В 2024 году в России зарегистрировано более 765 тысяч киберпреступлений — это показывает, насколько важно защищать личные данные даже дома. Эксперты провайдера цифровых услуг Дом.ру рассказали, с чего начать — с домашнего Wi-Fi.

- **Сложный и уникальный пароль.** Главное правило — надежный пароль для сети. Лучше использовать случайную комбинацию длиной от 12 символов, где есть заглавные и строчные буквы, цифры и специальные знаки. Пароль для Wi-Fi должен отличаться от всех остальных, особенно от пароля для доступа к настройкам роутера.
- **Название сети (SSID).** Часто Wi-Fi по умолчанию носит имя модели роутера. Это облегчает задачу злоумышленникам — они могут определить тип оборудования и использовать уязвимости. Уникальное название сети, не связанное с брендом или вашими данными, снижает риски.
- **Обновления прошивки.** Как и любой гаджет, роутер нуждается в регулярных обновлениях. Они устраняют уязвимости и повышают защиту. В новых моделях возможна автоматическая установка обновлений. Если у вас старая модель — проверяйте прошивку вручную через веб-интерфейс.
- **IP-адрес и DNS.** Роутеры часто используют стандартный IP-адрес, известный хакерам. Его стоит изменить в настройках. Также рекомендуется сменить DNS-сервер — это повысит фильтрацию интернет-трафика и добавит уровень защиты от вредоносных сайтов.
- **Контроль подключенных устройств.** Регулярная проверка подключений к сети позволяет выявить незваных гостей. Сделать это можно через настройки роутера или через приложение, если оно предусмотрено. Некоторые антивирусные программы также оповещают о новых устройствах.
- **Гостевая сеть.** Для гостей лучше настроить отдельную сеть с другим паролем. Это не даст им доступа к вашим основным устройствам и локальным данным.
- **Использование современного шифрования.** Если ваш роутер поддерживает стандарт WPA3 — используйте его. Это самый защищенный протокол на сегодняшний день. Устройства с поддержкой WPA2/WPA3 позволяют обеспечить безопасность и сохранить совместимость со старыми гаджетами. Например, такая функция есть у роутера Дом.ру WAVE.

Никита Шешин, эксперт по продукту Wi-Fi компании Дом.ру, отметил, что незащищенная домашняя сеть может привести к утечке личных данных, финансовым потерям и даже физическому повреждению подключенных устройств через вредоносное ПО. Взлом роутера позволяет злоумышленникам перенаправлять пользователей на фишинговые сайты, устанавливать вредоносные программы,

перехватывать трафик, использовать роутер для DDoS-атак или скрытого майнинга криптовалют.