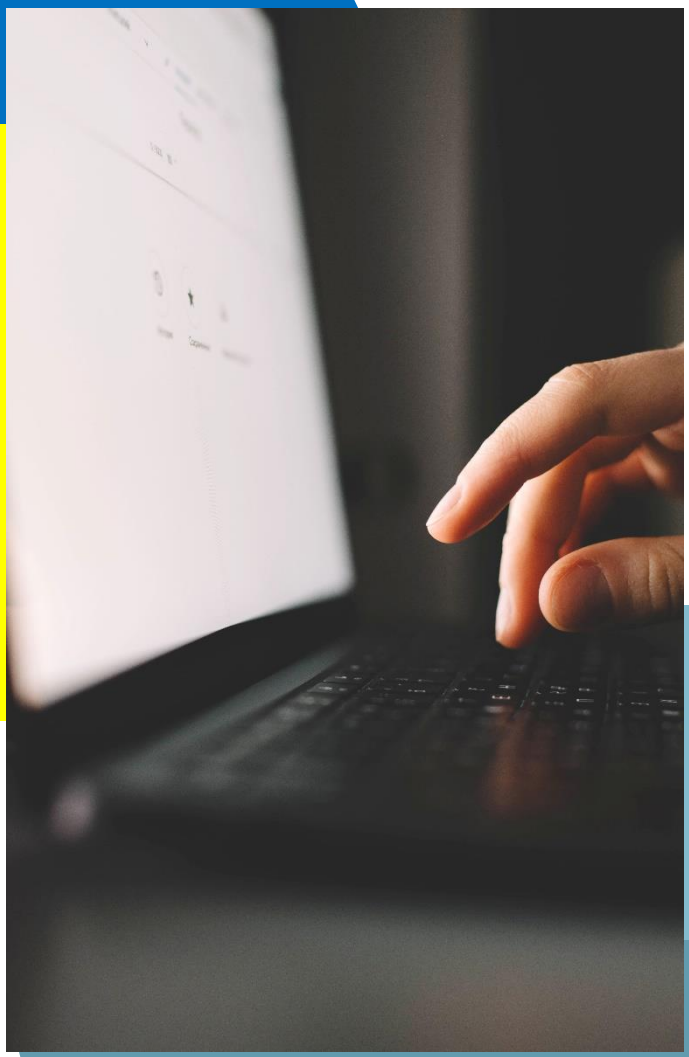
Руководство по анонимному общению.



Анонимность может иметь решающее значение.

Если ваш собственный мир перевернулся вверх дном, и вам приходится беспокоиться о том , что кто-то может читать ваши переписки, то из-за общения вы можете подвергнуть опасности других людей, друзей и семью.
Поэтому важно знать основы анонимного общения в зонах кризисов и военных действий.

