Настройка телефона для Документирования офлайн

Этот раздел является частью курса, посвященного Документированию при отключении интернета.

Последний пересмотр: 31 января 2020 г.

Несмотря на отключение интернета, документалисты по-прежнему могут записывать важные видеодоказательства, которыми можно делиться в автономном режиме или сразу после подключения к сети.

Вот несколько советов от активистов и других деятелей о том, как настроить телефон для автономной документации. Обратите внимание, что для некоторых шагов **требуется доступ в интернет**, поэтому их необходимо выполнить заранее, до наступления блокировки, или после возобновления работы интернета. Кроме того, не ждите наступления стрессовой ситуации, чтобы выполнить эти шаги; сделайте это сейчас и потратьте время на то, чтобы **попрактиковаться в использовании телефона,** прежде чем вам придется использовать его в кризисной ситуации.

Блокировки интернета часто сопровождаются усилением контроля над информацией и ограничениями свободы слова и собраний. Если вы документатор, примите дополнительные меры предосторожности для защиты себя и своей информации в эти периоды. Если есть риск, что власти конфискуют ваш телефон или заставят вас разблокировать его и раскрыть содержимое (в период блокировки или в иных условиях), подумайте о возможности использования отдельного телефона для документирования, вместо вашего основного личного устройства. Это может помочь минимизировать объем информации, которая может быть скомпрометирована (например, ваши контакты, аккаунты, сообщения и т.д.). Если вы не можете использовать другое устройство, все равно следуйте этому руководству, чтобы уменьшить объем конфиденциальных данных и повысить безопасность своего основного телефона.

Если используете старый телефон, сначала "почистите" его

Чтобы стереть все данные с телефона, вернитесь к заводским настройкам.

Примечание: Исследования показали, что восстановление на телефоне заводских настроек не обязательно приводит к стиранию всех данных. Фактически, единственный 100% безопасный способ стереть данные - это уничтожить сам телефон, но такой метод не подходит тем, кто хочет повторно использовать имеющееся устройство! В этой статье инженер-разработчик Android предлагает перед возвратом к заводским настройкам убедиться, что содержимое вашего устройства зашифровано. Так или иначе, шифрование

используется по умолчанию на большинстве современных телефонов; в противном случае перед сбросом настроек перейдите в «Настройки»> «Безопасность»> «Зашифровать телефон». Таким образом, при возврате телефона к заводским настройкам ключ шифрования будет утерян, и все неудаленные данные станут недоступными.

Практикуйте базовую защиту телефона

Существуют общие практики защиты телефона, которые актуальны в любой ситуации, независимо от того, занимаетесь вы документированием при отключении интернета или нет. Вот некоторые полезные ресурсы от ряда других организаций. Хотя никакие методы не дают 100% гарантию безопасности, некоторые ключевые советы подразумевают следующее:

- Убедитесь, что ваш телефон зашифрован. В новых телефонах шифрование включено по умолчанию. Если вы не уверены насчет своего телефона, проверьте его настройки безопасности.
- Регулярно запускайте обновления операционной системы (ОС), так как они часто устраняют уязвимости системы безопасности.
- Регулярно обновляйте важные приложения (например, мессенджеры).
- Установите на телефоне надежный код доступа, состоящий как минимум из 6 цифр и не использующий отпечатки пальцев (touch ID) или идентификацию лица (face ID).
- Установите блокировку экрана и таймер блокировки.
- Отключите службы геолокации, если они вам не нужны (включая службу экстренного определения местоположения, точность определения местоположения, историю локаций и функции "поделиться местоположением", а также опции сканирования Wi-Fi и Bluetooth). Также проверьте разрешения на доступ к местоположению для отдельных приложений.
- Чтобы избежать отслеживания устройств, выключайте Bluetooth и Wi-Fi, когда они вам не нужны.
- Выключайте телефон, когда вы им не пользуетесь.

Установите полезные приложения для документирования

Для фото- или видеодокументации вы можете использовать встроенную камеру на своем телефоне или специализированное приложение для документирования, например ProofMode или его аналоги, которые обеспечивают более надежные запись и экспорт метаданных, идентификацию и аутентификацию, шифрование, безопасные галереи или другие функции.

Полезным приложением для документирования *самой* блокировки является OONI Probe, приложение с открытым исходным кодом, которое запускает тесты с вашего телефона, чтобы определить, блокируются ли сайты или платформы. Оно может показать вам, как,

когда, где и кем блокируются сайты. Перед использованием этого приложения обязательно осознайте потенциальные риски.

Не уверены, какое приложение использовать для документирования? Мы освещаем некоторые наводящие вопросы в нашем руководстве «Стоит ли использовать это приложение для документирования?».

Установите несколько обычных приложений

Наличие на телефоне минимального объема данных и нескольких специализированных приложений может вызвать подозрение. Чтобы устройство выглядело, как обычный телефон, установите несколько повседневных приложений, которые популярны в регионе, где вы документируете (но которые загружаются из авторитетных источников), и сделайте несколько безобидных фотографий для своей галереи.

Для приложений социальных сетей вы можете создать альтернативные аккаунты и войти в них, однако имейте в виду, что фальшивые аккаунты нарушают Условия Обслуживания большинства платформ, а требования проверки личности на ряде платформ могут усложнить создание поддельных аккаунтов. Кроме того, вам нужно будет потратить некоторое время на наполнение аккаунта контентом и добавление друзей, что может быть довольно трудоемко.

