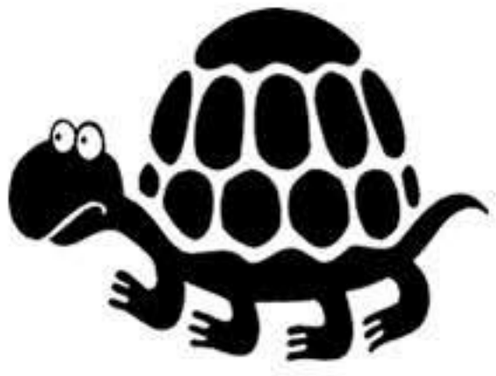
КОНФИДЕНЦИАЛЬНОСТЬ В СЕТИ ИНТЕРНЕТ ДЛЯ ЖУРНАЛИСТОВ

Обязательное к прочтению руководство 2017 года для журналистов

Автор: **МАЙКЛ ДЕГАН,**
экс-заместитель главного редактора газеты «Гаарец».

Профессиональный консультант: **Ариэль Хохштадт**,
эксперт по вопросам безопасности, экс-руководитель
отдела маркетинга Gmail в компании Google.

Аннотация: **Роман А. Захаров**,
руководитель службы безопасности Фонда защиты гласности.



Фонду защиты гласности выпала честь представить русский перевод превосходного пособия Майкла Дегана, посвященного актуальной теме интернет-безопасности. Точнее, сохранения конфиденциальности при работе в Сети. А ведь Интернет является одним из важнейших на сегодня инструментов для журналистов: мы ищем информационные поводы, проверяем информацию и данные в социальных сетях и на веб-сайтах, мы общаемся с источниками и коллегами посредством электронной почты, тех же социальных сетей и всевозможных мессенджеров, мы публикуем свою информацию в Сети и здесь же получаем отзывы и отвечаем на них. Иными словами, жизнь современного журналиста без Интернета сложно себе представить, но тем важнее научиться пользоваться им, чтобы не подвергать опасности себя и редакцию, а также наши источники. Журналистская тайна - это не прихоть, ведь без ее соблюдения мы не можем рассчитывать на доверие к нам со стороны тех, кто решается поделиться информацией на условиях сохранения анонимности. Особенно остро стоит вопрос овладения подобными навыками в России: увы, но в нашей стране за последние годы изменилось отношение властей и общества к журналистским привилегиям. Мы не можем рассчитывать на защиту государственных органов в вопросе охраны конфиденциальных данных, ставших нам известными в ходе профессиональной деятельности. Напротив, государство в лице сотрудников спецслужб и правоохранительных органов в целом раз за разом убедительно доказывают, что они готовы нарушать закон, взламывая (вместе с подконтрольными хакерами) редакционные сервера и почтовые ящики отдельных журналистов, аккаунты в социальных сетях и мессенджеры, подслушивая и записывая переговоры... И даже в тех случаях, когда подобные нарушения происходят без прямого участия властей, государство не спешит на помощь, а часто просто отказывает в расследовании и профилактических действиях, которые могли бы пресекать подобные преступления. Общество же безмолвствует, поскольку не понимает важности журналистской работы.

Поэтому призываем всех работающих в России коллег очень внимательно ознакомиться с советами, которые приводятся в пособии. Уверены, что следование им снизит риски, возникающие при работе с Интернетом.

Роман А. Захаров
Руководитель службы безопасности Фонда защиты гласности

СОДЕРЖАНИЕ

СОДЕРЖАНИЕ

01

ВВЕДЕНИЕ

Многие журналисты со стажем (и не только они) не могли не заметить, что все мы вдруг стали постоянно слышать и видеть упоминания Уотергейтского скандала. На полках книжных магазинов стоят экземпляры «1984» Джорджа Оруэлла и подобные им, а угроза свободе слова и свободе печати медленно расползается как черное облако по всему Западному полушарию, заставляя нас вспоминать давние страхи.

Действующий президент США обвиняет экс-президента в тотальной слежке за своими гражданами, он закрывает доступ центральным СМИ США к своим пресс-конференциям, до этого считавшийся неоспоримым правом, он непрерывно обвиняет СМИ в том, что они являются злейшими врагами своей страны. Неудивительно, что на ум после каждого жалостливого твита о выпуске новостей SNL то и дело приходит эпоха президента Никсона. Неудивительно, что даже сенаторы от Республиканской партии, такие как Джон Маккейн, выражают страх за будущее демократии.

И Маккейн не одинок в своих опасениях. Многие журналисты, с которыми я недавно говорил, озабочены тем, что же станет дальше со свободой печати. Во времена, когда можно заявить, что NSA находится под контролем Дональда Трампа, и тебя при этом не просчитают лжецом, возможно все. Добавьте к этому тот факт, что недавние новости, касающиеся ЦРУ, показали нам, что почти каждую систему шифрования можно взломать при достаточной настойчивости, – и вот мы уже на пути к претворению в реальность мрачной антиутопии, где вы не сможете даже расслабиться на своем собственном диване перед своим собственным «умным» телевизором.

Хорошие новости в том, что все же можно помешать тем, кто попытается перехватить ваши электронные письма, сообщения или звонки. Вы можете принять меры, чтобы значительно усложнить жизнь тому, кто захочет раскрыть ваши источники и выудить информацию, которую вам сообщили. Конечно, то, насколько сильно вы готовы постараться защитить свою конфиденциальность, анонимность вашего источника и

безопасность информации, всегда должно зависеть от вероятности подвергнуть все это реальной угрозе, будь то взлома или шпионажа.
«Старомодные обещания, типа «Я не раскрою личность своего источника и не отдам третьим лицам свои записи», уже ничего не стоят, если только вы не делаете что-то, что может действительно защитить ваши цифровые данные», – говорит Бартон Джеллман из газеты Washington Post, чей источник, Эдвард Сноуден (бывший служащий Агентства национальной безопасности США), помог обнародовать информацию о ряде операций АНБ и Центра правительственной связи Великобритании, дав интервью Тони Лоци. Сама же Лоци, освещавшая работу американской системы судебной защиты для изданий AP, The Washington Post и USA, и которая была обвинена в неуважении к суду за то, что отказалась открывать свои источники, возможно, одобрила бы это.

Итак, что же нужно сделать, чтобы надежно обезопасить рабочие материалы и источники журналиста? В общих чертах можно распределить советы по следующим категориям:

Изоляция своих устройств и/или среды, в которой они функционируют. Например, физическая изоляция компьютера с целью работы над документами или использование предоплаченных мобильных устройств.