Издано 2022

Анонимное общение означает безопасность



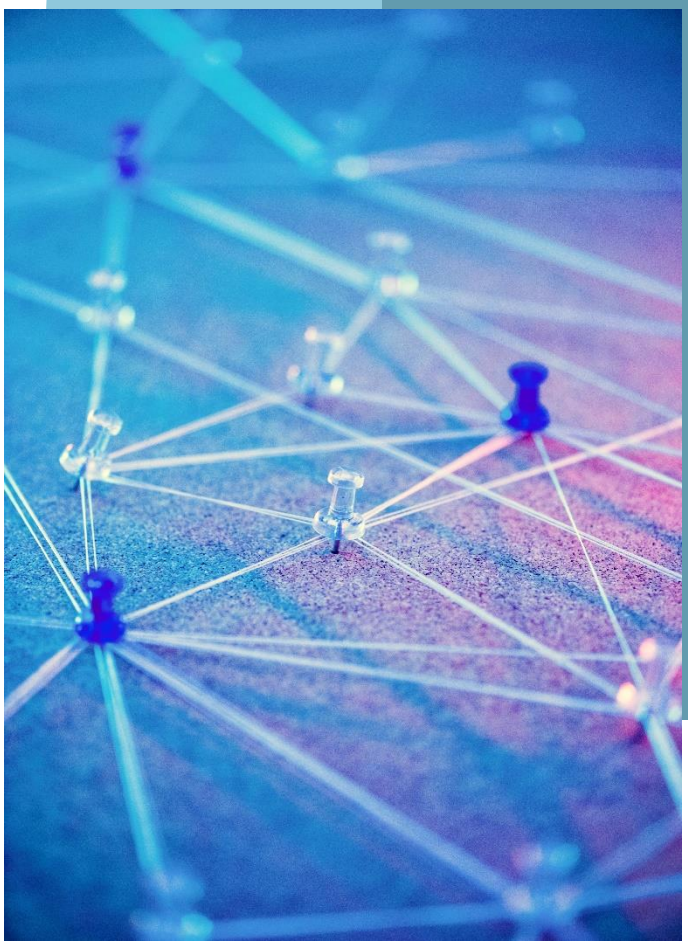
Nikolaus Stapels

С помощью этого руководства я хотел бы внести свой вклад в поддержку людей в кризисных и военных зонах. Во время кризиса мне удалось помочь многим наладить анонимное общение в зонах боевых действий

Программное обеспечение VPN под государственной цензурой

Некоторые страны ограничивают доступ к бесплатной информации в Интернете.

Программное обеспечение VPN — хороший первый шаг, потому что вы можете настроить зашифрованную линию с помощью программного обеспечения VPN , обойти так называемые блокировки DNS, и получить доступ к заблокированным веб-сайтам.



VPN-подключение также защищает вашу конфиденциальность в Интернете, изменяя ваш собственный IP-адрес, что затрудняет вашу идентификацию.

Кроме того, ваше общение невозможно или трудно поддается перехвату и, например, изменению.

Вы можете использовать обычные поисковые системы для смартфонов, планшетов или ноутбуков, чтобы быть еще безопаснее и анонимнее в Интернете

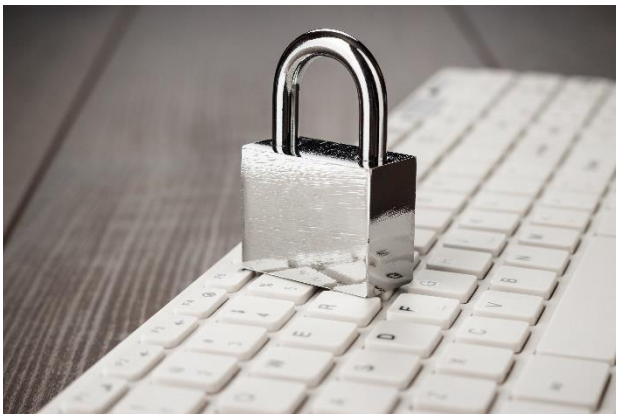
Сеть TOR

В мире, который оцифровывается все быстрее и быстрее, возможности мониторинга отдельных лиц ,групп людей или всего населения также быстро растут.

Это уже не только журналисты, проводящие взрывные исследования, и правозащитники, которые хотят оставаться анонимными при общении друг с другом.
«Обычным» пользователям также все чаще приходится принимать меры предосторожности, чтобы защитить себя и своих близких.
Хорошим и простым вариантом является использование сети TOR, поскольку пакеты данных не отправляются напрямую в веб-службу, а обходятся через различные серверы в сети

Сеть - TOR

С помощью браузера TOR, например, вы можете полностью автоматически установить анонимное подключение к сети и таким образом замести следы.
Этот метод анонимизации называется «луковой маршрутизацией»; веб-сайты маршрутизируются через так называемые «узлы».
Это соединение зашифровано, поэтому, защищает вашу личность.
Таким образом можно обойти интернет-блокировку определенных веб-сайтов в стране.



Защитите все свои коммуникации

Использование сети TOR; Давайте начнем...

