REPORTER
OHNE GRENZEN

ЦИФРОВАЯ БЕЗОПАСНОСТЬ

Это Маша, российская журналистка. Из-за её открытой антивоенной позиции Маше стало опасно оставаться в России, и она переехала в Германию. Маша знает, что переезд не обеспечит ей и её близким полную безопасность, поэтому она решила сама защититься от внимания российских силовых структур. Маша разобралась со своей цифровой безопасностью, и теперь готова поделиться советами и ссылками на полезные материалы!

Шаг 1. Оцените свои риски

- Начните с оценки своих собственных рисков. Подробную инструкцию составляла Теплица Социальных Технологий.

Пример. Маша заботится о защите своих источников и не хочет, чтобы их имена и внутренняя коммуникация попали в руки российских органов. Маша ведёт Телеграм-канал с несколькими тысячами подписчиков, который ей бы хотелось защитить от взлома. Кроме того, у Маши в России остались родственни:цы, в том числе мама, работающая в бюджетной больнице и уязвимая для давления со стороны государства.

Статья об отравлении российских журналисток от The Insider
Заявление главного редактора «Медузы» об атаке на издание с помощью Pegasus

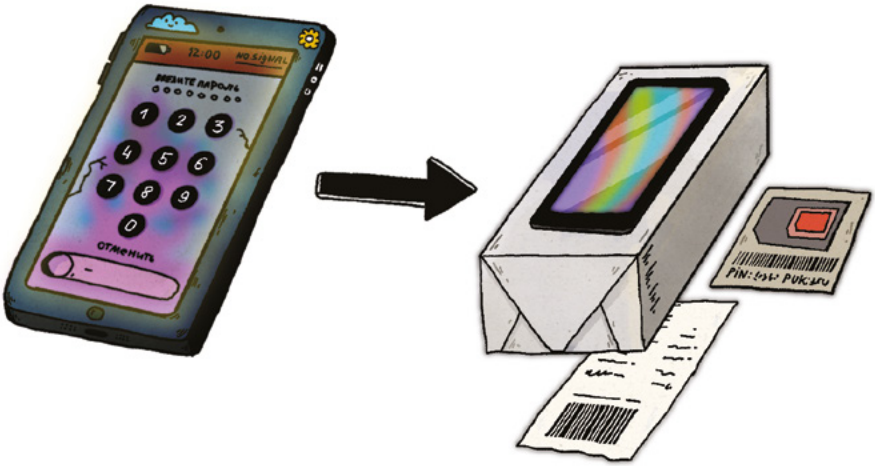
Шаг 2. Замените телефон и SIM-карту

- Сразу после переезда купите новую местную SIM-карту и новый мобильный телефон и начните использовать их как основные. Обратите внимание, что новый телефон нужно приобрести именно после переезда, а не в России: иначе Вы не сможете удалить с него предустановленные российские приложения, которые потенциально могут собирать о Вас данные.

  Почему? Мобильные операторы всегда знают, где находится телефон с Вашей SIM-картой. Российские операторы делятся всей доступной им информацией с органами. Кроме того, оператор уже знает всю информацию о Вашем старом телефоне, и по ней государство сможет идентифицировать Вас даже после смены SIM-карты, если Ваш телефон снова засветится в Сети.

- Не пользуйтесь встроенными в iOS/Android функциями переноса данных на новый телефон, вместо этого установите нужные приложения и скопируйте необходимые данные вручную. Не устанавливайте российские приложения, их можно использовать со своего старого устройства.

  Почему? Российские сервисы не имеют возможности не делиться с государством информацией о своих пользователь:ницах. При этом приложения могут собирать с телефона самые разные данные.



Примеры (это только краткая выжимка!) российских приложений:

- Яндекс (Почта, Браузер, Карты, Такси, YandexGo, Диск, Лавка, Музыка и т.д.)
- Госуслуги, Моя Москва
- ВКонтакте, Одноклассники
- Kaspersky Internet Security
- Авито
- Банковские приложения (Сбербанк, Альфа-Банк, Тинькофф и т.д.)
- Mail.ru (Почта, Новости)

- Оставьте старый российский телефон у себя и используйте со старой российской SIM-картой, но сначала сбросьте настройки телефона до заводских и не устанавливайте туда приложения, в которых работаете. Выключите на этом телефоне геолокацию, следите за разрешениями приложений и не позволяйте чувствительной информации попадать на этот телефон, в том числе в содержании переписок. Не берите с собой этот телефон, если не хотите, чтобы российские службы могли отследить Ваши перемещения по данным российского мобильного оператора.