Защита приложений и функций устройства. Эта тактика известна как уменьшение “поверхности атаки”. По сути, это ограничение числа установленных приложений до необходимого минимума, загрузка приложений только из надежных источников, выбор приложений, которые требуют меньше прав, поддержка системы в работоспособном и обновленном состоянии, а также наличие как можно меньшего количества систем безопасности (исходя из самых актуальных экспертных заключений, конечно же) на устройстве.

Осмотрительное поведение как в виртуальном, так и в реальном мире. Этот раздел относится не столько к программному обеспечению, сколько к здравому смыслу. Например, никогда не записывайте имя источника, особенно в приложениях или документах, которые установлены или хранятся на вашем компьютере, и уж тем более нельзя делать этого в файлах, которые хранятся в облаке.

02

КОММУНИКАЦИЯ С ИСТОЧНИКОМ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Начнем со списка действий, которые можно выполнить, когда вы общаетесь с источником и фиксируете конфиденциальную информацию, полученную от него:

1. Всегда шифруйте любые данные. Эксперты по безопасности прибегают к простейшей математике, чтобы донести до нас свою мысль: как только вы повышаете стоимость расшифровки своего файла (к примеру, для спецслужб, таких как АНБ), вы автоматически увеличиваете усилия, потраченные на слежку за собой. Если вы не являетесь при этом Челси Мэннинг, Джулианом Ассанжем или Эдвардом Сноуденом и не находитесь в зоне активного наблюдения где-то поблизости от апартаментов Трамп-тауэр, возможно, на вас махнут рукой, даже если вы храните зашифрованные файлы. А если кто-то все-таки решит отслеживать ваши данные, несмотря на все ваши усилия, вы станете настоящей головной болью, прибегнув к такому устойчивому шифрованию, как передовой стандарт шифрования (AES), и таким инструментам, как алгоритм шифрования PGP или протокол openVPN - самым надежным из доступных методов шифрования (виртуальные частные сети использует само правительство США).
Но если вам нужна непробиваемая защита, вам понадобится что-то существенней метода шифрования AES. Постскриптум: если вы хотите узнать, в каком году АНБ получило доступ к вашим данным, посмотрите здесь.

2. Выполняйте полное шифрование дисков. Это нужно делать на тот случай, если ваш компьютер или телефон попадет к третьим лицам. Полностью зашифровать данные на диске можно с помощью FileVault, VeraCrypt или BitLocker. Если вы оставляете компьютер в спящем режиме, а не выключаете его или не переводите в режим гибернации, злоумышленник может легко обойти защиту. Здесь вы найдете подробные инструкции от Мики Ли о том, как зашифровать свой ноутбук.

3. Не доверяйте программным продуктам крупных компаний. Всегда исходите из того, что в шифровальных системах крупных компаний и, возможно, даже в самых популярных операционных системах (в проприетарном ПО, иначе говоря) есть лазейки, через которые в них могут проникнуть секретные службы стран-производителей (как минимум, США и Великобритании). Брюс Шнайер, эксперт в области безопасности, поясняет эту мысль здесь.

4. Избегайте общения с источниками по телефону. Все телефонные компании хранят данные, связанные с номерами телефона звонящего и принимающего звонок, а также данные о местоположении устройств на момент совершения звонка. В США и ряде других стран такие компании

по закону обязаны предоставлять информацию о зарегистрированных звонках своей сети.
Что можно сделать в этом случае? Вам следует пользоваться безопасными приложениями для голосового общения – например, приложением Signal, которое неоднократно тестировалось на предмет безопасности. Хоть это и означает, что и вам, и вашему источнику нужно будет загрузить и установить приложение, но процесс занимает всего несколько минут. Вот руководство пользователя для этого приложения. Чтобы поднатореть в использовании приложения, проверьте, сколько ваших друзей, далеких от журналистики, сидят в нем.
Какой бы способ общения с источником вы ни выбрали, никогда не берите мобильный телефон на встречи, носящие конфиденциальный характер. Купите одноразовое устройство и найдите способ передать его номер источнику заранее. У источника также должен быть одноразовый безопасный телефон. Власти могут отслеживать ваши передвижения через сеть сотовой связи, и лучше бы вам сделать все возможное, чтобы задним числом не выяснилось, что вы сидели именно в том кафе, где находился источник. Если вы не будете следовать этому правилу, то все, что понадобится местным органам власти – попросить (вежливо и абсолютно законно) предоставить видео с камер безопасности кафе на тот момент, когда происходила ваша встреча.

5. Отдавайте предпочтение защищенным мессенджерам. Ваши звонки (как по сотовому, так и по стационарному телефону) могут отслеживаться правоохранительными структурами, и каждое SMS-сообщение подобно почтовой открытке, т.е. любой текст полностью видим для тех, кто перехватит его. Поэтому пользуйтесь такими мессенджерами, при помощи которых можно совершить прямой вызов абонента: Signal, который уже упоминался выше, и Telegram считаются самыми безопасными (хотя веб-приложения Telegram и WhatsApp ранее были взломаны, но затем эти уязвимости закрыли). Некоторые эксперты также утверждают, что в этих целях можно пользоваться SMSSecure, Threema и даже Whatsapp.
Вообще-то говоря, протокол Signal уже внедрен в WhatsApp, Facebook Messenger и Google Allo, поэтому разговоры, осуществляемые при помощи этих сервисов, шифруются. Тем не менее, в отличие от Signal и WhatsApp, Google Allo и Facebook Messenger не шифруют данные по умолчанию и даже не уведомляют пользователей, что изначально разговоры не шифруются, хотя в дополнительном режиме можно настроить межабонентское шифрование. Вы также должны иметь в виду, что оба мессенджера (Facebook и WhatsApp) принадлежат Facebook.

Adium и Pidgin – два наиболее популярных клиента мгновенного обмена сообщениями для Mac и Windows, которые поддерживают протокол шифрования OTR (Off the Record) и Tor – самый лучший зашифрованный браузер в сети, к которому мы еще вернемся позже (посмотрите, как подключить Tor к Adium здесь, а к Pidgin – здесь). Естественно, вы можете пользоваться непосредственно Tor Messenger, который, вероятно, является самым безопасным из всех.
Два последних замечания по поводу обмена сообщениями. Во-первых, эксперт по информационной безопасности, с которым я обсуждал этот вопрос, сказал, что вы всегда должны помнить о том, что текст может быть надежно зашифрован, но тот факт, что два конкретных человека конкретно сейчас о чем-то разговаривают, может не остаться незамеченным.

