Практическое руководство по защите данных, сетевой и мобильной безопасности для граждан

на Ближнем Востоке, в Северной Африке и других регионах

Это пособие создано для тех граждан Ближнего Востока и Северной Африки, которые хотят безопасно использовать современные коммуникационные технологии для общения, а также организации и передачи данных (новости, медиа-файлы и прочее). Настоящее пособие также может быть использовано пользователями сети Интернет, которые хотят защитить свои персональные данные и повысить уровень собственной цифровой безопасности. Руководство написано для широкой аудитории со средним уровнем компьютерной грамотности, для тех, кто хочет знать, какие шаги следует предпринять, чтобы чувствовать себя более безопасно в сети и во время использования мобильных телефонов. Руководство содержит советы и информацию об инструментах, позволяющих снизить вероятность мониторинга и слежки, защитить персональные данные и работать в условиях цензуры. Руководство охватывает следующие темы: безопасное использование электронной почты и чатов, правильный подбор паролей, советы по тому, как держать компьютер чистым от вирусов и вредоносных программ, как обходить сетевую цензуру оставаясь анонимным, тактики по безопасному использованию мобильных телефонов, а также ссылки на более подробные ресурсы.

(Если у вас возникли проблемы с доступом к ссылкам, указанным в этом документе, из-за блокирования сайтов уже после использования всех инструментов обхода блокировки упомянутых ниже, пожалуйста, напишите по адресу info@accessnow.org, и дайте нам знать, какие материалы вы бы хотели получить по электронной почте).

На данный момент вся информация в этом пособии считается верной и актуальной на июль 2011 года. Несмотря на это, имейте в виду, что защита в сети является комплексным процессом, изменяющимся с появлением новых технологий и возникновением новых угроз. Нет волшебного средства, гарантирующего абсолютную безопасность и обеспечение неприкосновенности вашей частной жизни, но есть средства и правила, которые точно помогут вам быть более защищенным.

Этот документ был разработан, и совместно редактирован, рядом организаций и частных лиц, специализирующихся на сетевой и мобильной безопасности. Если вы обнаружите неточности в этом документе, или у вас возникнут какие-либо предложения по его улучшению, напишите по адресу: info@accessnow.org

Некоторые важные основы

Безопасность вашей электронной почты

Среди наиболее популярных почтовых сервисов Hotmail и Gmail предлагают возможность безопасного пользования почтой, которое предусматривает шифрование соединения между вами и почтовым провайдером.

Сейчас у Gmail функция HTTPS включена по умолчанию, но вам придется ее включить на Hotmail, если вам этого еще не предложили сделать: нажмите Account (Аккаунт)> Other Options (Другие настройки) > Connect Using HTTPS (Соединение HTTPS) > Use HTTPS Automatically (Использовать HTTPS автоматически). В настоящее время Yahoo Mail не предлагает шифрование соединения, и хотя это хлопотно, мы рекомендуем вам создать альтернативный почтовый ящик, поддерживающий HTTPS, для общения, а также для получения, отправки и хранения важной корреспонденции. Помните, что HTTPS обеспечивает безопасное соединение только между вами и вашим провайдером электронной почты, а доставка до получателя все же может оказаться нешифрованной и уязвимой, если получатель не использует HTTPS или же он использует другой сервис электронной почты. Другие варианты сервиса безопасной электронной почты - Riseup.net и Vaultletsoft. В дополнение, можно использовать прекрасную систему шифрования и цифровой подписи вашей электронной почты – PGP и GPG. (Подробнее об этом на английском и арабском языках).

Если вы используете Gmail и хотите узнать больше о других функциях безопасности (таких как двухэтапная аутентификация и история IP), пожалуйста, обратитесь к проверке безопасности Gmail. Если вы используете Hotmail, вы можете выяснить больше о настройках безопасности, в том числе об одноразовых паролях для использования на компьютерах общего доступа, здесь.

Безопасность паролей

Очень важно, чтобы вы создавали надежные пароли и строго придерживались предписаний по их использованию. Несколько основных советов:

- Подумайте об использовании в качестве пароля фразы, а не отдельного слова.
- Создавайте свои пароли длиной 12 и более символов. Это затруднит взлом пароля с использованием различных программ.
- Используйте комбинацию символов, чисел, прописных и строчных букв. Один из способов состоит в том, чтобы создать пароль из начальных символов (букв и чисел) слов какого либо высказывания или строк(и) из песни или стихотворения.
- Не используйте тот же самый пароль для каждой учетной записи; если ваш пароль будет перехвачен при введении на сайте, не предлагающем HTTPS соединение, легко получить информацию о вашем логине/пароле и использовать ее для того, чтобы получить доступ к другим вашим учетным записям.
- Изменяйте свои пароли каждые 3 месяца, или даже чаще, если вы используете интернет-кафе или чужие компьютеры.
- Если вам сложно запоминать пароли, используйте надежные шифровальные программы для хранения паролей, например, KeePass.
- Некоторые учетные записи ставятся под угрозу благодаря системам восстановления утерянного пароля. Убедитесь, что секретные вопросы для ваших учетных записей, и ответы на них, не так просты и легко угадываемы.