  Почему? Старый телефон уже известен российским властям через мобильного оператора, можно продолжить использовать его для использования необходимых российских сервисов, например, Госуслуг или Яндекс.Почты. Однако информация с этого устройства потенциально может попасть в руки российских органов, поэтому вести через него важные разговоры и переписки потенциально опасно.

- Установите на все свои SIM-карты PIN-коды и настройте блокировки телефонов на случай их кражи или утери.

  Почему? Если на SIM-карте нет PIN-кода, при краже можно будет вставить её в новый телефон и воспользоваться ей для авторизации в сервисах, чтения новых сообщений и голосовой почты или (в случае обычной кражи ради денег) банально потратить все средства на счету.

> *Подробная инструкция об использовании смартфона за границей от Теплицы Социальных Технологий.*

Шаг 3. Смените электронную почту и телефонный номер в своих аккаунтах

- Если Вы используете российские сервисы электронной почты, например, Яндекс или Mail.ru, заведите новую электронную почту в не-российском сервисе. Старые почты можно проверять со старого телефона с российскими приложениями или настроить переадресацию.

  Почему? Российские силовые структуры могут получить доступ ко всем российским сервисам, в том числе к содержанию электронной почты.

  Пример. Маша выбрала для своей новой почты защищённый немецкий сервис Tutanota, поскольку у него есть русскоязычный интерфейс. Маша также рассматривала сервис ProtonMail. Для работы над общими документами в Google Drive Маша также завела отдельный анонимный аккаунт в Google, который не планирует светить публично.

- Проверьте настройки своих зарубежных аккаунтов – Google, Facebook, Telegram, Twitter и т.д., и замените в них свой старый российский номер на новый зарубежный, а старую почту – на новый адрес.

  Почему? SMS-сообщения не защищены шифрованием при пересылке, хранятся у оператора связи до трёх лет и будут предоставлены силовым структурам по требованию без Вашего ведома.

Шаг 4. Приведите в порядок свои пароли и настройки входа в аккаунты

- Выберите одну из специальных программ для хранения паролей – менеджер паролей, например, Bitwarden или 1Password. Научитесь им пользоваться и смените пароли всех своих аккаунтов на сгенерированные менеджером уникальные. Для важных аккаунтов: не используйте сохранение паролей, встроенное в браузеры, например, в Chrome.

  Почему? Пароли для аккаунтов должны быть разными, иначе утечка паролей в сервисе или взлом одного из аккаунтов поставит под удар все остальные Ваши аккаунты.

Почему не стоит доверять встроенным в браузер менеджерам паролей? Отвечает PCMag UK на английском языке
Инструкция по использованию менеджера паролей Bitwarden от Теплицы Социальных Технологий

- Несколько паролей Вам всё же понадобится запомнить – как минимум, пароль для входа в менеджер паролей. Можно придумать удобный для себя способ запоминать сложные для взлома пароли, взяв за основу, например, такой вариант от Lifehacker. Используйте цифры и специальные символы вперемешку, не только буквы.
- Установите на всех своих аккаунтах двухфакторную аутентификацию, отдавая предпочтение верификации через приложения, а не SMS.

  Почему? SMS-сообщения можно перехватить. Эта технология уязвима не только для российских SIM-карт. Простота перехвата в случае, когда известен номер телефона, описана в статье WIRED на английском языке.

Инструкция по двухфакторной аутентификации от Роскомсвободы

Шаг 5. Контролируйте публичную информацию о Вас

Журналист:ки – часто публичные лица, ведущие соцсети и открытую социальную жизнь, привыкшие к опасностям преследования властей и периодической травле. Однако собственные риски и риски для окружающих можно уменьшить, удалив некоторую информацию из публичного доступа.

Пример. Маша не хочет, чтобы тролли добрались до её младшей сестры-школьницы или напугали её дедушку, поэтому старается не делать публичной информацию о своей семье.

