

Топ-10 вещей, которые могут быть неожиданно легко взломаны

Скандальные новости о хакерах не покидают СМИ вот уже несколько лет.

Атаки на правительственные сайты, игровые платформы, услуги стриминга нарушают спокойное течение жизни миллионов людей.

Большинство взломов приходится на смартфоны и компьютеры, но это далеко не единственные устройства, подверженные атакам хакеров. Все, что подключается к Интернету или беспроводным сетям, рискует быть взломанным.

10. Телевизоры



Большинство новых телевизоров уже не просто устройства, которые получают сигнал через спутник или кабель. Они способны подключаться к Интернету и предоставлять доступ к различным приложениям и услугам. Исследования, проведенные экспертами по безопасности, показали, что современные телевизоры также уязвимы для взломов, как и телефоны и компьютеры. Вредоносный код может быть занесен через Skype, Twitter и Facebook. Кроме того, такой телевизор может быть использован в качестве составной части ботнета или использовать встроенную камеру для того, чтобы шпионить за людьми. Многие телевизоры становятся легкой добычей для хакеров, предоставляя им полный доступ к конфиденциальной информации их владельцев.

9. Туалеты



Это, наверно, одно из самых безопасных мест с точки зрения взломов. Казалось бы, какие технологии могут понадобиться вам в унитазах? Хотя многие компании не согласятся с вами, поскольку считают, что электронные туалеты – часть нашего будущего. Эти новинки уже прочно обосновались в Японии, так что не за горами тот день, когда у каждого будет свой унитаз с выходом в Интернет.

Что касается безопасности, компания Trustwave обнаружила уязвимость таких унитазов в 2013 году. Поскольку большей частью таких девайсов можно легко управлять через блютуз при помощи специального приложения для смартфонов, также легко их можно и взломать. Доступ к унитазу позволит злоумышленникам постоянно сливать воду, открывать и закрывать крышку и активировать функцию биде, разбрызгивая воду под высоким давлением.

8. Принтеры



Ряд исследований показали, что принтеры так же легко подвержены взломам. Слабое шифрование позволяет всем недоброжелателям внедрить в прошивку принтера свой код и получить полный контроль над ним. Такое стало возможным по причине того, что большинство современных принтеров подключены к вай-фаю. Некоторые эксперты полагают, что несанкционированный доступ может привести к печальным последствиям, вплоть до самоуничтожения принтера. Пару строк кода могут отключить работу тепловых датчиков и принтер может загореться. Кроме того, не следует упускать из виду такую проблему, как похищение конфиденциальной информации.

7. Ключи от автомобиля



Современные автомобили по большей части уже не требуют механического ключа для того, чтобы открыть двери и завести двигатель, для этого обычно достаточно наличия электронного ключа. Самым простым способом взломать систему автомобиля является брутфорс, поскольку многие производители опрометчиво используют шестизначные числа в качестве кода доступа. Более сложным способом является использование специального набора для перехвата сигнала от электронного ключа с последующим перепрограммированием его на другой ключ.

6. Банкоматы



Малоизвестный факт о банкоматах состоит в том, что 95% из них работают на Windows XP. Уже одно это делает их уязвимыми к массе вредоносного кода, который был разработан для этой операционной системы. Более серьезная проблема состоит в том, что Microsoft прекратили официальную поддержку этой системы, начиная с 2014 года. Это означает, что никаких обновлений безопасности для банкоматов больше не будет. Для перевода банкоматов под более современные операционные системы потребуется огромное количество инвестиций и времени. Все вышеперечисленное делает банкоматы уязвимыми для взломов и клонирования кредитных карт.

5. Холодильники



В 2013 году калифорнийская компания по электронной безопасности Proofpoint выявила несколько уязвимостей, которые могли бы быть опасными для бытовой техники. Что самое интересное, больше всего были подвержены этим уязвимостям современные холодильники, позволяющие владельцам контролировать их температуру и содержать еду в необходимых условиях.

Взлом таких «умных» холодильников обычно является легкой задачей, поскольку большинство их владельцев даже не удосуживаются сменить стандартный пароль, либо не ставят его вообще. Хакеры используют такие холодильники в качестве ботнета для рассылки спама, в то время как законные владельцы ничего не подозревают.

4. Детские мониторы



За последнее десятилетие технологии, используемые в детских мониторах, становились все более сложными, позволяя родителям следить за детьми более качественно. Тем не менее, такой скачок в развитии привел к тому, что они стали легкой добычей для хакеров. Некоторые модели постоянно отсылают сигналы, позволяя любому, кто находится в радиусе приема перехватывать все сообщения. То же самое касается и видеонаблюдения. Незапароленные мониторы позволяют любому желающему шпионить за помещением, что обычно не приводит ни к чему хорошему.

3. Автомобильные тормоза



Все чаще в автомобилях применяется электронная система контроля за их важнейшими функциями. В последнее время широкую популярность набирает электронный контроль торможения, вытесняющий механический. Исследователи из Университета Калифорнии и Университета штата Вашингтон смогли воспользоваться уязвимостями бортовых компьютерных систем и перехватить контроль над тормозами. Надеемся, что все представляют очевидную угрозу таких ситуаций в реальной жизни.

2. Сигналы светофоров



Эксперименты, проведенные исследователями, показали, что светофоры так же могут быть взломаны, наравне с остальной электроникой. Ряд эксплойтов позволяет контролировать и вовсе отключать светофоры. Что самое печальное – здесь не используется никакого шифрования сигналов, поэтому любой хакер способен перехватить и изменить информацию, поступающую из центров управления дорожным движением.

1. Медицинские имплантаты



Миллионы людей во всем мире уже пользуются медицинскими имплантатами. С каждым новым годом имплантаты становятся все более совершенными с точки зрения инноваций. К примеру, уже стало возможным управлять кардиостимуляторами при помощи специальных пультов дистанционного управления, которые позволяют корректировать работу устройства без необходимости хирургического вмешательства. Единственное, что вызывает тревогу, так это недостаточный уровень защиты имплантатов. Согласно многим исследованиям, устройства уязвимы для целого ряда угроз безопасности. Любое вмешательство посторонних может стать фатальным для обладателей таких устройств.