Антивирус и анти-шпионское ПО:

Одна из основных проблем, с которой сталкивается большинство пользователей компьютеров – это использование пиратского Программного Обеспечения (ПО), особенно Microsoft Windows. При нелегальном использовании ПО, вы экономите немного денег, но также вы становитесь уязвимы, так как вы не можете, на законном основании, получать обновления и исправления ПО, выпускаемые производителем. В случае если вы не можете получить официальную, легальную версию ПО и Операционной Системы (ОС), то вам стоит использовать эффективный антивирус и анти-шпионское ПО, для сведения рисков к минимуму. Но, для вашей собственной безопасности, постарайтесь по возможности приобрести официальные копии ПО.

- Если у вас установлено нелицензионное программное обеспечение, то в качестве хорошей бесплатной антивирусной программы для Windows можно использовать Avast, который защитит данные вашего компьютера от повреждения и поражения вирусом. Если компьютер уже был поврежден вирусом, в качестве надежной защиты можно использовать программу Malwarebytes.
- Также важно и анти-шпионское ПО, которое обнаруживает и удаляет вредоносные программы, которые могут отслеживать всю вашу деятельности на компьютере и в сети Интернет. Spybot - бесплатная и эффективная анти-шпионская программа.
- Чтобы снизить риск воздействия вирусов и шпионских программ, не открывайте письма и вложения от неизвестных, не вызывающих доверия источников. Если вы неуверенны в безопасности вложения, файла, веб-сайта, вы можете загрузить его в VirusTotal для проверки или отправить на scan@virustotal.com, указав в теме письма “SCAN” (или “SCAN” +XML, если вы хотите получить результат в XML-формате)
- Еще один общеизвестный способ проникновения вредоносного кода

Некоторые важные основы

– скрипты, с которыми вы сталкиваетесь при просмотре страниц в интернете. Мы настоятельно рекомендуем, чтобы вы скачали и использовали дополнение NoScript к браузеру Firefox. Это дополнение позволит вам блокировать большинство скриптов, позволяя работать только тем, которым вы доверяете.

Это позволяет избежать тотального «сбора» имен пользователя и паролей с помощью встроенного JavaScript, что в настоящий момент является тактикой, используемой правительством Туниса.

- Также широко известным источником заражения компьютеров вирусами и вредоносными программами является использование USB флэш-накопителей. Не подсоединяйте переносные запоминающие устройства к вашему компьютеру, если они не были предоставлены известным вам и надежным источником. Также используйте антивирус и другое ПО например Spybot и Avast для сканирования переносного запоминающего устройства на вирусы и вредоносные программы.

Рассмотрите вариант перехода на операционный систему Ubuntu, основанную на Linux. Конечно, только в случае если у вас нет серьезных причин продолжать использование Windows. ОС Ubuntu позволяет вам по умолчанию шифровать содержимое жесткого диска, и в основном неуязвима перед вирусами и вредоносными программами. Если не принимать во внимание направленные атаки, пользователь Ubuntu гораздо более защищен, чем пользователь пиратской копии Windows без исправлений и обновлений. Mint – другая ОС, основанная на Ubuntu, позволяющая использовать большее число приложений.

Безопасность мгновенных сообщений:

Если вы уверены, что хакеры не взломали ваши учетные записи в Skype и Google Chat, то, при безопасном соединении HTTPS, это отличные варианты использования служб мгновенных сообщений. Гораздо больший уровень безопасности дает использование Pidgin. Эта программа предоставляет доступ к некоторым службам мгновенных сообщений (в том числе и Google Talk). Дополнение к Pidgin под названием Off The Record (OTR) обеспечивает безопасность любых введенных ранее данных, даже если имеются ваши ключи шифрования. Узнайте больше о свойствах безопасности OTR, пример Privacy by Design.