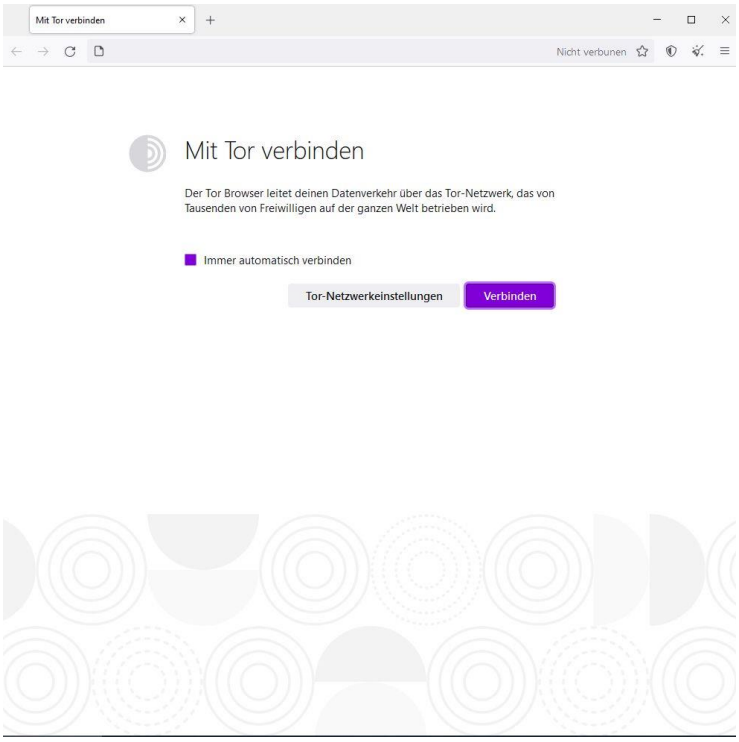
Когда в Интернете больше нет безопасных каналов, многие пользователи переключаются на сеть TOR. TOR хорошо известен благодаря широкому кругу пользователей, а программное обеспечение легко найти с помощью популярных поисковых систем.
При необходимости убедитесь, что вы загружаете программное обеспечение через общедоступную точку доступа, например загрузите в свой мобильный телефон, ноутбук или планшет, а затем раздайте через USB-накопитель, если это необходимо, чтобы никакие органы наблюдения не заметили, что вы напрямую загрузили браузер TOR.
Чем больше людей вокруг вас используют сеть TOR, тем безопаснее для всех

Начало

После того, как вы установили и запустили браузер, вы можете подключиться напрямую к сети TOR.
Заходить в настройки сети TOR (левая кнопка) нужно только в том случае, если браузер TOR заблокирован из-за ограничений в вашей стране.

В этом случае вы должны установить так называемые мосты;

Дополнительную информацию можно найти непосредственно по адресу: https://bridges.torproject.org/



Главный экран TOR Браузера

Важные замечания по использованию.

С технической точки зрения анонимность очень легко реализовать, поскольку большинство опций работает полностью автоматически.

Но есть одна большая опасность — некоторые ошибки, которые допускают многие пользователи в начале.
Поэтому обратите внимание на следующие моменты:

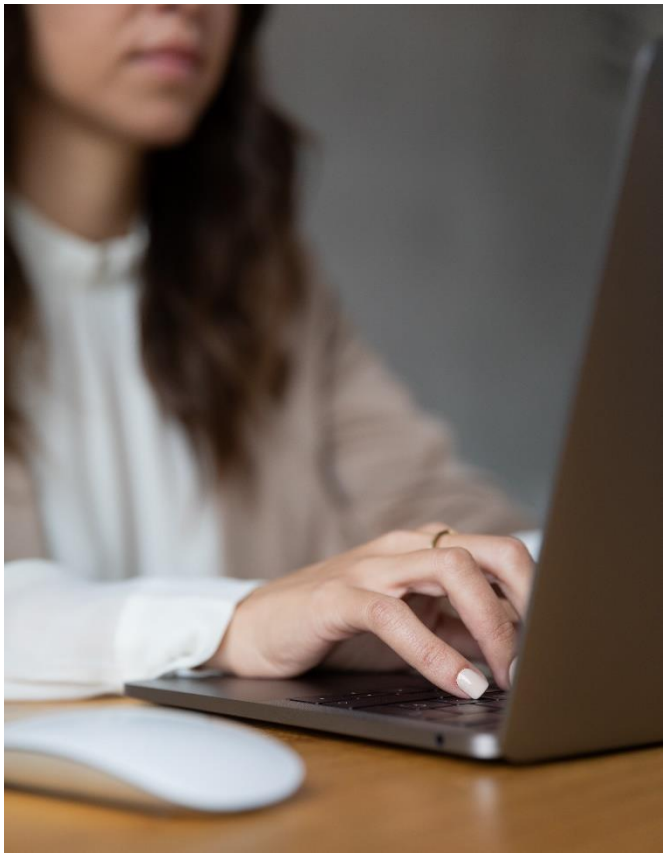
- Создавая (анонимные) учетные записи в социальных сетях, вас могут идентифицировать по старым.