Установка приложений при отсутствии интернета

Очевидно, что скачивание и установка приложений без доступа к интернету является проблемой. Если вы допускаете возможность отключения интернета, вам необходимо заранее скачать приложения.

Одна из стратегий, которая может помочь вам и другим в дальнейшем, - это скачать и сохранить установочный файл приложения формата Android Package (.apk) (**скачивается из надежного источника**, например, непосредственно у разработчика) в памяти вашего телефона или на диске. Наличие этих APK-файлов офлайн позволит вам или другим пользователям делиться приложениями в условиях отсутствия интернета.

Хотя у нас не было возможности попробовать этот сервис, приложение F-Droid предоставляет интерфейс для обмена APK-файлами офлайн. Вот их руководство.

Храните реальную личную или частную / конфиденциальную информацию вне устройства

Постарайтесь использовать устройство только для документирования. Не используйте его для электронной почты, телефонных звонков или обмена сообщениями с личными контактами или активистами, которые могут быть подвергнуты риску, и не подключайте это устройство к вашим реальным, основным аккаунтам.

Используйте функции сокрытия контента

В случае, если ваш телефон досматривается, будет полезно сделать ваши намерения менее очевидными, а контент - менее обнаруживаемым. Если ожидается, что ваш телефон будет *досмотрен бегло и поверхностно*, вы можете использовать такие простые приемы, как:

- Изменить названия и иконки ваших приложений с помощью лаунчер приложений (например, Nova Launcher, но их много), чтобы было не так очевидно, что представляют собой определенные приложения.
- Использовать встроенную функцию конфиденциальности, если она поддерживается на вашем телефоне, например "Режим конфиденциальности" (Private Mode) (для Samsung) или "Блокировка контента" (на LG).
- Поместить пустой файл с именем «.nomedia» в любую папку, чтобы медиафайлы из папки не показывались в вашей галерее. Примечание: Если медиа все еще отображаются, возможно, вам нужно почистить кэш галереи. Это может сработать не на всех устройствах.
- Создавайте скрытые папки (папки, название которых начинается с «.») с помощью приложения для управления файлами. Вы можете переместить файлы в скрытую папку вручную, либо, если пользуетесь приложением для камеры типа Open Camera, можете указать, где сохранять записанные вами медиафайлы. Обязательно отключите в настройках параметр «Показывать скрытые файлы», чтобы скрытые файлы не отображались.
- Некоторые специализированные приложения для документирования, такие как Tella или Eyewitness to Atrocities, хранят материалы в отдельных зашифрованных галереях, содержимое которых доступно только через приложение, так что при досмотре вашего телефона наличие подобных файлов будет не так очевидно. Для документации в этих защищенных галереях устанавливается отдельный код доступа в приложении, поэтому контент остается зашифрованным, даже когда ваш телефон разблокирован.

Важное примечание о сокрытии контента

Важно отметить: описанных выше техник может быть достаточно, чтобы сбить с толку того, кто бегло просматривает ваш телефон, но **они не смогут эффективно скрыть ваш контент от тех, кто действительно ищет.**

Также имейте в виду, что в некоторых странах могут действовать законы, которые ограничивают или криминализируют использование приложений для безопасности, которые шифруют или стирают ваши данные. Их использование для предотвращения доступа властей к вашим данным может рассматриваться как уничтожение улик или препятствование расследованию и может наказываться как преступление. Эта карта (всеобъемлющая, но 2017 года) служит хорошей отправной точкой, если у вас есть вопросы о действующих в вашей стране законах.

Настройте офлайн-доступ

В ситуации, когда вы записали контент, но у вас нет интернета, вы все равно можете перекинуть материал со своего телефона чтобы освободить место, поделиться им с другими или из соображений безопасности. Регулярная выгрузка материалов с вашего телефона также поможет свести к минимуму объем информации, которая может быть скомпрометирована, если ваш телефон будет конфискован и разблокирован.

Даже если вы не можете подключиться к интернету, вы все равно можете подключиться к локальным устройствам с Wi-Fi или Bluetooth, например к другому телефону или USB-накопителю с Wi-Fi. Ваши телефоны обычно снабжены приложением / интерфейсом для подключения и передачи файлов. Если ваш телефон поддерживает эту функцию, вы также можете подключить USB-флешку или переходник, чтобы выгрузить материалы на флешку или другое устройство.

Эти методы более подробно обсуждаются в нашем Руководстве по обмену файлами и коммуникации при блокировке интернета и в нашем пособии «Видео в качестве доказательства: Технические инструменты - Передача файлов».

Практикуйтесь до того, как окажетесь в кризисной ситуации

Настройте телефон сейчас, если и пока у вас есть доступ в интернет. Начните практиковать использование приложений в повседневных ситуациях (когда нет проблем с безопасностью), чтобы привыкнуть к работе с ними. Сделайте хорошую базовую защиту телефона своей стандартной практикой. Тогда, если вы окажетесь в кризисной ситуации, эти методы вспомнятся по привычке, и вы сможете сфокусироваться на других не менее важных вещах.

Прочтите следующую статью этого курса: «Стоит ли использовать это приложение для документирования?»