Обеспечьте безопасность своего пребывания в сети Интернет другими способами:

- Для обеспечения анонимности при участии в Сетевых проектах активистов, вы можете создать псевдоним. Используйте этот псевдоним, когда вас попросят представиться, в сети на сайтах и в социальных сетях. Уровень вашей анонимности зависит от вас: многие создают анонимное описание в Твиттере, но у большинства людей учетные записи в социальных сетях (типа Facebook) зарегистрированы на их реальные имена. Использование псевдонима зависит от вас и вашего ощущения серьёзности вероятности пристального наблюдения за вами в сети. Также важно знать, что для Facebook вам придется создать убедительное фальшивое имя. Используя банальный псевдоним в одно слово, ваш аккаунт будет удален вследствие нарушения соглашения о предоставлении услуг.
- Если же вы решили указать свое настоящее имя и пользоваться HTTPS для доступа к сайту, важно, чтобы вы не предоставляли дополнительно важной личной информации, например, такой как номер телефона.
- В настоящее время расширяются возможности применения GPS, для отображения вашего физического расположения, когда вы находитесь в сети Интернет. Это может быть мощным инструментом, используемым в качестве части координационной кампании, при ведении репортажей с помощью сотовых телефонов с места какого-либо рода происшествия или важного события. Однако эта технология также выдает важную информацию о вашем местоположении, и том, чем вы занимаетесь. Мы рекомендуем вам отключить отслеживание GPS в таких программах как Twitter или Bambuser. Вы можете временно включать функцию GPS, если это очень важно для активистского проекта, над которым вы в настоящее время работаете. Даже если значок датчика GPS не отображен на экране, важно чтобы вы отключили сбор подобной информации в вашем браузере, или другой программе.
- При отправлении важной информации другим людям, помните, что получатели могут быть ненадежны. Их списки контактов, адреса электронной почты и прочие способы связи могут быть под контролем и наблюдением. Будьте особенно осторожны, связываясь с людьми, чьи личные данные вы еще не проверили и не подтвердили. В дополнение к вышесказанному: любое прямое послание, посланное кому-либо (знакомому и незнакомому человеку) через Facebook или Twitter может быть прочитано третьими лицами, если только не предпринять определенных действий (ознакомьтесь подробнее с понятием HTTPS и средствами обхода цензуры, описанными ниже).
- Ограничьте до минимума или не используйте вовсе сторонние приложения, имеющие доступ к вашим учетным записям (программы с доступом к Twitter, Facebook, Gmail, и т.д.). Очень часто в них обнаруживаются угрозы безопасности, используемые для взлома учетных записей (вполне безопасных, в случае если вы не будете использовать подобные программы).

Безопасность в сети Интернет

Интернет в большой степени подвергается цензуре во многих странах региона, таких как Бахрейн, Кувейт, Оман, ОАЭ, Катар, Сирия и Саудовская Аравия. Он также находится и под контролем, хотя и неизвестно насколько серьезен этот контроль. Если вы сможете обойти цензуру, гораздо сложнее будет обойти контроль. Если вы предполагаете, что ваша деятельность может контролироваться и фиксироваться, вам стоит попробовать использовать безопасный, анонимизирующий прокси сервис. В дополнение мы настоятельно рекомендуем не использовать Internet Explorer в качестве вашего браузера, так как у него достаточно много уязвимых мест, особенно в его пиратских версиях. Превосходная замена ему – бесплатная программа с множеством полезных дополнений - Firefox от Mozilla.

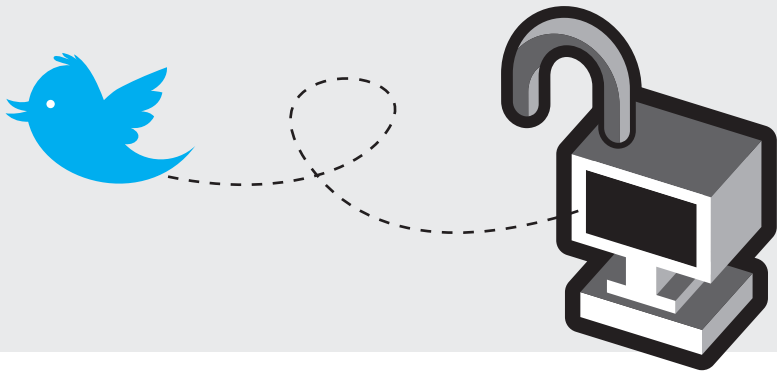
Шифрование своей деятельности в сети с помощью HTTPS

Если вы вовлечены в активистскую деятельность в Интернете, важно работать так, чтобы ваша личность и пароли остались неизвестными и в безопасности. Недавно мы наблюдали в Тунисе широкомасштабную фишинговую кампанию по сбору логинов и паролей граждан, пользующихся Facebook, путем использования уязвимости HTTP. К счастью, Facebook своевременно отреагировал, включив HTTPS, что очень помогло. По возможности, вы всегда должны использовать HTTPS. При невозможности использования HTTPS, очень важно чтобы вы пользовались системами безопасных прокси-серверов какого-либо вида. Цензор может запретить использование HTTPS для конкретных пользователей или определенных сайтов, а если вы используете такие анонимизирующие прокси как Tor, цензорам будет очень сложно, или вообще невозможно, осуществить подобные запреты.