- Проверьте, какую информацию о Вас, Вашей семье и близких можно найти в Сети. Обратите особое внимание на публикации адресов и планов – проживания, места работы или учёбы, указания на места, где часто бываете. Проверьте также профили в соцсетях ближайших родственни:ц. По возможности удалите информацию, которую сочтёте лишней.

  Пример. Маша обнаружила, что по её странице на Facebook можно узнать, в каком отеле она остановится на следующей неделе в отпуске и в какую школу и какой класс ходит её младшая сестра.

  Почему? Чем проще узнать, где Вы бываете или будете в скором времени – тем проще организовать за Вами слежку. Информацию об уязвимых близких можно использовать для публичных призывов к их травле. К сожалению, оппозиционные журналист:ки за границей не избавлены от опасностей: у российских органов всё ещё достаточно возможностей не только внутри страны, а гражданские пропутинские активист:ки активны как онлайн, так и оффлайн в разных странах.

  Подробная инструкция о сборе онлайн досье на себя от Global Investigative Journalism Network (GIJN)

- Проверьте настройки приватности в соцсетях, например, в Facebook, а также в Telegram. Оставьте открытой минимум информации: нужен ли Ваш список друзей широкой публике? Полезен ли Ваш список групп всем Вашим контактам? Нужно ли знать номер Вашего телефона людям, видящим Ваш комментарий под постом в открытом канале Telegram? Учитывайте, что сторис в Telegram доступны любым людям, добавившим Вас в список контактов.

  Почему? Информация о номере телефона, привязанного к профилю, будет весомым подспорьем для взлома или Вашей деанонимизации. Открытый список контактов и групп упростит вычисление данных о Вас и Ваших близких, создание профилей-клонов и другие практики фишинга (получение конфиденциальных данных обманом).

  Инструкция «Роскомсвободы» о настройках безопасности Facebook
  Гайд на английском языке по настройкам приватности в Telegram от LifeHacker

Шаг 6. Выберите мессенджеры для конфиденциальной коммуникации

- Переведите дискуссии на чувствительные темы из российских сервисов, Facebook Messenger и Telegram в более безопасные мессенджеры. Если используете WhatsApp или iMessage, избегайте использования бэкапов через сервисы Apple или настройте Расширенную Защиту Данных (Advanced Data Protection, ADP) для iCloud. Для особо конфиденциальных переписок включите функцию автоудаления сообщений по таймеру.

Пример. Личные переписки с близкими Маша продолжает вести в Telegram. Основное общение по журналистской работе Маша теперь ведёт в Signal, а по некоторым активистским проектам – в Element. Для чувствительных, но срочных коммуникаций в Telegram, когда у собеседни:цы нет возможности поставить новый мессенджер, Маша стала просить собеседни:ц перейти для обсуждения в секретные чаты, которые она затем оперативно удаляет. Сообщения в конфиденциальных переписках Маши автоматически удаляются через 2 недели.

Почему? В Telegram и Facebook Messenger отсутствует сквозное (end-to-end) шифрование по умолчанию: эти сервисы хранят содержание сообщений из групповых и личных не-секретных чатов на своих серверах в доступном для прочтения виде. Это значит, что, во-первых, сотрудни:цы сервисов имеют к ним доступ и потенциально могут подчиниться

требованию спецслужб о передаче информации или слить её в частном порядке, во-вторых – данные переписок могут попасть не в те руки в случае успешной хакерской атаки на сервис.

Компания Apple также хранит ключи шифрования в своих бэкапах и передаёт доступные ей данные властям в ответ на запросы от правоохранительных органов некоторых стран. Это касается как собственного мессенджера, так и данных WhatsApp, если используется опция бэкапа через iCloud.

Анализ безопасности при использовании Telegram от The Insider
Статья об особенностях разных мессенджеров и настройках групповых чатов от Теплицы Социальных Технологий

- Расскажите заранее своим постоянным источникам о безопасных способах с Вами связаться и о базовых настройках безопасности – например, о том, как настроить автоудаление в мессенджерах.
- Обратите внимание, что при использовании электронной почты сообщения защищены настолько, насколько защищены почтовые сервисы всех участни:ц переписки!

Пример. Если Вы используете защищённый почтовый сервис ProtonMail и посылаете с него письмо на Яндекс.Почту, по умолчанию содержимое письма не будет защищено на серверах Яндекса и будет доступно силовым структурам. Для дополнительной защиты в таком случае потребуется включить шифрование (external encryption) в настройках письма и передать пароль собеседни:це через другое средство связи.