Во-вторых, вы никогда не должны забывать удалять сообщения из памяти своего телефона (хотя даже этого может быть недостаточно, чтобы скрыть сообщения от судебных экспертов) – просто на тот случай, чтобы избежать огласки сообщений, если телефон попадет не в те руки.

Как долго вас прослушивает АНБ?

Если ранее вы продолжительное время пользовались электронной почтой, видеочатом или голосовым чатом, просматривали и выкладывали видео, фотографии, хранили информацию, совершали VoIP-звонки, передавали файлы, транслировали видео при помощи одного из следующих сервисов, то вы внесены в базу данных АНБ:

КОММУНИКАЦИЯ С ИСТОЧНИКОМ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6. Не пользуйтесь чатами организаций. Не заходите в Slack, Campfire, Skype и Google Hangouts для ведения конфиденциальных переговоров. Эти сервисы легко взломать, и они обязаны предоставлять частную информацию по требованию суда или для разрешения юридических вопросов на рабочем месте. Следовательно, лучше избегать их, и не только когда дело касается общения с источником, но и во время общения с коллегами, редакторами и т.д., когда вам нужно передать информацию, полученную от источника, чья личность должна оставаться тайной. Во многих популярных VoIP-сервисах (например, в Jitsi) есть встроенные функции чата, а в нескольких из них даже есть большинство тех же функций, что и у Skype, поэтому они могут стать отличной заменой.

7. В крайних случаях попробуйте воспользоваться Blackphone. Этот телефон, разработчики которого стремятся обеспечить непробиваемую защиту во время работы в сети, совершения звонков, отправки текстовых сообщений и электронных писем, является, вероятно, наилучшей заменой обычному телефону, если вы собираетесь свергнуть правительство или готовите публикацию секретных военных сведений. Пуленепробиваемый жилет тоже может пригодиться. Как вариант, постарайтесь обойтись без мобильного телефона, либо возьмите на вооружение блокирующий сигнал чехол для сотового, работающий по технологии RFID. Всегда остается вероятность, что даже криптофон можно отследить по его номеру IMEI (международному идентификатору мобильного устройства).

8. Защищайте данные на своем компьютере. Очень просто взломать обычные пароли, а вот на взлом кодовых фраз (случайных комбинаций слов) можно потратить годы. Мы рекомендуем воспользоваться безопасными системами управления паролями, такими как LastPass, 1Password и KeePassX. Вам нужно будет запомнить только один пароль вместо нескольких. И все же, когда вы работаете с важными сервисами (к примеру, вашей электронной почтой), не полагайтесь на диспетчеры паролей, а просто хорошенько запомните пароль.
В интервью Аластейру Райду для издания journalism.co.uk Арьен Кампхёйс, эксперт по информационной безопасности, посоветовал для шифрования жестких дисков, защиты электронных писем и блокировки ноутбуков подбирать пароль, состоящий из более чем 20 символов. Чем длиннее пароль, тем сложнее его взломать… и запомнить. Поэтому эксперт рекомендует использование для этих целей кодовых фраз. «Это может быть что угодно, например, строка из вашего любимого стихотворения, – говорит Кампхёйс, – или строка, написанная вами в девятилетнем возрасте, о которой никто не знает».

Райд выразил эту мысль наглядно, прибегнув к подсчетам с помощью вычислителя надежности пароля компании Gibson Research Corporation: пароль типа «F53r2GZIYT97uWB0DDQGZn3j2e», сгенерированный случайным образом, кажется очень надежным, и не зря, поскольку понадобится 1,29 сотен миллиардов триллионов столетий, чтобы перебрать все возможные комбинации, даже учитывая, что вычислительная техника проверяет сто триллионов комбинаций в секунду.

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

F53r2GZlYT97uWB0DDQGZn3j2e

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

Пароль из 26 символов...

Как подчеркивает автор, фразу «Как тучи одинокой тень, бродил я, сумрачен и тих…»[1] намного проще запомнить, и она также гораздо надежнее, поскольку та же вычислительная техника будет перебирать все комбинации 1,24 сотен триллионов столетий. Что ж, преимущество кодовых фраз неоспоримо.

1 *Прим. пер.: строчка из стихотворения Уильяма Вордсворта «Нарциссы» в переводе А. Ибрагимова*

GRC's Interactive Brute Force Password "Search Space" Calculator

*(**NOTHING** you do here ever leaves your browser. What happens here, stays here.)*

12 Uppercase | 6 Lowercase | 8 Digits | No Symbols | 26 Characters

i wandered lonely as a cloud

Enter and edit your test passwords in the field above while viewing the analysis below.

Brute Force Search Space Analysis:

Search Space Depth (Alphabet):	26+26+10 = **62**
Search Space Length (Characters):	26 characters
Exact Search Space Size (Count): (count of all possible passwords with this alphabet size and up to this password's length)	40,667,341,382, 973,472,945,117,556,132, 496,178,582,698,289,386
Search Space Size (as a power of 10):	4.07×10^{46}

Time Required to Exhaustively Search this Password's Space:

Online Attack Scenario: (Assuming one thousand guesses per second)	12.93 billion trillion trillion centuries
Offline Fast Attack Scenario: (Assuming one hundred billion guesses per second)	1.29 hundred trillion trillion centuries
Massive Cracking Array Scenario: (Assuming one hundred trillion guesses per second)	1.29 hundred billion trillion centuries

Note that typical attacks will be online password guessing limited to, at most, a few hundred guesses per second.

...намного слабее чем ключевая фраза (скриншоты с сайта GRC.com)

9. Двухфакторная аутентификация. Это тоже неплохая идея. Используя обычную двухступенчатую аутентификацию, вы входите в систему при помощи своего пароля и получаете второй код подтверждения, обычно в текстовом сообщении, на свой смартфон. Вы можете использовать ключи Yubikey или аппаратный ключ безопасности, чтобы обеспечить еще более надежную защиту конфиденциальных файлов на своем компьютере. Чтобы узнать больше, прочитайте 7 золотых правил защиты с помощью паролей.

10. Пусть у вас будет отдельный компьютер, на котором вы будете проверять подозрительные файлы и вложения. Самый простой способ распространять вредоносное и шпионское ПО – устанавливать его через USB-устройства или вложения и ссылки в электронных письмах. Поэтому рекомендуется использовать какой-то один физически защищенный компьютер, чтобы просматривать подобные

потенциально опасные файлы в режиме карантина. С таким компьютером вы свободно сможете пользоваться USB-устройствами и загружать файлы из Интернет, но не передавайте эти файлы на ваш рабочий компьютер и не используйте на нем эти USB-накопители/устройства.