HTTPS

HTTPS Everywhere – великолепное дополнение к браузеру Firefox, легкое в использовании, которое вы должны использовать. Оно «заставляет» сайты, по возможности, использовать HTTPS соединение. **Скачивание этого дополнения должно быть одним их первых шагов для использования полного (end-to-end) шифрования соединений с такими сайтами, как Facebook, Twitter, поиск Google и многих других.** Это также уменьшит вашу уязвимость в случае попыток злоумышленников перехватить ваши пароли, когда вы используете общедоступные или незащищенные беспроводные сети Wi-Fi.

- Если вы все еще не скачали последнюю версию Firefox, обязательно сделайте это. Затем скачайте HTTPS Everywhere и/или Force TLS, перезапустите Firefox, и произведите настройку этих дополнений. Примечание: в HTTPS Everywhere уже есть некоторое количество сайтов в настройках по умолчанию, которые можно изменить. В случае с Force TLS вам самой/самому придется настроить список сайтов для обязательного использования HTTPS.
- Если вы используете Google Chrome, скачайте KB SSL Enforcer Extension. *(Примечание: это дополнение не так эффективно как вышеуказанное дополнение к Firefox. В SSL Enforser есть несколько ошибок. Тем не менее, мы предполагаем, что со временем все ошибки будут устранены.)*



Facebook

Несмотря на то, что вышеописанное дополнение Firefox включает HTTPS на многих сайтах, если вы используете Facebook часто, хорошей идеей было бы убедиться, что доступ к Facebook через HTTPS настроен по умолчанию, особенно если вы заходите на сайт Facebook с разных компьютеров.

- Для включения HTTPS для Facebook, щелкните по надписи «Аккаунт» в верхнем правом углу > настройка аккаунта > щелкнув по слову «Изменить», в разделе «Безопасность аккаунта», включите «Безопасный просмотр».
- Использование некоторых игр или других приложений Facebook отключит использование HTTPS.
- Facebook также предлагает использовать и другие опции безопасности, такие как удаленный выход и уведомление о входе. Это позволит вам ограничить количество устройств, которые могут иметь доступ к вашему аккаунту. Видео, описывающее возможности безопасного доступа к Facebook, можно посмотреть на их сайте. Еще одно руководство по защищенному использованию Facebook вы можете найти здесь.

Twitter

Хотя дополнение Firefox, о котором говорилось выше, также работает и для сайта Twitter, лучше настроить Twitter на использование HTTPS соединения по умолчанию, с какого бы устройства вы не пользовались его сервисом. Это особенно важно, если вы заходите на этот сайт с нескольких или общественных компьютеров.

- Для включения HTTPS на Twitter, щелкните переключатель в верхнем правом углу > настройки > в самом низу страницы отметьте «Всегда использовать HTTPS».
- Примечание: в настоящее время применение этой настройки не работает для сотовых телефонов. До тех пор, пока это не будет исправлено, с мобильных устройств всегда заходите на сайт по ссылке https://mobile.twitter.com.

Обход цензуры: посещение заблокированных сайтов

Несколько стран региона широко применяют фильтрацию большого числа сайтов и блогов. Было бы разумно предположить, что эта фильтрация означает также и высокий уровень контроля (слежки) за пользователями, хотя уровень этого контроля различен в разных странах. Для того чтобы посещать заблокированные сайты и загружать данные на них, вы можете использовать средства обхода цензуры. Важно отметить, что есть разница между шифрованием и анонимностью: хорошее средство обхода цензуры шифрует трафик между пользователем и провайдером этого средства обхода, но не сможет шифровать трафик между этим провайдером и сайтом, который вы просматриваете. Именно поэтому важно использовать HTTPS везде, где только возможно, так как это даст полное шифрование трафика. Но и использование только HTTPS не сможет дать вам доступ к заблокированному сайту, поэтому важен обход этой блокировки. Ваш IP адрес всегда определяется и запоминается сайтом, на который вы заходите. Только используя анонимизирующий прокси (такой как Tor) ваш IP адрес по настоящему, и надежно скрыт. Множество сайтов запоминают IP адреса ваших последних подключений, и, следовательно, в случае взлома ваших учетных записей, ваши предыдущие местонахождения будут известны злоумышленникам.