Шаг 7. Соблюдайте меры предосторожности при обмене файлами

- В общих документах Google Drive с чувствительной информацией настройте доступ к файлам по почтовому адресу вместо ссылки, и ограничьте другим людям возможность дальнейшей передачи прав (настройка скрыта за иконкой шестерёнки в параметрах общего доступа).

Почему? Распространение ссылки и личности пришедших по ней сложно проконтролировать.

- Удаляйте метаданные в файлах, которые храните и пересылаете.

  Почему? В метаданных может сохраняться, например, геолокация или имя пользователя, создавшего файл.

  Несколько способов удаления метаданных от SecurityLab

- Google Drive – привычный и удобный инструмент, но есть отдельные ситуации, в которых его использования лучше избегать. Ознакомьтесь с альтернативами заранее, чтобы информированно принимать решение в случае необходимости.

  Почему?

  - Google хранит ключи шифрования от Ваших файлов на своих серверах и сохраняет за собой право обращаться к их контенту. Потенциально компания может выдавать документы по запросам правительств некоторых стран, также данные могут пострадать из-за недобросовестности сотрудни:ц (подобное случалось в 2018 году, CNBC, на английском).
  - При открытии документа Google Drive видно всех пользователь:ниц, у которых этот документ также открыт. Если документ редактируется широким кругом людей и часть редакторо:к используют свои личные аккаунты или аккаунты с настоящими именами, информация об их участии может стать доступной органам.
  - Google Drive сохраняет историю просмотра файлов. Если Ваши коллеги работают из России и их устройства досмотрят, силовики, скорее всего, будут заинтересованы в получении доступа к их аккаунтам Google и анализе ранее открытых файлов.

  Пример. На одной из уличных антивоенных демонстраций в Германии Маша поделилась с публикой QR-кодом на документ Google с агитационным обращением. Это было не лучшей идеей: ссылку было легко получить кому угодно и увидеть список людей, у кого также открыт документ.

  Статья «Роскомсвободы» об альтернативном сетевом офисном пакете CryptPad
  Статья Теплицы Социальных Технологий об альтернативных облачных хранилищах

Шаг 8. Проверяйте, с кем общаетесь онлайн

- Способы войти в доверие к журналист:кам и активист:кам в Сети и выведать у них информацию или заразить их устройства постоянно развиваются. Такой вид обмана называется фишингом. Старайтесь подтверждать личности собеседни:ц, особенно, если используете новый канал связи. Например, просите своих коллег включать камеры в начале созвонов, чтобы проверить, с кем именно разговариваете.

Статья о защите от фишинга от Теплицы Социальных Технологий

- Будьте внимательны в групповых чатах, где Вы не знаете всех участни:ц. Не делитесь в них конфиденциальной информацией: к сожалению, иногда в протестные или оппозиционные чаты попадают сотрудни:цы силовых структур.

Пример. Маша состояла в чате активистской онлайн конференции на чуть более ста человек. В чате активно обсуждали способы выехать из России при официальном запрете на выезд. Маша не стала рассказывать известные ей малопопулярные лайфхаки. Как оказалось, не зря: через пару дней после начала конференции организатор:ки обнаружили, что один из участников чата подделал свои данные и на самом деле являлся сотрудником российских органов.

Шаг 9. Соблюдайте несколько простых правил при работе в общественных местах

- Держите в поле зрения свои устройства, не оставляя их разблокированными. Включите требование заново ввести пароль при закрытии крышки ноутбука.

  Почему? Устройства могут быть украдены или, если они разблокированы, заражены вредоносными программами.

- Старайтесь избегать публичных сетей Wi-Fi. Если подключиться всё же необходимо: обращайтесь только к страницам сайтов, адрес которых начинается с «//https:» и не пренебрегайте предупреждениями браузера о недобросовестности сайта (например, не игнорируйте перечёркнутую иконку замка в адресной строке или предупреждения об опасности введения пароля), либо держите включённым VPN на протяжении всего подключения.

  Почему? Подавляющее большинство публичных сетей (включая запароленные гостиничные) не защищены от хакерских атак. Злоумышленни:ца может подключиться к сети и получить информацию со всех подключённых к ней устройств, включая сохранённые логины и пароли, подключиться к Вашим сеансам связи с незащищёнными сайтами, подменить содержимое запрашиваемых сайтов или заразить Ваши устройства вредоносными программами.