11. Как приобрести защищенный компьютер. Эксперт по безопасности Арьен Кампхёйс советует купить IBM ThinkPad X60 или X61, выпущенный до 2009 года. Это единственные более-менее современные модели ноутбуков с достаточно современным ПО, где можно заменять низкоуровневые программы. Другой совет, который стоит принять во внимание – не покупайте компьютер через Интернет, поскольку его могут перехватить во время доставки.

ThinkPad X60. Не покупайте эту модель в интернет-магазинах

Кампхёйс советует покупать ноутбук в магазине подержанных товаров за наличные. Он также настаивает на том, что нужно убрать из ноутбука все средства связи с другими устройствами: Ethernet, модем, модули Wi-Fi и Bluetooth. Лично я знаю экспертов по безопасности, которые и таким компьютерам не доверяют.

12. Проведите ликбез источникам. Всегда есть вероятность того, что к тому времени, как вы получите эксклюзивную и ценную информацию, будет уже слишком поздно. Ваш источник мог сделать какую угодно ошибку и оставить за собой хвост улик. Вы должны не только защитить имеющиеся у вас на руках данные, но и приложить все усилия, чтобы научить источники прятать их: безопасно хранить информацию, безопасно общаться при помощи защищенных устройств. Большинство людей вообще не имеют ни малейшего представления о том, как обращаться с конфиденциальной информацией. Пытаясь связаться с вами, мало кто из источников будет иметь четкое представление о том, с чем они вообще столкнулись.

13. Пользуйтесь защищенной выделенной системой для передачи документов. Замените Dropbox или Google Drive на что-то менее популярное и более безопасное. Например, SecureDrop – это выделенная система, в которой вы можете получать сообщения от анонимных источников, а также

безопасно просматривать и сканировать эти файлы. Эдвард Сноуден отзывался о Dropbox как о «враге конфиденциальности» и советовал вместо этого сервиса использовать Spideroak. OnionShare - еще один бесплатный сервис, где можно просто и анонимно передавать файлы.

Насколько безопасны облачные хранилища данных?

Большинство крупных провайдеров облачных хранилищ (Amazon, Dropbox, Apple, Google и Microsoft) сотрудничали с АНБ в тот или иной период в прошлом. Большинство из них сохраняют за собой право исследовать все загруженные файлы и будут обязаны передать эти файлы властям при наличии соответствующего постановления суда.

Вот как вы можете решить эту проблему:

1. Постарайтесь загружать в облачные хранилища как можно меньше файлов и всегда шифруйте их надежным способом. Самый надежный и простой метод – шифровать файлы вручную, тогда вы сможете пользоваться любыми облачными сервисами. При этом не забывайте, что вместе с зашифрованными файлами нельзя загружать в хранилище ключи шифрования.

2. Пользуйтесь облачными хранилищами, которые автоматически шифруют файлы перед загрузкой и полностью синхронизируются с клиентом. У провайдера могут быть ключи дешифровки, но риск утечки данных намного меньше, чем при работе с другими провайдерами. У SpiderOak, который я уже упоминал ранее, есть приложения для Android и iOS.

3. Безоблачная синхронизация BitTorrent Sync – это не совсем облачная служба, ее нельзя использовать для долговременного хранения данных; тем не менее, сервис BitTorrent Sync бесплатный и разработан так, чтобы стать заменой Dropbox. Все, что вам нужно, – выбрать файлы, затем вы получите пароль и сможете связать нужную папку с папкой на другом устройстве (конечно, для этого на нем тоже должно быть установлено приложение BitTorrent Sync).

14. Никаких заметок! Не фиксируйте имена источников, их инициалы, номера телефонов, адреса электронной почты и имена пользователей в мессенджерах ни на ноутбуке, ни в календарях, ни в списке контактов своего мобильного телефона, и уж тем более – в компьютере или облачном хранилище. Просто никогда так не делайте.

КОММУНИКАЦИЯ С ИСТОЧНИКОМ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

15. Визуальное слежение. По пути на конфиденциальные встречи не пользуйтесь общественным транспортом, своему источнику посоветуйте сделать так же. Не встречайтесь, к примеру, в современных торгово-развлекательных центрах, где за вами повсюду следят камеры.

16. Как не попасть в социальные сети? Некоторые люди предпочитают подходить к вопросу анонимности радикально. Если по какой-то причине вам нужно исчезнуть с лица земли, не оставив при этом в каждой из возможных социальных сетей чересчур подробный профиль, полностью и безвозвратно удалите свои учетные записи. Это не то же самое, что «деактивировать» их, потому что в этом случае вся информация сохраняется, а сам профиль можно заново активировать.

17. Заведите несколько друзей-хакеров. Это поможет вам не совершить фатальных ошибок, сбережет ваше время и нервы, а еще вы всегда будете в курсе новинок технологической гонки вооружений.

18. Способы оплаты. Всегда и везде платите наличными; подумайте, а не перейти ли вам на биткойны? Их нужно покупать анонимно (для этого воспользуйтесь вот этим руководством на Business Insider), и если кто-то готов будет принять их, воспользуйтесь платежной системой Darkcoin. Предоплаченная банковская карта, полученная через онлайн-магазин, тоже вполне себе вариант.

19. Делая пометки на бумаге, будьте благоразумны. Если вы набросали какую-то информацию на клочке бумаги (в доисторическую эпоху наши предки называли это «заметка»), уничтожьте ее. И не забудьте про тот бумажный замятыш на самом дне своего кармана. Да, тот, который к жвачке прилип.

03

КАК СОХРАНИТЬ АНОНИМНОСТЬ В ИНТЕРНЕТ?

