Kp.ru, Москва, 25 марта 2020

БЕЗОПАСНЫЙ УМНЫЙ ДОМ: УЯЗВИМОСТИ РОБОТА-ПЫЛЕСОСА

По данным экспертов количество умных устройств, подключенных к интернету вещей превысило 22 млрд

При помощи wi-fi пользователи включают чайник, регулируют мощность лампочек, заряжают телефоны. Умные гаджеты делают жизнь намного проще. Тем не менее, при их использовании стоит соблюдать осторожность, ведь они все чаще становятся объектами опасных кибератак. Так, в феврале 2020 года компания ESET провела исследование, по результатам которого, что своей безопасностью рискуют более половины пользователей умных гаджетов в России.

Уязвимости умных гаджетов

К сожалению, во многих гаджетах просто не предусмотрена надежная система защиты от взлома. При этом подключившись к вашей домашней сети, они способны открыть брешь, через которую преступник может получить доступ к вашим личным устройствам: смартфонам, компьютерам.

Например, владельцы популярных IP-камер рискуют оказаться жертвами шпионажа. Более того, существует потенциальная опасность, что камера станет частью ботнета - преступной компьютерной сети.

Кроме того, исследователи из Мичигана обнаружили уязвимости в умных колонках и голосовых помощниках. Они позволяли злоумышленникам отправлять команды на устройства и с их помощью открывать умные замки и осуществлять другие действия, позволяющие получить доступ к домашней сети.

Наконец, следует помнить об уязвимостях умных гаджетов, предназначенных для детей; ведь они тоже - компонент семейной системы безопасности. Так, детские часы с возможностью GPS-трекинга в руках злоумышленника превращаются в устройство для слежки.

Как сделать умный дом безопаснее

Несколько простых правил помогут защитить домашнюю сеть от киберугроз при внедрении в нее умных гаджетов.

• В первую очередь, следует приобретать умные устройства от известных производителей в надежных, проверенных магазинах. Внимательно изучите рынок, почитайте отзывы.

• Не стоит покупать б/у гаджеты. Предыдущий владелец мог намеренно изменить прошивку с целью захватить умный дом нового владельца.

• Обязательно установите сложные, неочевидные пароли на смартфонах, компьютерах, роутерах. При создании аккаунтов в приложениях для управления умными устройствами, заведите дополнительные номер телефона и адрес e-mail и не сообщайте их никому. Таким образом вы усложните задачу хакеру, желающему проникнуть в вашу домашнюю сеть.

• Не используйте один и тот же пароль на всех устройствах.

• Воздержитесь от желания похвастаться в социальных сетях фотографиями новеньких телевизора или колонки-голосового помощника. Не распространяйтесь о том, какие именно модели умных гаджетов вы используете дома. Тем более, не сообщайте никому их серийный номер и прочие технические данные. Злоумышленник может представить мастером по ремонту и настройке и попытаться выманить указанную информацию. Эти сведения упростят для него возможность взлома вашей домашней сети.

• Необходимо своевременно устанавливать обновления на все гаджеты, поскольку в них содержатся исправления уязвимостей прошивки.

Итак, жить в умном доме приятно и удобно. Запланировать уборку для робота-пылесоса можно за пару часов до возвращения после тяжелого дня. Мультиварка подогреет остывший ужин. Однако во всем этом комфорте важно оставаться бдительным и не полагаться на производителей умных гаджетов в вопросах личной безопасности. ESET предлагает комплексное антивирусное решение для защиты домашней сети от вторжения - ESET NOD32 Internet Security.

https://www.kp.ru/daily/27108/4183908/