- Будьте аккуратны в рабочем или активистском общении вслух в публичных местах. Обращайте внимание на посторонних людей, прислушивающихся к Вашему общению.

  Пример. Не обсуждайте конфиденциальные темы по телефону в общественном транспорте так, чтобы их слышали другие пассажир:ки.

  Почему? Вне России достаточно много русскоязычных людей и далеко не все они придерживаются критических по отношению к российскому режиму взглядов. Есть опасность нарваться на агрессивных пропутинских активисто:к или упростить слежку за Вами или за кем-то, с кем Вы общаетесь.

Шаг 10. Заведите несколько регулярных привычек

- Соглашайтесь на предлагаемые обновления своих устройств и приложений. Периодически проверяйте обновления вручную для тех программ, у которых не стоит настройка автообновления.

  Почему? Это снизит риск подхватить вирусы и шпионские программы, использующие известные уязвимости операционных систем и программ.

- Периодически проверяйте, кто имеет совместный доступ к Вашим файлам – если человек с Вами уже не работает, отключите ему доступ.

  Почему? Аккаунты могут взламывать, люди сами могут давать к ним доступ силовикам под давлением разного толка. Если доступ к данным больше не нужен для работы – нет смысла оставлять его, это лишняя точка уязвимости.

- Меняйте пароли минимум раз в год, хотя бы от самых важных аккаунтов. Рассмотрите более частую смену для рабочих аккаунтов, если работаете с конфиденциальными

данными. Используйте менеджер паролей для генерации новых паролей. Проверить, участвовали ли конкретные Ваши аккаунты и пароли в известных утечках данных, можно здесь или с помощью встроенных в Ваш менеджер паролей инструментов.

Почему? Смена пароля не столь сложна при использовании менеджера паролей, но может значительно снизить урон от незамеченного взлома. Если кто-то смог узнать пароль (с помощью фишинга, кражи устройств, шпионских программ и т.д.) и получить доступ к Вашему аккаунту, смена пароля этот доступ отзовёт.

Поездки в Россию (или другие страны с авторитарными / тоталитарными режимами)

На границе и внутри России есть опасность столкнуться с задержанием и обыском имущества. Даже если Вы не планируете поездок в ближайшее время, подумайте заранее о том, что может потребоваться для этого в будущем: например, Маше пришлось поехать домой в срочном порядке, чтобы уладить домашние дела.

Инструкция о подготовке к пересечению границы от Теплицы Социальных Технологий

- Удалите с устройств компрометирующие данные и очистите чувствительные переписки в мессенджерах. Вы можете предварительно сохранить нужные переписки на устройствах, которые не возьмёте с собой в Россию. Не забудьте синхронизировать аккаунты на разных устройствах, чтобы убедиться, что данные удалены и на телефонах, и на планшете, и на ноутбуке.
- Перепроверьте, какие документы можно открыть из Ваших облачных аккаунтов (например, Google) и временно ограничьте свой доступ к отдельным файлам или удалите с устройств рабочие аккаунты.
- Обратите внимание на свою историю в браузерах, картах, магазинах приложений, Google Drive и на список сохранённых Wi-Fi сетей. Удалите то, что не хотите раскрывать силовым структурам.

Пример. Маша в Берлине посещает Reforum Space, но не хочет светить такие явные связи с российскими диссидентами, поэтому удалила историю поиска и перемещений из Google

Maps и сохранённую Wi-Fi сеть Reforum Guest. Маша использует приложение Meduza и удалила его с телефона, а также на всякий случай из списка приложений в Google Play.

- Поставьте на мессенджеры и другие приложения отдельные PIN-коды, если не хотите, чтобы они стали доступны силовым органам при разблокировке телефона по их просьбе, например, на границе.
- Отключите биометрическую разблокировку устройств с помощью Face ID или отпечатка пальца, если подозреваете, что Вас могут попытаться заставить разблокировать устройство силовыми методами.
- Если в течение поездки требуется доступ к конфиденциальным данным или данные нужно провезти через границу, позаботьтесь об обеспечении их безопасности. Файлы можно зашифровать и запаролить на своём устройстве, либо работать с ними из облачного хранилища через VPN, а по окончанию работы закрывать к нему доступ и удалять временные локальные копии.