Помимо того, что вы обезопасите общение со своим источником и закроете уязвимости, чтобы не допустить кражи конфиденциальной информации, которой владеете, вы также должны быть начеку, чтобы вас не отследили во время работы с веб-сайтами. История запросов может раскрыть или дать намеки на тему, над которой вы работаете, или, что еще хуже, намекнуть на личность вашего источника, а то и полностью ее раскрыть. Вот золотые правила безопасной работы в Интернет, а в следующей главе я расскажу, как защитить свою учетную запись электронной почты:

1. Работа в Интернет в режиме инкогнито. Есть два основных способа сохранить анонимность, пока вы работаете в сети. Первый, самый простой и популярный, но все же недостаточно надежный – работать в режиме инкогнито, который есть в большинстве интернет-браузеров. В этом случае история ваших запросов не сохраняется, а основные технологии отслеживания, которыми пользуются рекламщики, такие как отслеживание файлов cookie (маркеров HTTP), будут блокироваться, не давая составить детальный отчет о вашей деятельности. Тем не менее, это больше похоже на подарок от заведения, чем на реальную анонимность: фактически, такой режим может скрыть вашу историю запросов от членов семьи, у которых есть доступ к вашему компьютеру, а вот ваш IP-адрес все еще можно отслеживать, и информация о сайтах, которые вы посетили, все еще доступна вашему провайдеру.

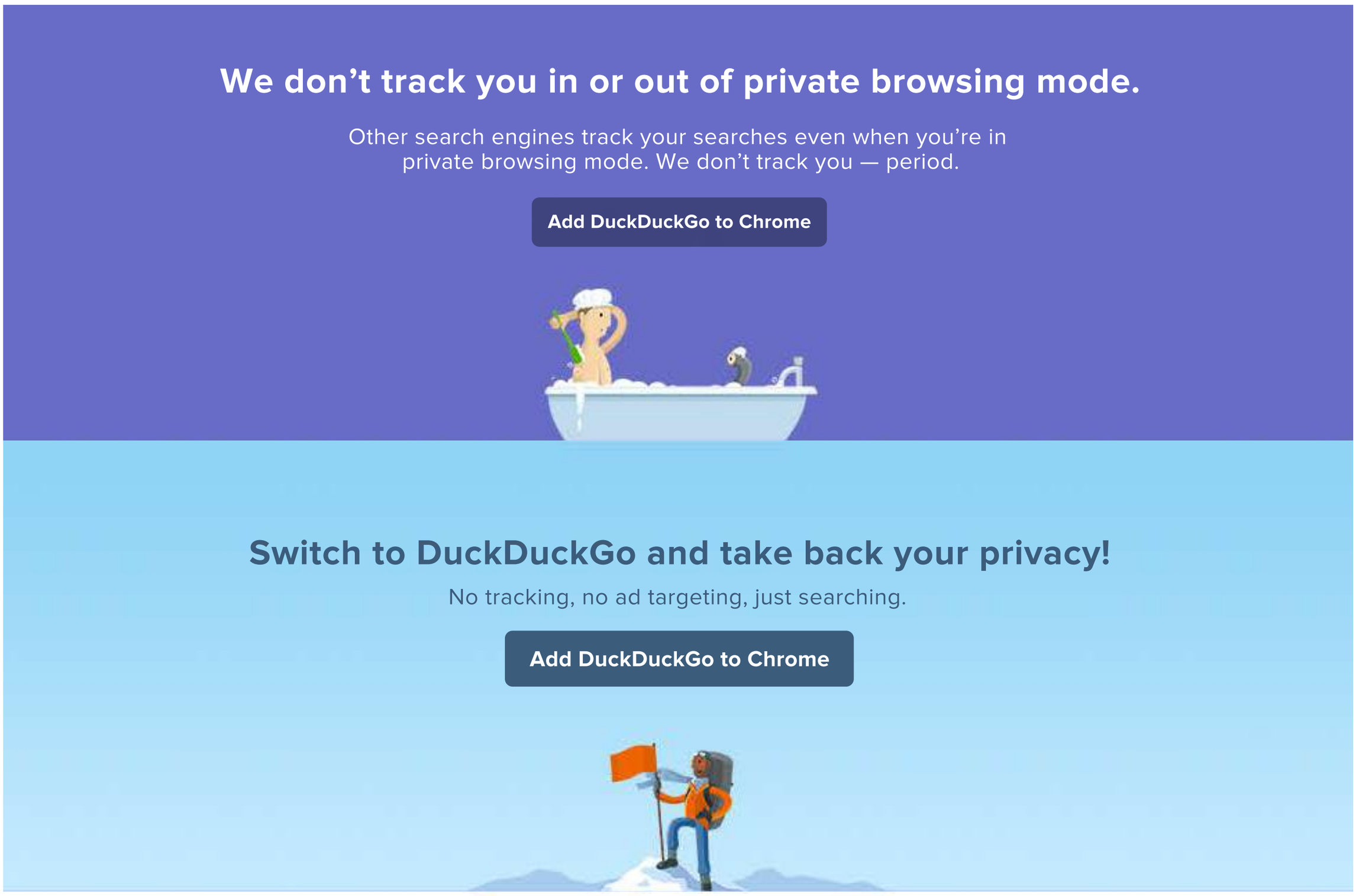
2. Пользуйтесь альтернативными интернет-браузерами. Такие браузеры, как Dooble, Comodo Dragon или SRWare Iron обеспечивают анонимность пользователю, но функционально ограничены. Вы сможете в какой-то степени обеспечить себе анонимность при работе с этими браузерами, просто удаляя cookie-файлы – фрагменты кода, которые при посещении сайтов загружаются в вашу систему, а затем отслеживают вашу активность и иногда даже тип потребляемого вами контента! Другой способ сохранить анонимность – отключить настройки отслеживания местоположения в браузере, а также активировать различные функции, нацеленные на обеспечение анонимности. Чтобы проверить, отключили ли вы cookie, можно воспользоваться приложением CCleaner, которое также работает с Flash-cookie, но ни один из этих браузеров не зашифрован полностью. Единственный браузер, обеспечивающий полную анонимность – это Tor. Да, он уродлив и медлителен. Зато так вы защитите себя и свои источники. В следующем разделе я подробно опишу этот браузер.

3. TOR. Этот «печально известный» браузер, разработанный ВМС США, дает вам возможность работать в скрытой сети, общаться в частном порядке и посещать веб-сайты анонимно. Браузер можно загрузить на Torproject.org; в нем очень трудно будет отслеживать вашу активность в Интернет, а правительству или вашему провайдеру придется попотеть, чтобы определить ваше местоположение. Единственный недостаток – временами браузер очень медленный, довольно громоздкий, но это все происходит лишь по той причине, что Tor прокладывает соединение через три случайно выбранных по

сети, прежде чем дать вам доступ к нужному сайту. Также держите в уме, что даже ваш сосед может оказаться сомнительной личностью.

