальные коды доступа. Двухступенчатая верификация, пожалуй, самая сильная защита, которую можно обеспечить вашим аккаунтам. Пользоваться этой услугой намного проще, чем вы думаете .

Резервные копии

Иногда, несмотря на все предосторожности, ваши компьютеры и устройства могут взломать. В этом случае единственной возможностью восстановить данные будет резервная копия. Убедитесь, что вы регулярно делаете резервные копии данных и с них возможно восстановить данные. Большинство мобильных устройств делают резервные копии на Облаке автоматически. Для большинства компьютеров можно приобрести недорогие программы для создания резервных копий, которые довольно просты в обращении.

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 securingthehuman.sans.org/ouch/archives.

Ресурсы

Парольные фразы:	https://securingthehuman.sans.org/ouch/2017#april2017
Менеджер паролей:	https://securingthehuman.sans.org/ouch/2017#september2017
Надёжная защита вашего аккаунта:	https://securingthehuman.sans.org/ouch/2017#december2017
Резервное копирование и восстановление:	https://securingthehuman.sans.org/ouch/2017#august2017

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