- Не используйте настоящие имена или существующие псевдонимы (никнеймы) с других сайтов.

- Не вводите реальные адреса электронной почты.

- Не используйте куки при сёрфинге в сети TOR, вы можете отказаться от них прямо в браузере.

- Продолжайте защищать свои компьютеры с помощью антивирусного программного обеспечения и брандмауэров.



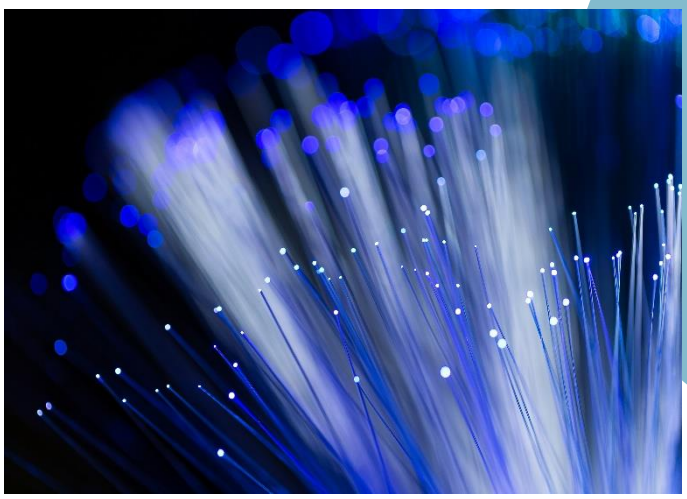
IT-Безопасность

Хотя вы можете просматривать страницы анонимно и свободно перемещаться по сети TOR, обратите внимание, что ваши данные по-прежнему хранятся в незашифрованном виде на вашем устройстве и поэтому могут быть прочитаны третьими лицами.

Навигация

Навигация в сети TOR не такая удобная, как в обычном Интернете.
Однако, с помощью браузера TOR вы также можете запрашивать обычные веб-сайты и поисковые системы и искать там определенные услуги.
В результате вы должны убедиться, что открываете веб-сайты с расширением .onion.
Так же как веб-сайты могут содержать расширения .de или .com, все веб-сайты в сети TOR имеют расширение .onion.
Затем вы можете получить доступ к этим страницам только с помощью браузера TOR и просматривать их анонимно.

Окончание .onion говорит о том, что веб-адрес находится в сети TOR.



Некоторые TOR-сайты

почта

ProtonMail

Пользователи могут отправлять и получать электронные письма анонимно через провайдера.
Также есть свободный доступ..

TOR Link

Поисковые - системы

DuckDuckGo

Это поисковая система, которая предлагает высокую степень конфиденциальности. Обратите внимание, что поиск в даркнете часто может не работать, потому что сайты отключены.

TOR Link

Социальные сети

Facebook

Многие пользователи зарегистрированы в социальных сетях, таких как Facebook. Вот почему Facebook также перенес свой сервис в сеть TOR. При необходимости поиск дополнительных услуг .