В дополнение к Tor можно загрузить Whonix – безопасную операционную систему, приоритетной задачей которой является анонимность пользователя. Такая система служит своеобразным пропускным пунктом для Tor и разрешает соединения только через Tor с сайтами и пользователями. Впрочем, наиболее популярная ОС для Tor – это Tails (The Amnesiac Incognito Live System). ОС Tails можно загрузить через USB-накопитель или DVD-диск. Эта ОС делает анонимными все данные. Говорят, Эдвард Сноуден – фанат этого программного обеспечения. ОС Qubes совместима с Whonix, ее советует Сноуден.

4. Альтернативные поисковые системы. Самая популярная поисковая система (Google) сохраняет историю ваших запросов, чтобы скорректировать выдачу результатов. Чтобы отключить эту функцию персонализации, нужно щелкнуть на: Инструменты > Все результаты > Точное соответствие (под строкой поиска). Либо войдите в свой аккаунт Google на странице www.google.com/history, найдите список своих предыдущих запросов и удалите то, что вы хотите удалить, нажав кнопку «Удалить».



DuckDuckGo. Поисковая машина, которая не хранит ваши данные

Чтобы быть полностью уверенным в том, что за вами не следят, лучше пользоваться поисковой системой типа DuckDuckGo. Если вам трудно отказаться от Google, загрузите Searchlinkfix, чтобы хотя бы не волноваться об URL-трекерах.

5. Прямая обработка кратковременной памяти компьютера. Избавиться от слежения за вашей активностью в сети можно и с помощью удаления кеша DNS (системы доменных имен). Это можно сделать при помощи простых команд в операционной системе. Во время перезагрузки роутера, в котором иногда тоже есть DNS-кеш, или перезагрузки компьютера также перезагружается и DNS-кеш устройств (если в роутере он изначально есть).

6. Избегайте веб-хранилищ HTML. Функция веб-хранилища встроена в HTML5, и, в отличие от cookie-файлов, сохраненную в нем информацию невозможно отследить или выборочно удалить. Веб-хранилище функционирует по умолчанию, поэтому, если вы пользуетесь браузерами Internet Explorer или Firefox, просто отключите его. Можно также воспользоваться расширением Better Privacy для Firefox, чтобы сохраненная информация удалялась автоматически. То же самое сделает расширение Click and Clean в Google Chrome.

7. Работайте с VPN. Как я уже упоминал выше, ваш провайдер может отслеживать сайты, которые вы посещаете, и всякий, кто захочет подглядеть за вами, также может перехватить вашу переписку. Чтобы защитить все входящие и исходящие данные, важно научиться работать с VPN-сервисами (подробная инструкция находится здесь). Виртуальные частные сети шифруют все ваши данные так, что даже ваш провайдер, спецслужбы или просто хакеры, вьющиеся вокруг точки доступа Wi-Fi вашей любимой кофейни, не смогут узнать, кому вы отправили электронное письмо, каким сервисом для этого воспользовались и так далее.

VPN-сервисами зачастую пользуются люди, которые, например, хотят посмотреть полный каталог фильмов канала Netflix, но при этом находятся за пределами США; но будьте внимательны: не все VPN подходят журналистам. Сеть VPN для журналиста не обязательно должна быть самой быстрой и иметь самую лучшую поддержку, но она обязательна должна придерживаться «безлоговой» политики, только тогда нельзя будет определить, кто вы, какие сайты вы посещаете и т.д.

Безопасная сеть VPN должна принадлежать компании, которая не находится в одной из стран списка "14 Eyes", ведь там разведывательным структурам разрешено собирать и делиться друг с другом информацией, в первую очередь и в особенности такая практика есть в США. Вот почему обслуживающие VPN компании, которые находятся в странах бывшего СССР, наиболее предпочтительны. В судах этих стран не так-то просто получить постановление о выдачи информации, собранной местными компаниями, причем это касается как граждан самой страны, так и иностранных граждан. Вот список из 5 VPN-сервисов, которые больше всего заботятся о сохранении анонимности пользователей, и находятся за пределами стран из списка "14 Eyes".

Кстати, даже если правительства активно охотятся за потоком данных, передаваемых внутри VPN, можно стать пользователем скрытых VPN-сетей, таких как TorGuard, чтобы бороться с подобным вмешательством, будь то цензура или просто слежка за вами. Tor и VPN-сети станут вашей надежной защитой, когда кто-то попытается заполучить историю ваших запросов, чтобы разузнать о вас побольше.

Несколько советов от Эдварда Сноудена

По материалам интервью для Intercept, автор Мика Ли

1. Шифруйте телефонные звонки и текстовые сообщения. Это можно сделать при помощи простого в работе приложения Signal.
2. Шифруйте жесткие диски, чтобы в случае кражи компьютера посторонние не могли извлечь из него информацию.
3. Используйте диспетчер паролей. Одна из основных причин, по которой раскрывается личная информация, – потеря данных. Ваши реквизиты могут «всплыть» из-за того, что сервис, которым вы перестали пользоваться еще в 2007, взломали, а пароль оттуда до сих пор подходит для вашего Gmail-аккаунта. Диспетчер паролей создает уникальные пароли для каждого сайта, которые невозможно взломать, и при этом вам не нужно их запоминать.
4. Пользуйтесь двухфакторной аутентификацией, чтобы ваш провайдер мог выслать вам другие средства аутентификации, если кто-то украдет ваш пароль.
5. На каждом этапе работы вы должны задумываться: «Что бы случилось, если бы мои недоброжелатели узнали о моих действиях?» Если вам не нравится ответ, смените направление деятельности или вовсе от нее откажитесь, а еще попробуйте смягчить последствия, прибегнув к каким-либо инструментам или средствам для защиты информации и снижения риска ее утечки. В крайнем же случае просто смиритесь с рисками или возможностью разоблачения и продумайте план ответных действий. Вы не можете держать что-то в секрете вечно, но вы точно можете продумать, как справиться с последствиями разоблачения.
6. Фильтруйте информацию, которой намерены с кем-то поделиться: не разбрасывайте свои личные данные повсюду.
7. Пользуйтесь блокировщиками рекламы. Провайдеры услуг предоставляют их вместе с рекламой в виде активного контента, который может стать тем слабым местом, через которое веб-браузер подвергнется атаке. Так что не сидите, сложа руки, и активно блокируйте подобные угрозы.
8. Напоследок – краткая инструкция для информаторов:
   а) Не говорите тем, кому не обязательно это знать, о неправомерных действиях, которые вы собираетесь предать огласке.

b) Пользуйтесь чем-то типа SecureDrop, передавайте данные по сети Tor. Люди, живущие при репрессивном режиме, всегда должны пользоваться сетью Tor.

