Безопасность в сети

January 26, 2023

Доброго времени суток, ценители анонимности и, как кажется на первый взгляд, лёгких денег. Сегодня мы расскажем вам о *базовых способах защиты персональных данных и уменьшения своего цифрового следа.*

Для начала, кратко пробежимся по темам, которые мы упомянули в нашем видео, а также заполним информацией все пробелы, успевшие возникнуть в ваших пытливых умах.

Google, Apple, Microsoft и другие вендоры представляют угрозу для вашей деятельности. Некоторые компании, ввиду отсутствия возможности разглашать информацию о получении запроса от властей, могут передавать скрытые послания своим юзерам через молчание, используя «свидетельство канарейки». Например, ***до 18 сентября 2014 года*** в отчётах ***Apple*** находилось уведомление о том, что компания ***никогда не получала ордер от силовых структур***. Однако, после наступления этой даты заголовок исчез. Это еще раз подтверждает наше утверждение о том, что подобные компании представляют угрозу.

> *Оптимальное решение в контексте операционной системы на рабочем пк - это Linux: Kali, Kodachi, Tails.*

> *Для смартфонов: Sailfish os, Linage os, Ubutu Touch.*

Все мы знаем, что такое фишинг, и многие сталкивались с проблемами, которые он создаёт для жертвы. Возможно, для многих станет открытием тот факт, что огромное количество ***onion*** браузеров для смартфонов занимается им в промышленных масштабах. Мы рекомендуем использовать только оригинальный ***Tor Browser*** для вашего смартфона, а также ***Orbot*** для режима *VPN*.

Используя маркетплейсы: первое, что стоит выучить наизусть - это использование ***PGP*** и ***Google authenticator***, если это предусмотрено

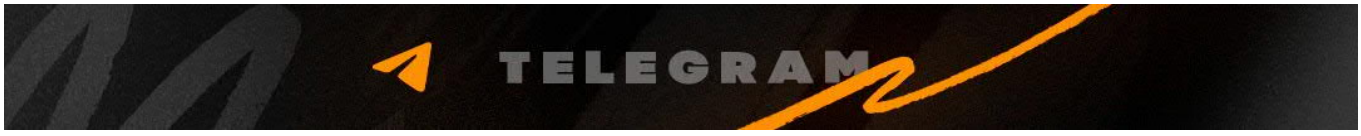
площадкой, на которой ведётся деятельность. Эти простые шаги помогут сберечь ваши нервы и деньги.

Мы уже рассказывали, что нужно внимательно подходить к выбору VPN, но что если вы не доверяете представленным на рынке решениям? Ответ прост: необходимо арендовать собственный сервер, подключение к которому будет только у вас, причём по зашифрованному каналу. В дополнение к этому мы настоятельно рекомендуем использовать функцию ***KillSwitch***, которая не пропустит ваш оригинальный ip, если оборвется подключение к *VPN*. Гайдов в интернете на эту тему предостаточно, мы рекомендуем ознакомиться с ними.

Но что если вам нужно подключение не только из определенной страны, но и из города? Для такой проблемы у нас тоже есть решение: использование прокси. ***Proxyfier*** в паре с браузером ***Chromium*** и расширением ***WebTRC***

> *(в настройках расширения нужно выбрать Use the default public interface and private interface)*

- неплохой вариант. Это менее защищенное решение, но вполне подходящее для определенных ситуаций.



Что если для вашего рода деятельности требуется использование Telegram?

Хоть мы и ***не рекомендуем им пользоваться***, ситуация временами того требует - не стоит пренебрегать теми же правилами безопасности. С помощью встроенного функционала трафик в нем можно направить через ***Tor***, а перед этим поставить *VPN*.

> *Для этого нужно перейти в: Данные и память > Прокси, в поле IP указать: 127.0.0.1, а порт: 9150. (рекомендуется делать это везде, где есть возможность, включая jabber).*

Таким образом, ***Telegram*** будет работать только при запущенном ***Tor*** *браузере*, а в списке ваших сессий не будет личного ip адреса. При этом важно не регистрировать ***Telegram*** на свою ***личную симкарту***, а прокси должен быть настроен до регистрации. Зарегистрировать аккаунт без использования телефона можно через ***Bluestacks*** и другие аналоги.

Бонусом к вашей легенде (зарубите себе на носу) **НИКОГДА не используйте никнеймы из личной жизни в работе**, даже если вам очень нравится никнейм из любимой игры. В разговорах с коллегами не рассказывайте о своих увлечениях, путешествиях или редких вещах, которые вы приобрели. Вам может показаться, что это простейшая вещь, но трудно даже вообразить, сколько людей пострадало от этого.

Если вам нужно обменяться каким-либо файлом с вашим коллегой - худшим решением будет отправить его в ***Telegram***. Для этого мы рекомендуем использование ***Onionshare*** или ***Qtox***.

