Ежемесячник по информационной безопасности для пользователей

OUCH!

В ЭТОМ ВЫПУСКЕ…

Интернет вещей (IoT)

Что такое Интернет вещей?

Об авторе

Джеймс Лин (@jameslyne) – руководитель отдела исследований информационной безопасности компании Sophos. Джеймс называет себя «Компьютерщик до мозга костей». У него глубокие технические знания во многих областях информационной безопасности. Джеймс - сертифицированный инструктор Института SANS. Он часто выступает на профессиональных конференциях.

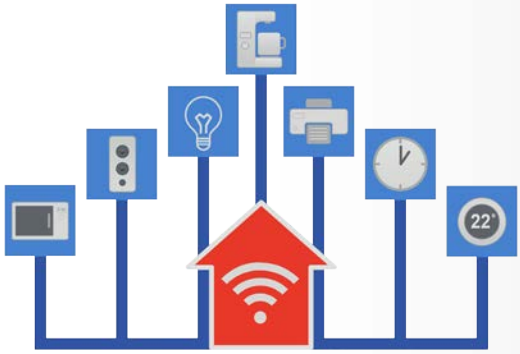
Не так давно, технологии были довольно простыми: вы просто подключали компьютер к Интернету и использовали его для своих повседневных дел. Но технологии развивались и в нашу жизнь вошли мобильные устройства, такие, как смартфоны и планшеты. В этих устройствах возможностей не меньше, чем в ноутбуке, и они очень компактны. В силу мобильной сущности этих устройств, они создали новые, уникальные проблемы безопасности. Сейчас самой важной новой технологией стал Интернет вещей. Интернет вещей (Internet of Things, или сокращенно IoT) - это все устройства или вещи, которыми мы пользуемся ежедневно и которые можно подключить к Интернету, например, дверной звонок, светильник, термостат или игрушка. Все эти устройства намного облегчают нам жизнь: например, свет может включиться автоматически, как только ваш телефон определит, что вы подошли к дому. Рынок IoT растет быстрыми темпами, каждый день появляются какие-то новинки. Подобно мобильным устройствам, IoT вещи тоже имеют свои особенности в обеспечении их безопасности. В этом выпуске мы поговорим о рисках и о способах обеспечения безопасности IoT устройств, вашего дома и, в конечном итоге, вашей семьи.

Проблемы Интернета вещей

Достоинство IoT устройств в том, что большинство этих устройств очень простые. Например, вы можете подключить к вашей домашней Wi-Fi сети кофе-машину. Однако за все приходится платить. Самая большая проблема заключается в том, что большинство производителей IoT устройств не имеют опыта обеспечения безопасности бытовой техники, которую производят. Некоторые производители - новички на рынке; их цель – быстро и с наименьшими затратами разработать новинку и вывести её на рынок, например, через Kickstarter. Эти компании сосредоточены на прибыли, а не на безопасности. Результатом этого является то, что большинство устройств IoT имеют очень слабую защиту или её нет совсем. В некоторых устройствах установлены стандартные пароли, которые можно найти в Интернете, и их нельзя изменить. Кроме того, в

Интернет вещей (IoT)

большинстве IoT устройств даже нет возможности их сконфигурировать, вы можете использовать только стандартную заводскую конфигурацию. Многие из этих устройств очень сложно или невозможно обновить. В результате, эти устройства очень быстро устаревают, их уязвимости становятся хорошо известными, и нет возможности их устранить. Всё это делает вас уязвимым.



Если вы знаете, какие IoT устройства подключены к вашей сети, изолируйте их, если возможно; обновляйте их и защитите их с помощью сильных парольных фраз.

Защита Интернета вещей

Возникает вопрос: что же делать? Мы расскажем, как использовать Интернет вещи эффективно и безопасно. У этих устройств есть возможности сделать вашу жизнь проще, сэкономить деньги и даже повысить физическую безопасность вашего дома. Кроме того, по мере развития технологий, у вас может не быть другого выбора, кроме как купить или использовать IoT вещи. Следующие шаги помогут вам защитить IoT устройства и себя.

- **Подключайте к сети только то, что действительно вам нужно**: Самый простой способ защитить устройство – не подключать его к Интернету. Если вам не нужно подключать устройство к сети, отключите его от сети Wi-Fi.
- **Разделите сеть Wi-Fi**: Если вам действительно нужно подключить IoT устройства к интернету, создайте для них отдельную сеть. Многие точки входа Wi-Fi позволяют сконфигурировать отдельные сети, например, для гостей. Другой вариант: купить дополнительную точку входа специально для IoT устройств. Это поможет обеспечить устройству отдельный выход в Интернет. В случае взлома этой сети, ваш компьютер и мобильные устройства, подключённые к основной сети (которая является приоритетным интересом кибер преступников), будут в безопасности.
- **Обновляйтесь, если возможно**: обновляйте ваши IoT устройства, также, как вы обновляете свой персональный компьютер или мобильное устройство. Если есть возможность настроить автоматическое обновление IoT устройства, воспользуйтесь ей.
- **Защитите сильным паролем**: смените пароль, поставленный производителем и установите сильный, уникальный пароль, который будете знать только вы. Сложно запомнить все пароли? Не

Интернет вещей (IoT)

расстраивайтесь, никто не может. Попробуйте использовать менеджер паролей для их хранения.

- **Настройки приватности**: Если у вашего IoT устройства есть настройки приватности, максимально ограничьте с их помощью обмен данными. Оптимальный вариант - воспользоваться настройкой, запрещающей любой обмен данными.
- **Подумайте о замене**: В некоторых случаях стоит рассмотреть возможность замены IoT устройства, если оно устарело и у него слишком много уязвимых мест, которые нельзя исправить или в новом устройстве защита намного лучше.

Нет универсальных советов для всех устройств, поэтому стоит учитывать мировой опыт и читать публикации по безопасности этих устройств. К сожалению, многие IoT устройства были разработаны без учёта требований безопасности, поэтому производители и не предоставляют достаточной информации о их безопасности. Но осведомлённость в сфере информационной безопасности растёт, и мы надеемся, что все больше и больше производителей будут встраивать системы защиты в IoT устройства и обеспечат их информационную поддержку и обновления.

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
Безопасность домашней сети:	https://securingthehuman.sans.org/ouch/2016#february2016
Интернет вещей:	https://ru.wikipedia.org/wiki/Интернет_вещей
Интернет вещей небезопасен:	http://www.gazeta.ru/tech/2014/07/30_a_6152017.shtml

OUCH! выпускается Институтом SANS в рамках программы «Securing The Human». Распространение журнала регулируется Creative Commons BY-NC-ND 4.0 license. Вы можете использовать и распространять журнал при условии, что ничего не будете менять. Для перевода или получения более подробной информации, пожалуйста, обращайтесь: ouch@securingthehuman.org

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

