VPN-сервисы: Новая угроза для конфиденциальности пользователей

10.11.2025

Новая волна интереса к VPN-сервисам возникла на фоне блокировки звонков в мессенджерах WhatsApp и Telegram (принадлежат компании Meta, которая признана в России экстремистской и запрещена). Выросло и количество мошенничеств в сети, в том числе, связанных с использованием сервисов для обхода блокировки зарубежных сайтов. В 2025 году интернет и телефонные мошенники выманили у россиян более 120 млрд руб.

Мошенники представляются сотрудниками госслужб, при этом выманивают коды для доступа к банковским счетам или сайтам с конфиденциальными данными. В 2025 году на фоне растущего интереса к VPN-сервисам мошенники освоили один из самых коварных способов обмана. Они создают поддельные сервисы для обхода блокировок, которые вместо защиты данных пользователей передают их киберпреступникам.

Иногда данные продают в компании по настройке рекламы, что тоже нарушает личное пространство пользователя, который не давал на это согласие. В результате возникает ситуация, когда человек не оставлял номер телефона на сомнительных сайтах, но номер вместе с другими важными сведениями попал к мошенникам.

Название VPN-сервисов расшифровывается как Virtual Private Network («виртуальная частная сеть»), что создает иллюзию безопасности. Такие сервисы действительно создают закрытый «туннель» связи между пользователем и сервером VPN-провайдера. Но как будут использованы эти данные — вопрос не только порядочности VPN-провайдера.

Даже если провайдер старается сделать все, чтобы защитить данные пользователей, надежная защита требует больших вложений, а любой недостаточно

защищенный криптографически протокол может привести к потере данных. Именно поэтому надежные VPN-сервисы не бывают бесплатными. По данным исследования Group-IB, в 2025 году каждый третий россиянин, скачавший VPN из непроверенного источника, становился жертвой утечки данных.

В платных сервисах подобного рода тоже скрываются свои подводные камни. Один из самых очевидных — подключение подписки, которую бывает не просто отключить. В итоге деньги утекают со счета даже тогда, когда человек уже перестал пользоваться VPN-сервисом.

Только в течение первого полугодия Банк России заблокировал 11 тысяч интернет-ресурсов, принадлежащих нелегалам. Такие сайты строятся по шаблонам, требуют для регистрации коды sms-подтверждения. Чаще всего это сайты для получения кредитов, доступа к криптокошелькам и финансовым ресурсам, заблокированным Роспотребнадзором в целях безопасности.

Если VPN-сервис используется только для доступа к запрещенным социальным сетям, во время его работы в закрытый «туннель» передачи данных может попасть то, что пользователь не хотел бы разглашать. Особенно, если VPN работает во время звонков через мессенджеры, через которые зачастую пересылается очень личная информация. Весь цифровой след в сети — пароли к аккаунтам в социальных сетях, к банковским счетам, цифровые токены оказываются у мошенников.

Современная криптографическая защита требует значительных средств, поэтому имя компании и ее действие в правовом поле сегодня не пустой звук. В мире, где страны находятся в противостоянии, опасность могут представлять многие зарубежные бесплатные приложения, которые пользователи массово скачиваются с Google Play и AppStore, становясь мишенью для кибермошенников.

Эксперты по кибербезопасности предупреждают — не стоит подключать сервисы, которые намеренно могут передать контроль над данными третьим лицам или стать причиной утечки личных данных.