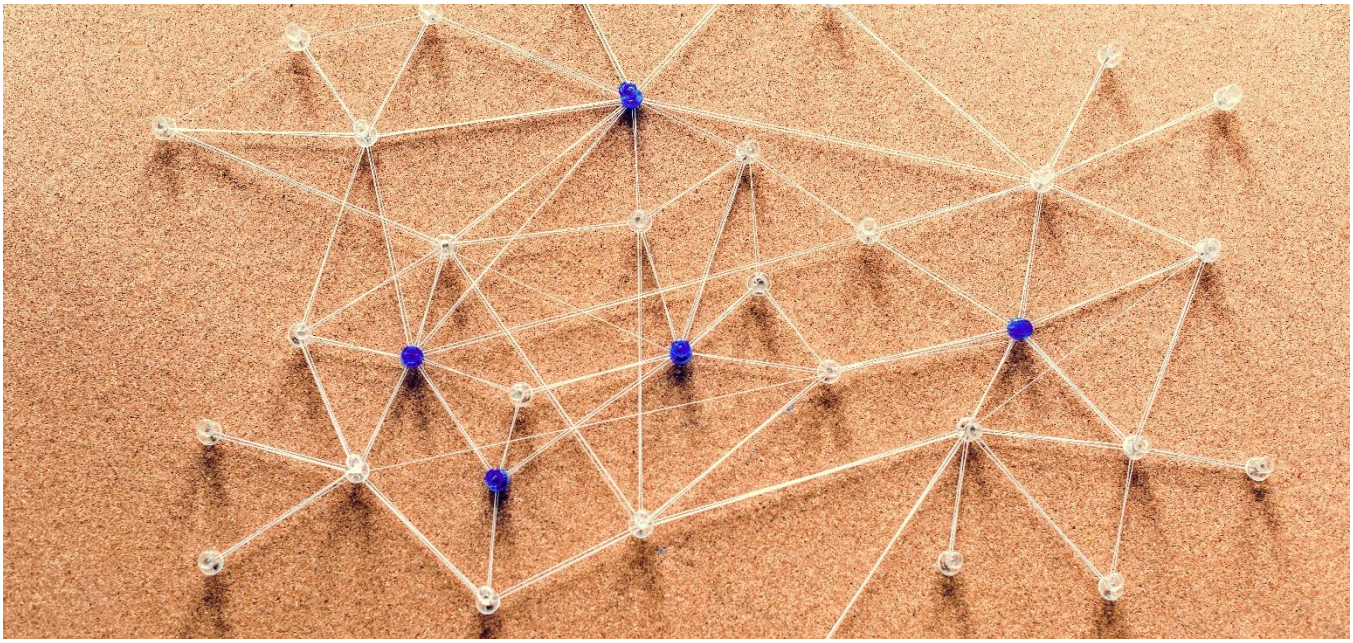
TOR Link

новости

SecureDrop

Документы и файлы могут быть переданы медиа-организациям по всему миру через SecureDrop.

TOR Link



Какие существуют «безопасные» мессенджеры?





По сути, вы всегда должны полагаться на безопасный мессенджер независимо от сообщений. Но в условиях кризиса или войны вам особенно следует уделять больше внимания данным, которые вы отправляете, и используемому программному обеспечению. Вот несколько мессенджеров в качестве примера:

Signal

Сам Эдвард Сноуден рекомендовал использовать Signal, так как этот мессенджер считается одним из самых безопасных в мире.
Шифрование было протестировано несколько раз и показало хорошие результаты.

Threema

Компания Threema родом из Швейцарии и именно там расположены серверы. Помимо прочего, провайдер обещает высокий уровень безопасности и защиты данных за счет расположения серверов.

Telegram

Этот мессенджер также использует сквозное шифрование (активируйте его), чтобы третьи лица не могли его прочитать. Тем не менее, проект не является полностью открытым исходным кодом (не может быть проверен на 100% третьими лицами).

У вас есть вопросы?



Мы рады поддержать вас
info@cyber-fuchs.de
Наша почта в распоряжении
для ваших запросов

Это руководство предназначено для того, чтобы сориентировать вас и помочь безопасно общаться.
Мы не углублялись в технические подробности чтобы дать вам понятный первоначальный обзор.