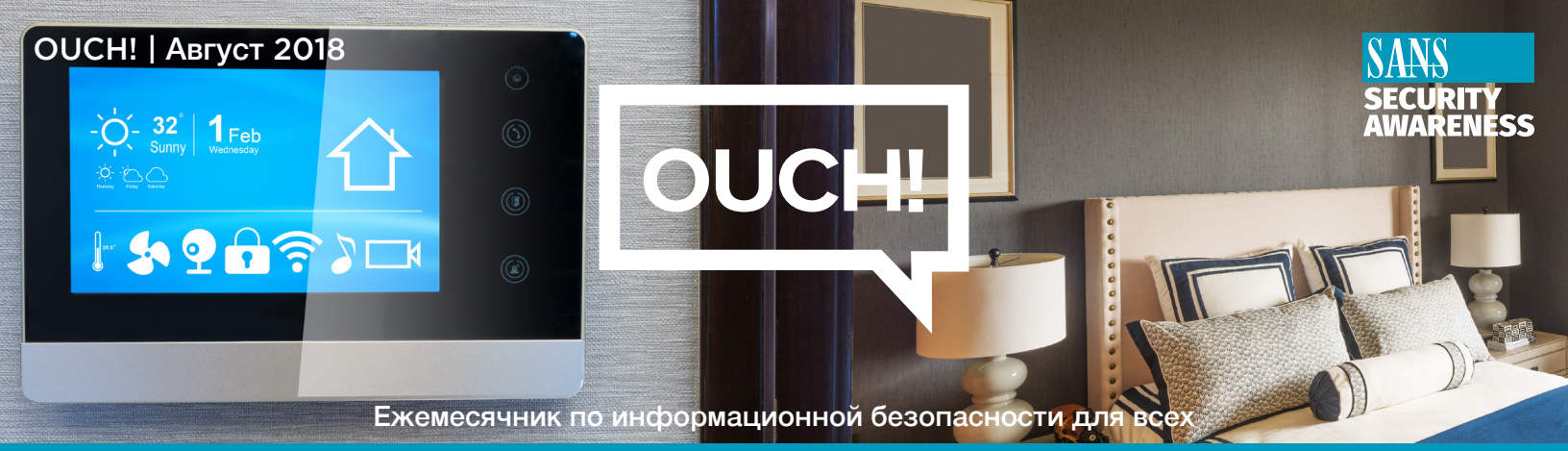
OUCH! | Август 2018



SANS SECURITY AWARENESS

OUCH!

Ежемесячник по информационной безопасности для всех

«Умные» домашние устройства

Что такое «умные» домашние устройства?

Совсем недавно к Интернету подключались только некоторые домашние устройства, например, ноутбуки, смартфоны или игровые приставки. Но в наше время все больше устройств подключены к Сети, от настольных ламп и колонок телевизора до замков на двери или даже автомобилей. В недалёком будущем каждое устройство в вашем доме, возможно, будет подключено к Интернету. Эти устройства, подключённые к Сети, называют «Интернет Вещей» (Internet of Things, IoT) или устройства «Умного Дома» (Smart Home). Эти вещи, помимо удобства, приносят и ряд опасностей в наш дом.

В чём заключается проблема?

Чем больше вещей в доме подключены к Интернету, тем больше рисков. Хакеры могут запрограммировать устройство для атаки других систем, поставщики могут собирать детальную информацию о вас и ваших действиях или ваши устройства могут быть инфицированы и действовать против вас. Большинство производителей этих устройств не имеют опыта в кибер защите и воспринимают её как дополнительные расходы. В результате, большинство устройств имеют очень примитивную защиту или не имеют её вовсе. Например, в некоторых устройствах установлен пароль по умолчанию, который все знают, и вы не можете его изменить или обновить.

Как себя защитить?

Что же делать? Мы хотим, чтобы вы пользовались устройствами безопасно. Ведь многие современные функции устройств упрощают нашу жизнь. С дальнейшим развитием технологий у вас, скорее всего, не будет шанса обходиться без таких устройств. Поэтому следуйте следующим правилам безопасности:

Подключайте устройства к сети только по мере необходимости: самый простой способ обезопасить устройство – не подключать его к Интернету. Если вы не выходите с устройства онлайн, то не стоит подключать его к домашней сети WiFi. Подумайте, действительно ли ваш тостер должен отправлять вам уведомления на смартфон?

Нужно точно знать, что подключено к сети: какие устройства подключены к вашей домашней сети? Не знаете или не можете вспомнить? Отключите ваш роутер и посмотрите, какие устройства перестали работать. Возможно, вы обнаружите не все устройства, но точно удивитесь тому, как много устройств вы забыли.

Регулярно обновляйте ваши устройства: также, как компьютер и мобильные устройства, необходимо регулярно обновлять все ваши устройства. Если есть возможность настроить автоматическое обновление, обязательно ей воспользуйтесь.

Пароли: смените все пароли на устройствах на уникальные, сильные и надёжные парольные фразы, известные только вам. Скорее всего, вам нужно будет разово их ввести. Не можете их все запомнить? Не переживайте, никто не может. Воспользуйтесь менеджером паролей для их безопасного хранения.

Настройки конфиденциальности: если в вашем устройстве можно ограничить количество информации, которую оно собирает и передаёт, воспользуйтесь этой функцией. Лучше всего совсем отключить функцию сбора и передачи данных.

Поставщики: покупайте устройства только у известных и проверенных временем производителей. Выбирайте продукцию с возможностью модификации настроек безопасности, смены паролей и автоматического обновления.

Постоянная прослушка: если устройство поддерживает голосовые команды, то оно постоянно прослушивает ваш дом. Например, Алекса или Google Home могут записывать конфиденциальные разговоры. Поэтому следует внимательно выбирать место для таких устройств и сконфигурировать настройки конфиденциальности.

Гостевая сеть: «умные» устройства следует подключать к отдельной гостевой сети WiFi; не стоит использовать общую сеть с компьютерами и мобильными устройствами. В случае, если устройство будет инфицировано, ваши компьютеры или мобильные устройства будут в безопасности.

Нет причин избегать современные технологии, но следует понимать опасность, которую они несут. Следуя этим простым правилам, вы обеспечите безопасность «умному» дому.

Об авторе

Роберт М Ли *(@RobertMLee) – сертифицированный инструктор Института SANS и автор курсов FOR578 – Интеллектуальные кибер угрозы и ICS515 - ICS Активная защита и действия в случае атаки. Роберт является основателем и CEO компании Dragos, предоставляющей кибер защиту в индустриальной сфере.*

Ресурсы

Парольные фразы:	https://www.sans.org/u/GEB
Менеджер паролей:	https://www.sans.org/u/GEG
Безопасность домашней сети:	https://www.sans.org/u/GEL

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». *Редакция: Уолт Скривенс, Фил Хоффман, Кэти Клик, Шерил Конли | Русский перевод: Александр Котков, Ирина Коткова*