  Пример. Маше требовалось работать с файлами на компьютере во время поездки и она зашифровала их с помощью программы VeraCrypt. Особо конфиденциальные данные, к которым силовые структуры не должны получить доступ ни при каких условиях, Маша спрятала в «скрытые» контейнеры VeraCrypt.

  Инструкция по использованию шифровальной программы VeraCrypt от Роскомсвободы
  Инструкция по использованию простой шифровальной программы Picocrypt от Теплицы Социальных Технологий

- Если в поездке Вам потребуется работать с чужих компьютеров, рассмотрите вариант использования операционной системы Tails. Tails устанавливается на флешку, шифрует сохраняемые данные и не оставляет следов использования на устройстве, в которое вы вставляете флешку.

  Инструкция по использованию Tails от Теплицы Социальных Технологий

- Некоторые модели телефонов Android позволяют настроить зашифрованное и запароленное второе пространство. Им можно пользоваться как вторым, скрытым телефоном со своими приложениями, аккаунтами и данными. **Полностью скрыть присутствие второго пространства в телефоне невозможно**, рассчитывать можно лишь на то, что его наличие не заметят при поверхностной, случайной проверке Вашего телефона.

  Пример. У Маши телефон Samsung. Она настроила на нём зашифрованное второе пространство с помощью встроенного приложения Secure Folder, в котором стала временно сохранять сделанные на телефон фотографии, которые хотела бы скрыть от случайного досмотра.

Инструкция по использованию второго пространства от Android Insider

Куда и когда обращаться

Если у Вас появляются вопросы о своей цифровой безопасности, Вам есть, с кем проконсультироваться! Например, если Вас взломали или о Вас собирают информацию через Ваших знакомых, или Ваши данные утекли в Сеть и Вы не знаете, как это произошло и что делать или не знаете, как обеспечить безопасность конфиденциальных данных в конкретной ситуации – не стесняйтесь задавать вопросы.

- Репортёры без Границ
- Роскомсвобода
- Теплица социальных технологий
- Access Now
- The Committee to Protect Journalists

Обращайте внимание на работу своих телефонов. Скорее всего, Вы не сможете самостоятельно определить, что Ваше устройство заражено шпионской программой уровня Pegasus, однако существуют и более распространённые вирусы, присутствие которых проще заметить. Если возникли подозрения, что телефон может быть заражён шпионской программой, мы настоятельно рекомендуем обратится в Лабораторию цифровой безопасности организации «Репортеры без границ», чтобы проверить свое устройство (mail@lab.rsf.org).

Поводы насторожиться

- Телефон внезапно выключается или перезагружается, либо подолгу не реагирует на попытки его выключить или перезагрузить, либо перезагружается необычно долго
- Телефон начал использовать необычно много Интернет-трафика или данные на телефоне начали занимать необычно много места и Вы не можете определить, с чем связаны изменения
- Настройки телефона изменились, но Вы уверены, что не вносили эти изменения сами (например, включились GPS или разрешение установки приложений не из стандартного магазина приложений)
- На телефон приходят необычные уведомления или SMS-сообщения с непонятным содержанием
- В списке вызовов есть звонки, которые Вы не совершали, или Вы обнаруживаете незнакомые SMS в отправленных сообщениях
- Экран телефона мигает или телефон издаёт звуки уведомлений, находясь в спящем режиме, однако новых вызовов и уведомлений не обнаруживается
- Вы заметили приложение, которое не устанавливали, и не находите о нём информацию в магазине приложений и Интернете

Помните: цифровая безопасность – только один из важных аспектов в Вашей работе! Не забывайте также про свою физическую и психологическую безопасность.

Советы по цифровой безопасности тем, кто переехал, от Теплицы Социальных Технологий
Серия статей о безопасности журналисто:к от Global Investigative Journalism Network (GIJN)
Статья о психологической безопасности журналисто:к от Committee to Protect Journalists

REPORTER
OHNE GRENZEN

Reporter ohne Grenzen e. V., Postfach 304108, 10756 Berlin

Telefon +49 30 60989533-0
kontakt@reporter-ohne-grenzen.de
www.reporter-ohne-grenzen.de/spenden