Обход межсетевых экранов

Простейшие веб-прокси позволяют пользователям получить доступ к заблокированным сайтам через свою страничку. Пользователь открывает сайт прокси и вводит в специальной форме адрес того сайта, на который он хочет зайти, а прокси сам заходит на этот сайт и отображает его пользователю. Прокси HTTP/SOCKS перенаправляют трафик по протоколам, позволяющим пройти через брандмауэры. IP адреса и номера портов прокси вы сможете найти на общедоступных сайтах, и их нужно будет ввести в настройках браузера.

Несмотря на то, что простейшие веб-прокси и прокси HTTP/SOCKS обычно используются для обхода блокировки, они не предоставляют анонимности (ваше использование этих прокси может быть отслежено) и почти всегда неизвестно кто предоставляет эти прокси. Существует вполне определенный риск использования подобных прокси сервисов, так что мы рекомендуем использовать такие системы как Tor, которые одновременно предоставляют средство обхода и обеспечивают анонимность.

Еще одно средство, основанное на прокси - Psiphon, это веб-прокси, работающий на компьютерах с Windows и Linux. Узлы Psiphon`а не открыты широкой публике как обычные прокси. Psiphon позволяет людям без специального компьютерного оборудования, желающим предоставить небольшому количеству «друзей», находящихся в другой стране, возможность зайти на сайт, заблокированный в их стране. Эта схема называется сеть-на-доверии (web-on-trust), так как «друг», предоставляющий прокси Psiphon`а сможет получить доступ ко всему трафику, проходящему через его узел, и, следовательно, необходимы доверительные отношения между предоставляющим свой узел и теми людьми, которые его используют. **Psiphon ведет запись данных пользователей, но их IP адреса анонимны.** Psiphon`у сложно работать с HTTPS и сайтами Web 2.0. Эти ограничения устраняются в новом PsiphonX.

Обход цензуры: посещение заблокированных сайтов

Tor: анонимность в сети

Tor – сложный и высококачественный инструмент, помогающий обойти фильтрацию и обеспечить вашу анонимность в сети. Однако его основной недостаток заключается в том, что он работает медленнее других решений для просмотра веб-страниц. Tor Browser Bundle отвечает за всю процедуру установки, а использование Tor Bridge поможет получить доступ в условиях жесткой фильтрации.

Существует множество способов использования Tor, но мы рекомендуем загрузить Tor Browser Bundle, который позволит использовать Tor на компьютерах с ОС Windows, Mac OS X или Linux, не требуя установить многочисленные приложения. Просто запустите Tor Browser Bundle, одновременно активируется настроенная версия Firefox вместе с приложением Vidalia, которое контролирует работу Tor, и сконфигурировано таким образом, чтобы соединять и пересылать весь трафик через сеть Tor. Вы можете установить Tor Browser Bundle на USB-носитель и использовать на любом компьютере, когда вам это понадобится. Найти Browser Bundles с функцией отправки мгновенных сообщений или без нее на разных языках (включая арабский и фарси) можно здесь: сайт загрузки Tor. Поскольку использование Tor может замедлить работу браузера, мы советуем использовать 2 браузера: один с Tor для доступа к конфиденциальной или заблокированной информации, а второй браузер для работы с неконфиденциальными данными. Если Tor будет все время подключен, со временем он станет работать более эффективно, и вы заметите это за счет увеличения скорости. Если вы находите, что доступ к сайтам через Tor все же слишком медленный, а информация, которую вы хотите увидеть, выложена в виде текста, вы можете отключить загрузку картинок и java-скриптов в своем браузере. Это намного ускорит загрузку страниц через Tor.

К сожалению, главный сайт проекта Tor, указанный выше, зачастую блокируется в большинстве стран региона. Но вы сможете получить программу одним из следующих способов:

- Посетив сайт проекта Tor через HTTPS соединение: https://www.torproject.org/
- Задав в строке поиска Google “tor mirror”, чтобы посмотреть зеркало страницы torproject.org. Вы также можете просмотреть официальный перечень зеркал, если введете в Google-поиске “site:torproject.org mirrors” и посмотрите кеш страницы “Tor Project: Mirrors”.
- Также вы можете отослать запрос роботу «GetTor» на электронную почту gettor@torproject.org. Примечание: для обеспечения безопасности используйте защищенную HTTPS почту Gmail для отправки письма на gettor@torproject.org. Выберите один из вариантов комплекта и напишите его название в тексте вашего письма:

• tor-im-browser-bundle для Windows (Tor и клиент мгновенных сообщений);

• tor-browser-bundle для Windows ИЛИ Intel Mac OS X ИЛИ Linux (Tor браузер);

• torbutton (только дополнение к Firefox).

