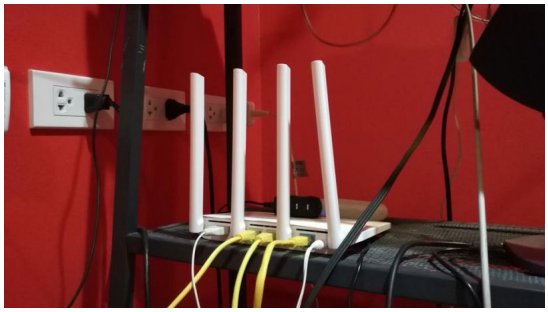
Европейские специалисты обнаружили очередную уязвимость Wi-Fi. Причём такую, что она потенциально угрожает не только роутерам, но и вообще всем гаджетам, которые используют Wi-Fi. А ведь это — только одно из несовершенств беспроводной связи. Лайф разбирался, чем воры взламывают беспроводные сети и как защититься от вторжения.

Производители закрывают глаза на уязвимости

Ещё в 2014 году специалисты компании Tripwire выяснили, что 20 из 25 самых

популярных модемов для дома и малого бизнеса уязвимы для взлома уже из коробки. Производители знают о многих уязвимостях, но по каким-то причинам их не "латают". Как следствие, часто хакерские атаки на роутеры носят стихийный характер. Один из показательных случаев произошёл в 2017 году: зловредная программа Mirai всего за 60 часов взломала около 100 000 устройств компании ZyXEL.



Чужие Wi-Fi-устройства используются как оружие

Изучение электронных писем пользователя подарит злоумышленникам много ценного: например, пароли и логины от соцсетей, данные с карт или геолокацию. Также взломанные Wi-Fi-гаджеты нередко становятся оружием в ходе масштабных DDoS-атак. В 2016 году одна из разновидностей упомянутой Mirai захватила кучу устройств и помогла хакерам вызвать сбои в работе Twitter, Periscope, PlayStation Network и других крупных онлайн-сервисов. Самой же приземлённой и популярной причиной взлома домашних Wi-Fi-точек является бесплатный и безлимитный интернет-трафик.

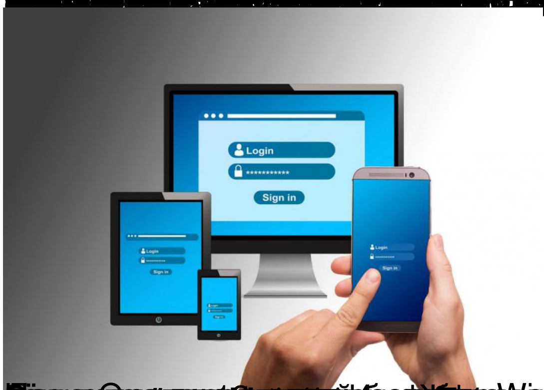
Взломать можно всё

У каждой Wi-Fi-сети есть свой протокол защиты. Самые популярные — WEP, WPS, WPA или WPA2. Все они отличаются методами шифрования. Они кодируют информацию между передатчиком (роутером) и приёмником (например, смартфоном) так, чтобы понимали её только два устройства. Шифруются в том числе и коды, которые пользователи вводят при подключении к роутерам. Суть любого взлома Wi-Fi — поиск этого самого PIN'a. На сегодня его можно подобрать, дешифровать или узнать обманом практически во всех случаях. Вопрос только в количестве затраченного времени. Чем сильнее устарел протокол защиты, тем быстрее "пойдёт" процесс. Начнём с WPS. Так как WPE настолько древний, что взламывается за секунды, сейчас им почти не пользуются.

Хакеры любят ленивых

WPS (Wi-Fi Protected Setup) — это стандарт защиты, придуманный для ленивых. В случае с WPS для настройки Wi-Fi дома пользователю достаточно воткнуть вилку в розетку, нажать на модеме кнопку WPS и ввести на компьютере 8-значный числовой код. Он чаще всего напечатан на корпусе модема.

Собственно, из-за последнего специалистами WPS считается одним из самых "дырявых". PIN-код из цифр легко вычисляется брутфорсом. Брутфорс — метод взлома, в ходе которого PIN-код находится перебором чисел. Легко это потому, что математически пароль из 8 чисел имеет всего 100 млн комбинаций.



которые, только, всем, одно, ведь, используют, сети, беспр