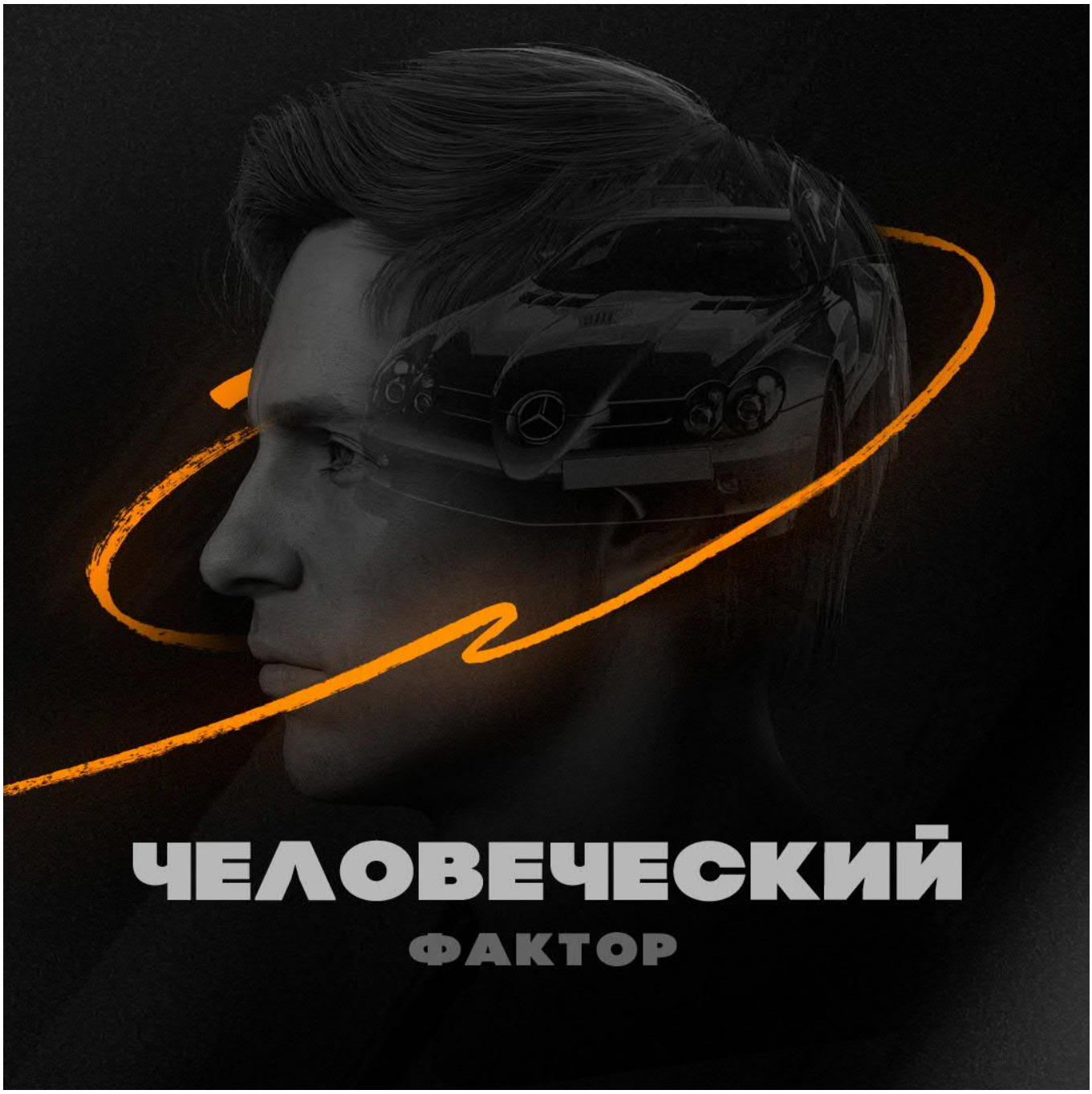
Еще одна важная тема - это очистка денег и их вывод.

Полученные средства всегда необходимо проводить через *миксеры* и *прачечные,* а также проверять их чистоту по ***AML***. Только после этого можно готовить их к выводу. Политика ***KYC*** присутствует практически во всех обменниках, и вам с радостью заблокируют грязные активы, запросив паспорт. Также необходимо учитывать, что со временем ***BTC*** могут *пачкаться*. Если вы очистили монеты и положили их на счет в качестве сбережений, периодически нужно проводить проверку повторно. Чистые средства никогда

не должны пересекаться с грязными, для этого необходимо делать новые кошельки для них (новые адреса не считаются новыми кошельками).

> *При отправке - округляйте значения (к примеру, 0.3BTC вместо 0.3219),*

так ваши транзакции сложнее отследить. Также в настройках кошелька ***Electrum*** (вкладка транзакции) нужно отключить адреса для сдачи. Так, шанс того, что средства запачкаются, будет меньше.



Следуя этим правилам в технической части, не стоит забывать о главной слабости человека - он сам.

Человеческий фактор - это то, что будет преследовать вас всегда. Детально проработанная легенда, а также отсутствие кича станут гарантами безопасности. ***Инстраграм*** не должен пестрить фотографиями красивой жизни, как бы ни хотелось похвастаться успехами. Ненадежные знакомые не должны знать того, что не входит в вашу легенду. Зависть - это двигатель ненависти.

Никогда не показывайте того, что создаст лишние вопросы. Например, *телефон с защищенной ОС* на людях заставит их задуматься, зачем она тебе?

В диалогах со знакомыми, друзьями, не стоит блистать знаниями в *темной сфере*.

Избегайте личного контакта с коллегами по работе, чаще всего это приводит к плачевным последствиям. Не доверяйте личную информацию, не совершайте необдуманные поступки и всегда будьте настороже.