вскоре после отправки письма, вы получите ответ от робота «GetTor» с ПО, которое вы запросили, в архиве ZIP. Для получения дальнейшей помощи при использовании Tor – пишите на tor-assistants@torproject.org.

Примечание: Tor также работает на телефонах с ОС Android под именем “Orbot”. Это приложение можно найти на Android Market или закачать прямо с веб-сайта Tor, в том числе с его зеркал.

Еще один способ обхода цензуры, шифрующий соединение и предоставляющий анонимность – это сеть VPN. Вы можете прочитать более подробно о настройке сети здесь. Также вы можете скачать бесплатную версию VPN Hotspot Shield здесь или, отправив электронное письмо на адрес hss-sesawe@anchorfree.com (в теме письма укажите одно из этих слов: “hss”, “sesawe”, “hotspot”, “shield”).

Другие широко используемые способы обхода цензуры - Ultrasurf и Freegate. Все вышеуказанные VPN - хороши для доступа к заблокированным сайтам, но важно понимать что, как и обычные веб-прокси или прокси HTTP/SOCKS, они не являются анонимайзерами (не скрывают вашу идентификационную информацию при их использовании). В дополнение, эти службы сами фильтруют и блокируют сайты, которые они не поддерживают или которые не одобряет их оператор. Более того, известно, что эти сайты собирают данные обо всех пользователях. Это коммерческие проекты, и зарабатывают они на рекламе, отображаемой в зависимости от ваших предпочтений (сайтов на которые вы заходите; того, что вы ищите; и т. д.). Это является очень важной проблемой для людей, ищущих полной анонимности, или просто конфиденциальности при использовании инструментов для обхода цензуры.

Важное примечание: Когда власти страны имеют возможность контролировать Интернет, они могут применить несколько других вариантов контроля, ставящих под угрозу вашу безопасность и конфиденциальность. Например, с помощью вредоносного кода и установки сертификатов безопасности. Для борьбы с этими угрозами, используйте средства и тактики, описанные выше, а также пытайтесь следить за новостями или предупреждениями сетевых активистов вашей страны, которые могут распознать эти угрозы и заблаговременно известить вас о них.

Больше сведений: Видео уроки использования различных средств обхода цензуры на английском, арабском, русском и узбекском языках (от 12 pm Tutorials).

Мобильные устройства

Множество активистов были выслежены через свои сотовые телефоны. Одни страны осуществляют более сильный контроль (и прослушивание) мобильной связи, чем другие. Например, египетские активисты испытали на себе этот сильный контроль на всех уровнях. Египетские власти использовали технологии для удаленного использования телефонов в качестве устройств прослушивания, даже если в это время телефоны были отключены. Вам самим нужно оценить риск для ваших мероприятий, в соответствии с обстановкой в вашей стране. Нужно принять во внимание, фактор важности вашей работы, а также информацию о том, что люди из вашего окружения испытали на себе. Операторы сотовой связи имеют возможность отследить и собрать информацию об использовании вашего сотового телефона, включая ваше местонахождение. Операторы сотовой связи могут передать эту информацию властям по их запросу.

Также существует опасность установки на ваш телефон программы слежения, которая работает в фоновом режиме, не информируя пользователя. Этот риск существует, если вы оставляете свой телефон без присмотра.

Когда ваш телефон включен, он постоянно обменивается с вышками сотовой связи следующей информацией:

- Номер IMEI – это уникальный серийный номер вашего телефона.
- Номер IMSI – уникальный номер SIM карты, привязанной к вашему телефонному номеру.
- Номер TMSI – временный номер, переназначающийся регулярно, в соответствии с местонахождением или изменением покрытия сети, но его можно отследить системами прослушивания, находящимися в продаже.
- Соту сети, в которой телефон находится в настоящее время. Соты могут покрывать любую площадь от нескольких метров до нескольких километров. В городе – соты меньшего размера, а размер соты в здании (с использованием репитера, усиливающего сигнал в помещении) еще меньше.
- Положение абонента в соте, определяется методом триангуляции (измерением уровня сигнала от ближайших вышек). И снова – точность определения местонахождения телефона зависит от размера соты – чем больше вышек на ее территории – тем точнее будет определение положения.