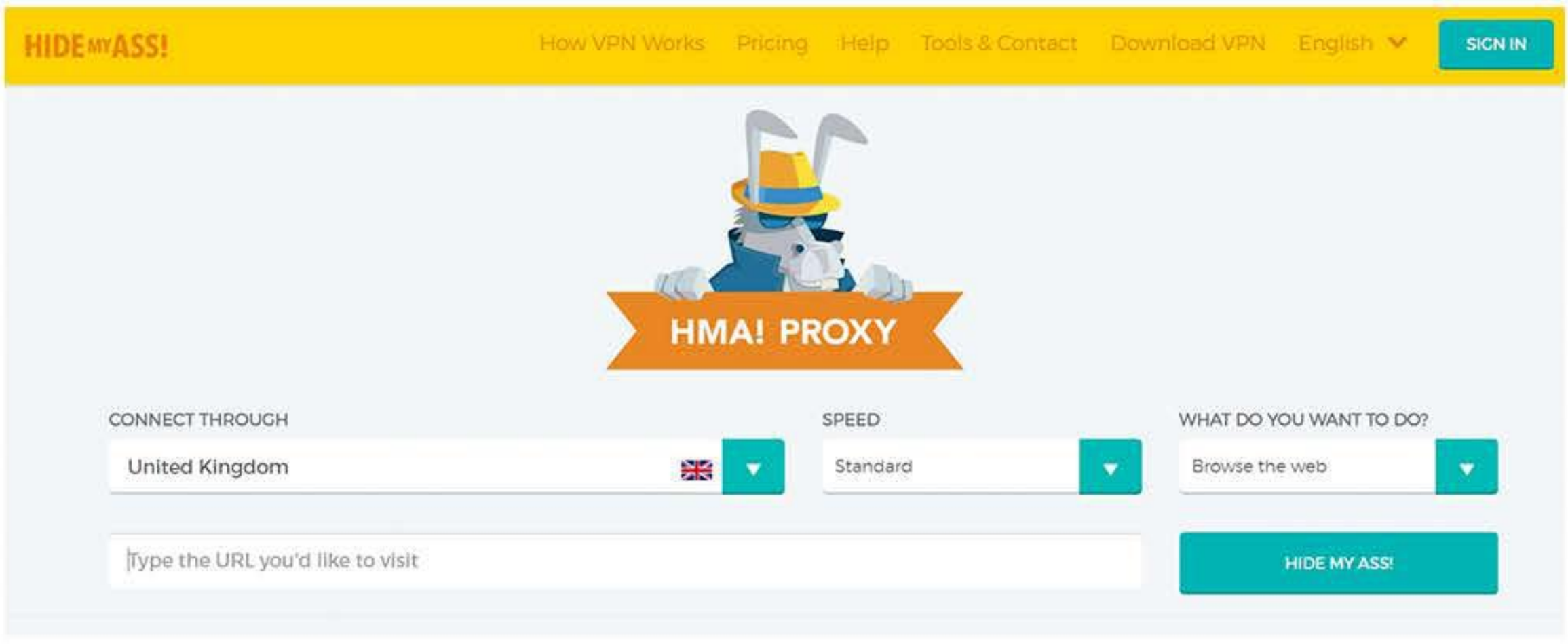
c) Пользуйтесь временными ОС типа Tails.

d) Пользуйтесь одноразовыми устройствами, от которых можно избавиться.

e) Иными словами – не оставляйте следов. Единственным последствием вашей оперативной работы должны быть статьи, опубликованные журналистами.

8. Устраняйте DNS-утечки. То, что вы пользуетесь VPN, еще не значит, что вы полностью защищены, поскольку DNS-трафик может дать представление о том, кто вы. Пройдя тестирование на DNSLeakTest.com, вы сможете обнаружить такие утечки. Если тест покажет, что DNS принадлежит вашей VPN, можете расслабиться. Если же окажется, что DNS принадлежит вашему провайдеру, вы работаете не анонимно. Почитайте здесь, что можно сделать в этом случае.

9. Виртуальные вычислительные машины. Весьма полезный и хитрый трюк! Фактически, это второй (но виртуальный) компьютер, который функционирует как приложение в вашей операционной системе. Вы можете загружать файлы и переходить по ссылкам так же, как и при работе с изолированным компьютером, о котором я писал ранее, поэтому ваш компьютер будет меньше подвергаться вредоносному и шпионскому ПО разного рода. ПО для виртуализации типа VirtualBox нужно открывать на защищенной операционной системе. После загрузки файла интернет-соединение с виртуальной машиной прерывается; когда вы закончите работу с файлом, нужно его удалить. В зависимости от того, каким людям/организациям вы противостоите, может потребоваться удалить и виртуальную машину.



Прокси-сервер HideMyAss. Я спрячу твой прокси, если ты спрячешь мой.

10. Прокси-сервер. Как и в случае с виртуальной машиной, здесь вся деятельность также переносится в другое «место», что позволяет вам не бояться слежки и других атак. Фактически, прокси-серверы подменяют ваш IP-адрес своим, и это может пустить по ложному следу недоброжелателей, например, заставив их думать, что вы находитесь в другой стране. HideMyAss.com/proxy, Psiphon (с открытым кодом) и JonDonym предоставляют схожие услуги. Некоторые эксперты считают, что эти сервисы следует использовать вместе с VPN и/или Tor, чтобы надежнее защитить себя. В то же время, другие эксперты, с которыми я разговаривал, заявляют, что при работе в сети Tor вы в любом случае защищены настолько, насколько это возможно.

11. Три дополнительных типа расширений, которые могут повысить вашу безопасность. Чтобы проверить, является ли интернет-протокол, которым вы пользуетесь, защищенным протоколом https, можно установить расширение HTTPS Everywhere, разработанное некоммерческой организацией Electronic Frontier Foundation (Фонд электронных рубежей), которая в числе прочих финансирует проект Tor Project. Это расширение советуют многие эксперты по информационной безопасности. С ним вы будете уверены, что веб-сайты, которые вы посещаете, используют надежный протокол, что, конечно же, не гарантирует защиту от всего на свете, но уже намного надежнее, чем незащищенный протокол.

Второй тип расширений фильтрует данные, которые посредством JavaScript передаются веб-сайтам (чтобы оптимизировать вашу работу в сети, ага). Два самых известных расширения такого типа – это ScriptSafe и NoScript.

