Резервное копирование с телефонных носителей без интернета или компьютера

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

Последний пересмотр: 31 января 2020 г.

Резервное копирование - ключ к тому, чтобы ваши данные и материалы не были случайно удалены, повреждены или утеряны, если ваше устройство будет конфисковано. Во время отключения или замедления интернета вы не сможете запустить обычное резервное копирование в облако или отправить свои материалы в безопасное удаленное хранилище. Выгрузка на настольный компьютер или ноутбук - это один из способов резервного копирования, но поскольку у людей часто нет доступа к компьютеру, существует несколько вариантов и советов по резервному копированию мультимедиа с телефона без компьютера в период блокировки интернета.

Используйте флешку или беспроводной диск

Флэш-накопитель для смартфона (или OTG) - это тип USB-накопителя, совместимый со многими (но не всеми) Android-устройствами. Вы можете подключить флэшку для смартфона непосредственно к своему телефону или использовать соответствующий адаптер для подключения телефона к обычному жесткому диску USB. В случае флэшки для смартфона (OTG) диск питается от вашего телефона.

К популярным брендам флэш-накопителей для смартфонов (или OTG) относятся SanDisk, Kingston, Samsung и множество других. Обычно они стоят в диапазоне от 8 до 25 долларов США в зависимости от емкости.
Беспроводные флэш-накопители / жесткие диски похожи на обычные жесткие диски, но не используют кабели. Это позволяет подключать устройства, которые обычно не подключаются к жестким дискам, такие как, например, ваш телефон. Преимущество беспроводного накопителя перед флэш-накопителем для смартфона заключается в том, что вы сможете подключить к одному беспроводному диску одновременно несколько пользователей. Это может быть полезно, например, в ситуации протеста, когда вы снимаете материал командой - отснятые видео каждого участника можно скопировать на жесткий диск, который находится у одного из членов команды. Обратите внимание: беспроводные накопители не потребляют энергию от подключаемого к нему устройства; их питание обеспечивается собственным аккумулятором, который нужно заряжать.

SanDisk, пожалуй, самый популярный бренд беспроводных флэш-накопителей, хотя есть и другие. Беспроводные флэш-накопители обычно дороже, чем флэшки для смартфона; цены на них варьируются в диапазоне от 25 до 100 долларов США в зависимости от емкости. Цены на более крупные беспроводные внешние жесткие диски начинаются от 150 долларов США в зависимости от емкости.

Альтернатива: старый неиспользуемый телефон

Если у вас нет флэшки для смартфона или беспроводного накопителя, но есть старый неиспользуемый телефон в рабочем состоянии, его тоже можно задействовать для резервного копирования. Пока оба телефона находятся в физической близости, вы можете подключить устройства и копировать мультимедиа с одного на другое через Bluetooth, WiFi Direct или Near Field Communication (NFC) / Android Beam. Bluetooth и Wifi Direct - это беспроводные технологии, которые могут «связать» два устройства без участия роутера или точки доступа. WiFi Direct обеспечивает более широкий диапазон и более быструю передачу данных, чем Bluetooth, но потребляет гораздо больше энергии. Между тем, NFC имеет гораздо более короткий радиус (~ 4 см) и значительно более медленную скорость передачи, чем Bluetooth или WiFi Direct, но подключается быстрее и потребляет меньше энергии, поэтому может быть полезен для быстрой передачи небольших объемов данных, когда оба устройства находятся у вас в руках.

Ваш телефон, вероятно, имеет встроенные приложения / функции Bluetooth, WiFi Direct или NFC, позволяющие выбрать ближайшие устройства для обмена данными. Если на обоих телефонах установлена программа Files By Google, вы также сможете обмениваться файлами в автономном режиме, используя эти технологии в приложении.

Важно: помимо преимущества в виде простоты подключения, эти сервисы имеют и недостаток они небезопасны. Маяки / сканеры Bluetooth и Wi-Fi могут использоваться для отслеживания вашего местоположения или "прощупывания" вашего устройства на предмет информации. Злоумышленники могут попытаться подключиться к вашему устройству, отправить вам нежелательные файлы или даже получить контроль над вашим устройством, если оно уязвимо. **Для большей безопасности отключайте эти сервисы, когда не пользуетесь ими, и включайте только находясь в безопасных местах; ограничьте разрешения приложений только тем, что вам действительно нужно, и применяйте стандартные практики безопасности телефона, такие как установка обновлений и использование надежных паролей.**

Добавляйте любые отдельные описания / метаданные

При копировании медиаданных на флешку, беспроводной накопитель или старый телефон полезно добавлять любую описательную информацию или метаданные, которые могут существовать отделено от носителя. Например, многие приложения для

документирования создают текстовые документы CSV или JSON, которые включают извлеченные с устройства метаданные (такие как геолокация, время, дата) и любое другое описание, введенное пользователем вручную. Обязательно экспортируйте и добавляйте эти документы с метаданными в свои резервные копии.

Защищайте жесткие диски паролями

Многие беспроводные накопители можно защитить паролем с помощью мобильного приложения, которое поставляется вместе с накопителем. Обратите внимание, что защита паролем - это не то же самое, что шифрование (см. ниже). Большинство беспроводных накопителей или флешек не позволяют полное шифрование диска с использованием только мобильного телефона, хотя поддерживают полное шифрование с компьютера.

Подумайте о возможности шифрования файлов

Если для хранения файлов вам нужна большая безопасность, вы можете рассмотреть возможность шифрования резервных копий. Хотя вы, вероятно, не сможете зашифровать большинство беспроводных накопителей или флешек с мобильного телефона, вы можете зашифровать сами файлы перед выгрузкой их на накопитель. Среди приложений, которые шифруют файлы на Android, ZArchiver и RAR. Имейте в виду, что вам нужно помнить свои пароли шифрования. В случае потери пароля восстановить зашифрованные файлы будет невозможно.

Имейте в виду, что в некоторых странах могут действовать законы, ограничивающие или криминализирующие использование шифрования. Их использование для предотвращения доступа властей к вашим данным может рассматриваться как уничтожение улик или препятствование расследованию и может наказываться как преступление. Эта карта 2017 года, возможно, немного устарела, но она служит хорошей отправной точкой, если у вас есть вопросы о действующих в вашей стране законах.

Держите 2 резервные копии в разных местах

Одна резервная копия не всегда надежна. Например, вы можете потерять устройство резервного копирования, повредить его, или оно может просто вдруг выйти из строя. IT-специалисты обычно советуют иметь 2 резервные копии (т.е. всего 3 копии) на отдельных устройствах, хранящихся в разных местах. Это помогает снизить различные риски для каждой копии.

Прочтите последнюю статью этой серии «Обмен файлами и коммуникация при отключении интернета».