Из всего вышесказанного следует, что люди и службы, имеющие доступ к информации телекоммуникационной компании, могут использовать ваш телефон как устройство слежения, если телефон включен и у него есть связь с сетевыми вышками. А телекоммуникационная компания может предоставить следующую информацию о вашем телефоне:

- Входящие и исходящие звонки телефона.
- Ваши СМС отправленные/полученные, с информацией о получателях/отправителях.
- Любые данные по использующимся услугам (например, просмотр страниц без использования HTTPS, и небезопасный клиент мгновенные сообщений) а также объем переданных данных (например, «закачивали ли вы что-нибудь на YouTube»)
- Ваше приблизительное местонахождение (с точностью от нескольких метров до нескольких километров, в зависимости от плотности расположения вышек).

Мобильные устройства

Важное примечание: если вы считаете, что за вами установлено наблюдение, не всегда достаточно сменить SIM карту – вас всегда можно будет отследить по номеру IMEI вашего телефона.

Также очень много информации находится непосредственно в вашем телефоне, и эта информация может быть использована против вас, если телефон будет конфискован или если его попросту у вас заберут. У всех сотовых телефонов есть небольшой объем памяти на SIM карте, а также есть внутренняя память самого телефона. (В дополнение к этому у многих телефонов есть возможность увеличить объем памяти с помощью SD (или MicroSD) карт памяти для хранения мультимедийных и прочих файлов). **Обобщая, можно сказать следующее: лучше хранить данные на SIM карте и карте памяти SD (если таковая имеется), чем в памяти телефона, потому что гораздо легче извлечь и уничтожить данные на SIM и/или SD карте.**

Данные, хранящиеся на SIM карте, внутренней памяти телефона, и (если такая имеется) на SD карте памяти, включают в себя:

- Вашу телефонную книгу – имена контактов и номера телефонов.
- Вашу историю звонков – кто звонил вам, кому звонили вы, и когда эти звонки совершались.
- Полученные и отправленные СМС.
- Данные любых приложений, используемых вами, таких как календарь или список дел.
- Фото и видео, снятые с помощью камеры телефона, конечно если у вашего телефона есть камера. Большинство телефонов отмечают время, когда была сделана фотография, а также могут отмечать и место (координаты), где была сделана эта фотография.

В телефонах, позволяющих просматривать страницы Интернет, также сохраняется история просмотра страниц. По возможности, очищайте эту историю. Сообщения электронной почты тоже таят в себе потенциальную угрозу, в случае если злоумышленник получит доступ к SIM карте или памяти телефона.

Также как и жесткий диск компьютера, память SIM карты вашего телефона содержит любую информацию, сохраненную на ней. Только при заполнении памяти поверх старых данных будут записаны новые. Это означает, что даже удаленные СМС, данные о совершенных звонках и контакты, потенциально могут быть восстановлены с SIM карты. (Для этого даже существует бесплатная программа, использующая считывающее устройство смарт-карт). Вышесказанное применимо и к внутренней памяти телефона, и к картам памяти. Как правило, чем больше памяти в телефоне, тем дольше удаленные данные могут быть восстановлены.

Так что же это для вас значит?

Мобильные устройства могут быть очень полезными инструментами для активистов, но также они могут стать невероятной обузой, если власти или службы безопасности будут работать совместно с телекоммуникационными компаниями для слежения за вами. **Если вы находитесь в стране, власти которой активно используют сотовые телефоны для слежения, особенно если вы считаете, что за вами ведется наблюдение из-за вашей деятельности, рекомендуем не использовать для связи сотовые телефоны. Лучше встречайтесь лично.**

В конце концов, оценка рисков на которые вы идете, зависит только от вас. Если вы не считаете, что вас воспринимают как важного активиста или как часть кампании по наблюдению, и вы хотите использовать свой сотовый телефон для связи с товарищами-активистами, хотите записывать видео и делать фотографии, или передавать информацию, то вы можете воспользоваться следующими практическими советами:

