

Россиянам рассказали, как понять, что к вашему Wi-Fi подключились посторонние

Эксперты предупреждают, что незаметное подключение посторонних к домашнему Wi-Fi-роутеру может стать серьёзной проблемой для владельцев. Признаками чужого доступа обычно становятся замедление скорости интернета и периодические обрывы связи, рассказал специалист по ИТ Павел Мясоедов. Иногда о взломе сигнализируют моргающие индикаторы на роутере, когда никто из домочадцев не пользуется сетью. Ещё один способ проверить подозрения — посмотреть через личный кабинет провайдера, сколько данных скачивается. Если трафик неожиданно вырос, значит, кто-то подключился к вашей сети.

Более продвинутые пользователи могут зайти в настройки роутера, где отображаются все активные подключения и объем трафика. Мясоедов объяснил, что каждый выход в интернет называется [сессией](#), и в админке роутера можно увидеть их количество за день и сколько данных было передано. Это помогает понять, сколько людей одновременно пользуются вашим Wi-Fi.

Помимо обычных пользователей, к домашней сети могут подключиться и злоумышленники. Эксперт по [кибербезопасности](#) Алексей Курочкин предупреждает, что таким образом [хакеры](#) получают доступ ко всем гаджетам, подключённым к роутеру. Это может привести к краже личных данных, установке [вредоносных программ](#) или даже удалению файлов. Курочкин добавил, что если через ваш Wi-Fi кто-то совершит преступление, правоохранители выйдут на вас, что хотя и не грозит наказанием, создаст серьёзные проблемы.

Чтобы защитить домашнюю сеть, специалисты советуют ставить сложные пароли и менять их регулярно. В настройках роутера можно ограничить доступ, составив список разрешённых устройств и блокируя подозрительные подключения. Генеральный директор Telecom Daily [Денис Кусков](#) отметил, что опасность есть и при использовании мобильной [точки](#) доступа. Подключившись к смартфону, злоумышленники смогут увидеть всю информацию на телефоне, включая банковские приложения. Поэтому не стоит давать интернет незнакомцам и всегда ставить сложный пароль на [точку](#) доступа, рекомендовал он.