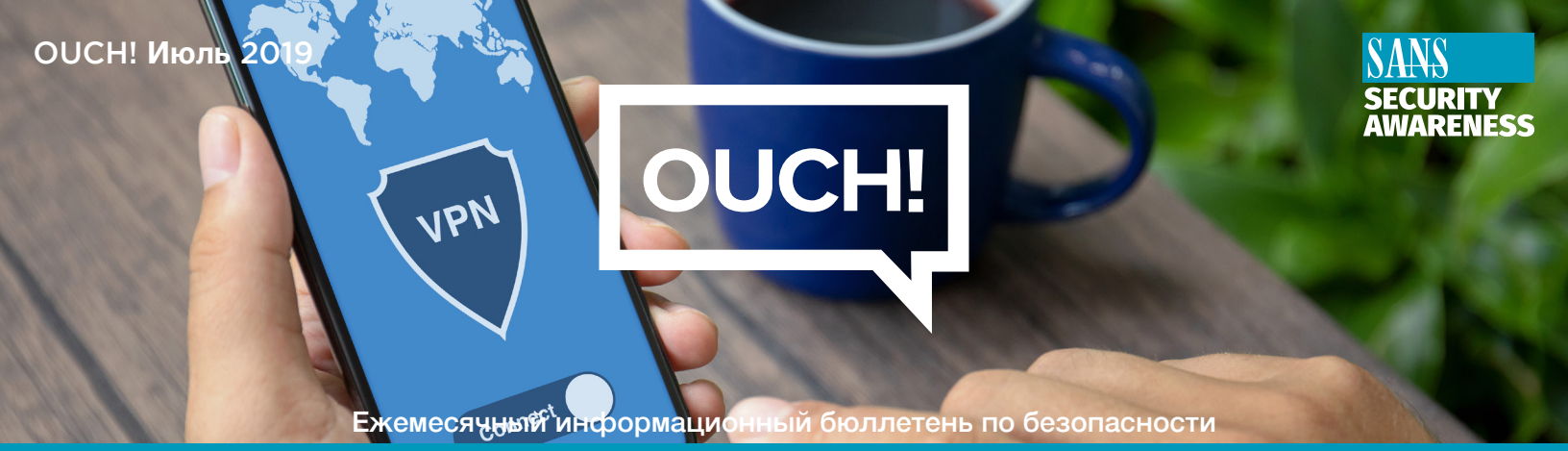


Ежемесячный информационный бюллетень по безопасности

# Виртуальные частные сети (VPN)

## Обзор

Вам может понадобиться использовать общедоступный Wi-Fi для доступа к Интернету, когда вы вдали от дома, например, когда вы находитесь в местном ресторане или кафе или когда вы путешествуете в отеле или аэропорту. Но насколько безопасны эти публичные сети, и кто смотрит или записывает то, что вы делаете в Интернете? Возможно, вы не доверяете своему ISP (интернет-провайдеру) дома и хотите быть уверенным, что он не может отслеживать, что вы делаете в Интернете. Защитите свою деятельность и конфиденциальность в Интернете с помощью так называемой VPN (виртуальной частной сети). VPN - это технология, которая создает частный, зашифрованный туннель для вашей онлайн-активности, что значительно усложняет наблюдение или мониторинг того, что вы делаете в сети. Кроме того, VPN помогает скрыть свое местоположение делает его гораздо сложнее, для веб-сайтов, которые вы посещаете, чтобы определить, где вы находитесь.

## Как это работает?

VPN работает путем создания частного зашифрованного туннеля к выбранному вами провайдеру VPN. Вся ваша онлайн-активность проходит через этот туннель, а затем покидает сеть вашего VPN-провайдера по назначению. Например, если вы находитесь в Тампа, штат Флорида, и подключаетесь к VPN-серверу в Мюнхене, Германия, любой веб-сайт, к которому вы подключаетесь, будет думать, что вы подключаетесь из Мюнхена, Германия. VPN прост в использовании. Первым шагом является поиск VPN-провайдера, которому вы доверяете, а затем создание учетной записи с ним (для этого обычно требуется покупка их услуги). Получив учетную запись, вы загружаете, устанавливаете и настраиваете их программное обеспечение VPN. После установки и настройки вы как обычно подключаетесь к Интернету. Программное обеспечение VPN автоматически создаст ваш зашифрованный туннель и начнет защищать вашу конфиденциальность, даже если вы этого не осознаете.

## Выбор провайдера VPN

Ваша онлайн-деятельность является настолько же безопасной и конфиденциальной, как и ваш поставщик VPN. Обязательно выберите того, которому вы можете доверять. Вот ключевые моменты при выборе поставщика услуг VPN.

⚠ **Ведение журнала: ищите службу, которая не ведет журналы и фокусируется на конфиденциальности. Если ваш поставщик услуг VPN не собирает какие-либо журналы, кому-то намного труднее вернуться назад и посмотреть, что вы сделали в Интернете.**

**Где находится компания:** Разные провайдеры VPN находятся в разных странах. Убедитесь, что вы выбрали провайдера VPN, базирующегося в стране, в которой действуют строгие законы о конфиденциальности. Провайдеры VPN, расположенные в странах с очень небольшим или слабым законодательством о конфиденциальности, могут быть вынуждены отказаться от информации, которую они собирают о вас.

**Серверы:** найдите службу VPN, в которой есть серверы, расположенные в нужных вам странах или городах. Некоторые провайдеры VPN имеют тысячи серверов и мест по всему миру. Вам нужно, чтобы ваши соединения выглядели так, как будто они приходят из определенной страны, может ли ваш провайдер VPN предоставить их?

**Совместимость:** ищите сервисы, которые работают на разных компьютерах и мобильных устройствах. Например, вы можете использовать ноутбук с Windows, планшет и iPhone. Вам понадобится VPN-сервис, который будет работать на всех этих устройствах.

**Избегайте бесплатных :** будьте очень осторожны с «бесплатными» VPN-сервисами, как они зарабатывают деньги и остаются в бизнесе? Бесплатные сервисы могут собирать и продавать вашу информацию.

VPN - это фантастический способ защитить вашу конфиденциальность в Интернете. Однако VPN ничего не делает для защиты вашего компьютера, устройств или ваших сетевых учетных записей. Поэтому, даже если вы используете VPN, убедитесь, что вы всегда следуете основным шагам безопасности, включая обеспечение обновления ваших устройств, использование блокировки экрана и всегда используйте надежные уникальные пароли для всех ваших учетных записей.

## Приглашенный

***Фил Джонси*** *(@peakreflections) - ИТ-специалист в округе Палм-Бич, имеющий опыт работы в области безопасности, криминалистики и аудита. SANS сертифицирован в цифровой криминалистики, необходимости обеспечения безопасности, а также член комиссии по рассмотрению сообщества OUCH. Его страсть делает безопасность простой для других.*

## Ресурсы

| | |
|---|---|
| Персональные атаки: | https://www.sans.org/u/Sd8 |
| Защита ваших мобильных устройств: | https://www.sans.org/u/Sdd |
| Остановить вредоносное ПО: | https://www.sans.org/u/Sdi |

*OUCH! публикуется SANS Security Awareness и распространяется под лицензией Creative Commons BY-NC-ND 4.0. Вы можете свободно распространять этот информационный бюллетень или использовать его в своей информационной программе, если вы не вносите изменения в информационный бюллетень. Для перевода или получения дополнительной информации, пожалуйста, свяжитесь с www.sans.org/security-awareness/ouch-newsletter. Редакция журнала: Уолт Скривенс, Фил Хоффман, Алан Ваггонер, Шерил Конлиie*