- Создайте и используйте систему кодовых слов для общения с товарищами-активистами.
- Используйте сигналы в качестве системы оповещения (например, два раза позвонить и сбросить означает, что вы добрались на место и с вами все в порядке.)
- Не используйте настоящие имена друзей-активистов в телефонной книге контактов. Используйте номера или псевдонимы. В этом случае, если спецслужбы изымут у вас телефон или SIM карту, у них не будет данных на всю сеть активистов.
- Захватите с собой на митинг протеста запасные SIM карты, если вы знаете, что их у вас отберут. Также важно, чтобы с вами был рабочий сотовый телефон. Если вам нужно будет избавиться от SIM карты, постарайтесь физически ее уничтожить.
- Если ваш телефон может быть защищен паролем – используйте его. Это может быть PIN номер вашей SIM карты: у SIM карты есть номер PIN по умолчанию, по возможности смените его и включите блокировку на вашу SIM карту. В этом случае вам будет необходимо вводить пароль (ваш PIN номер) перед каждым использованием телефона.
- Если вы считаете, что митинг может быть встречен большими силами спецслужб для его разгона, вам, возможно, нужно будет перевести телефон в режим полета на это время. В этом режиме вы не сможете позвонить или принять вызов, но вы сможете фотографировать и снимать на камеру, и позже загрузить все это в сеть. Этот совет также будет полезен, в случае если вы подозреваете, что службы безопасности при разгоне будут задерживать любого человека с сотовым телефоном. Позже власти могут запросить данные по звонкам, СМС, переданным данным на всех людей, находящихся в определенном месте в определенное время для проведения впоследствии массовых арестов.
- Отключите отслеживание положения и фиксирование географических координат во всех приложениях на

Мобильные устройства

вашем телефоне, если конечно вы не используете эти приложения как часть вашего проекта для привязки определенных медиа-файлов к какому-либо событию. Если вы используете ваш телефон для живых видео трансляций в сеть, отключите GPS/фиксирование географических координат в свойствах телефона / программы. (Указания для Bambuser).

- Если ваш телефон работает под управлением ОС Android, вы можете использовать несколько средств, созданных Guardian Project и Whispersys для шифрования просмотра веб-страниц, мгновенных сообщений, СМС и голосовых звонков.
- При использовании телефона для просмотра веб-страниц, по возможности всегда используйте HTTPS.

Другие ресурсы:

- Mobiles in a Box (английская версия) от Tactical Tech
- Mobile Security Risks Primer (английская версия) от MobileActive

Пользователям BlackBerry:

Производитель BlackBerry компания Research in Motion (RIM) предоставляет два вида сервиса с соответствующим уровнем шифрования. Для обычных частных потребителей никогда не существовало полного E2EE шифрования коммуникации – RIM или ваш провайдер мобильной связи в любой момент могут перехватывать звонки, электронные письма, SMS, отслеживать работу в браузере и т. д. И наоборот, корпоративные пользователи, чья компания использует BlackBerry Enterprise Server (BES), имеют полное E2EE шифрование в своей почте, клиенте обмена мгновенными сообщениями и браузере. Однако, даже если вы корпоративный пользователь, помните, что человек, отвечающий за сервер компании (обычно это ваш системный администратор) располагает средствами для расшифровки вашей коммуникации. Более того, существует множество легальных полулегальных процедур, которые правительство может использовать для доступа к вашей зашифрованной коммуникации.

Недавно правительство ОАЭ пыталось заставить производителя BlackBerry – RIM дать им ключи дешифровки для всех способов связи BlackBerry, но компания отказалась это сделать. Пользователям BlackBerry стоит постоянно быть в курсе последних переговоров правительства их стран с RIM по этим вопросам. Также пользователям стоит опасаться других попыток перехвата шифрованных видов связи BlackBerry. В 2009 году в ОАЭ компания Etisalat разослала пользователям BlackBerry неофициальное «обновление», позволяющее телекоммуникационным компаниям получать копии всех сообщений пользователя. Вскоре RIM разослала владельцам BlackBerry обновление, удаляющее это вредоносное ПО. Однако пользователям телефонов BlackBerry стоит опасаться любого подозрительного обновления ПО, которое выпущено не компанией RIM.

Другое:

Блоги:

Если у вас есть блог или вы хотите его создать, существует ряд полезных ресурсов для установки и настройки блога. Ваша главная задача – сохранить личную информацию в тайне и обеспечить возможность другим пользователям читать ваш блог, если госструктуры ставят на него блокировку. Ниже указаны ресурсы для настройки и зеркалирования вашего сайта, если вход через первоначальный URL-адрес заблокирован:

- Ведение анонимного блога с помощью wordpress и Tor (Global Voices)
- Зеркалирование блога wordpress, подверженного цензуре (Global Voices)
- Советы, как вести безопасно блог (EFF)
- Справочник для блоггеров (Reporters Without Borders)

Запись видео:

Книга: Видео ради перемен на арабском и видео: Как создавать видео ради перемен с арабскими субтитрами (Witness).

Другие ресурсы по обеспечению безопасности и использованию цифровых технологий в общественно-политической деятельности:

Tactical Tech & FrontLine:
Security in a Box:
арабская версия
английская версия

The Electronic Frontier Foundation:
подробное руководство:
Surveillance Self-Defense
и краткая инструкция:
International edition of SSD
(оба на английском).