Третий вариант – браузерное расширение Ghostery. Это расширение покажет, какие из 2000 компаний отслеживают вашу активность, и даст вам заблокировать нежелательных наблюдателей из этого списка. Опция приятная, но вы, скорее всего, не сможете заблокировать АНБ таким образом. Проект Privacy badger, разработанный EFF, работает схожим образом.

Антивредоносное ПО, антивирусы и файрволы

Антивредоносное ПО. В сети Интернет есть несчетное количество вредоносного кода, известного как вредоносное ПО. Bitdefender установлен на всех версиях ОС Windows новее Vista. Есть также приложения Malwarebytes и Spybot Search and Destroy, которыми можно пользоваться бесплатно.

Антивирусы. Первым делом после покупки нового компьютера или полной переустановки операционной системы следует устанавливать именно эти программы. Вирусы могут не только безнадежно испортить компьютер, но и способствовать краже данных, которые в нем обрабатываются. Большинство людей действительно устанавливают антивирусы на свои компьютеры, но не на смартфоны. Телефоны под управлением систем с открытыми исходным кодом, например, на базе Android, более уязвимы перед вирусами, чем телефоны на системе с закрытым кодом типа iOS (Apple).

Файрволы. Файрвол закрывает доступ к вашему компьютеру стороннему программному обеспечению. Недостаток такой защиты в том, что файрвол плохо определяет, какие программы безопасные, а какие – нет.

04

КАК ЗАЩИТИТЬ СВОЮ ЭЛЕКТРОННУЮ ПОЧТУ?

Как нам лучше защитить свою электронную почту? Проблема конфиденциальности электронных писем стоит еще более остро: компании Google и Microsoft скорее всего просто выдадут ваши личные письма госорганам, если их попросят об этом. Что же с этим делать?

1. Безопасные расширения. Самое простое решение для тех, кто пользуется популярными электронными почтовыми службами типа Yahoo и Google заключается в том, чтобы установить плагин Mailvelope. При этом следует убедиться, что человек на «другом конце провода» тоже это сделал. Это расширение просто шифрует и расшифровывает электронные письма. Похожее, но менее функциональное расширение для Gmail, SecureGmail, работает аналогичным образом. Проходящие через плагин письма шифруются, и Google не может их расшифровать. Также можно воспользоваться простым расширением для Firefox - Encrypted Communication. Здесь вам понадобится придумать пароль, который будет знать получатель, но помните, что нельзя передавать пароли по электронной почте!

2. Безопасные почтовые домены. Hushmail – пример почтового сервиса, в котором уровень безопасности выше, чем у большинства популярных сетей, которыми вы пользуетесь. Тем не менее, по решению суда правительство США также может обязать этот сервис передать личные письма пользователей, а ведь еще там хранятся записи об IP-адресах! Другой почтовый сервис со схожими функциями и уровнем безопасности – это Kolab Now, который среди прочих своих преимуществ выделяется тем, что все данные хранятся исключительно в Швейцарии.

3. Одноразовые адреса электронной почты. Речь идет об электронном ящике, который создается специально для конкретной цели, он полностью анонимный и удаляется сразу же после использования. Такое решение широко применяется, когда люди регистрируются на различных сервисах и не хотят получать спам на почту, также это отлично помогает сохранить анонимность. Однако я бы не советовал журналистам общаться с источниками таким образом, поскольку безопасность при этом не на высоте. Есть десятки подобных почтовых сервисов, но британская газета The Guardian, к примеру, рекомендует пользоваться только Guerrilla Mail и Mailinator.
Если вы будете пользоваться сервисом Guerrilla Mail в браузере Tor, это гарантирует, что даже сам сервис не сможет связать ваш IP-адрес и адреса электронной почты. Таким же образом, если вы пользуетесь специальной программой для шифровки электронных писем типа GnuPG, а также браузером Tor, вы в безопасности. Так что давайте немного поговорим о шифровании электронных писем.

4. Как зашифровать свою почту? Журнал Wired опубликовал рекомендации от Мики Ли, технического специалиста по конфиденциальности, который работал с организациями EFF и First Look Media

(вот его интервью с Эдвардом Сноуденом): шифрование сообщений электронной почты может быть довольно трудным делом. Зачастую пользователю нужно копировать свое сообщение и вставлять его в текстовое окно, а уж потом использовать PGP, чтобы зашифровать или расшифровать его (PGP – «Pretty Good Privacy» - программа шифрования, с помощью которой данные можно зашифровать и распознать). Вот почему Ли предлагает другой способ защиты электронных писем – сервис для работы с электронной почтой, где в приоритете конфиденциальность пользователей, например, Riseup.net, почтовое приложение Mozilla Thunderbird, плагин шифрования Enigmail и еще один плагин TorBirdy, который направляет сообщения через Tor.

В интервью с Капхёйсом для journalism.co.uk Райд пишет, что Гринвальд чуть не потерял свою историю об АНБ, потому что изначально проигнорировал все инструкции Сноудена о шифровании электронных писем. Другими словами, если вы хотите написать материал, который останется в веках, разумно соблюдать правила безопасности. Кампхёйс согласен с тем, что программе PGP можно доверять. Он вместе с Райдом объясняет это так: начав работу с программой PGP, вы получите общедоступный ключ (как номер вашего телефона, который известен всем), а также секретный ключ. Общедоступный ключ можно выложить в профиле Twitter, напечатать на визитках, указывать на веб-сайтах и вообще везде, где публикуются ваши работы, а вот личный ключ необходимо хранить в безопасности, как и другую конфиденциальную информацию. Затем, когда источник захочет поделиться с вами информацией, он воспользуется вашим общедоступным ключом, чтобы зашифровать свое сообщение, а расшифровать его можно будет только при помощи вашего личного ключа безопасности.

Кампхёйс также посоветовал в этой связи версию PGP с открытым кодом – GNU Privacy Guard. Эта программа проста в установке, плюс у нее активное сообщество поддержки. Чтобы узнать больше о шифровании файлов, данных и жестких дисков, почитайте его бесплатную электронную книгу, опубликованную совместно с Силки Карло и выпущенную Центром расследовательской журналистики (CIJ); в ней подробно описан весь процесс.

Если же вы захотите просто зашифровать сообщение без оглядки на почтовую службу, хорошей идеей будет создать zip-архив, защищенный паролем, а в этом вам поможет программа 7ZIP.

5. Еще раз о прописных истинах. Да, я знаю, этот пункт снова касается безопасности «для начинающих», но постарайтесь не попадаться на удочку фишинга. Смотрите, чтобы в поле «От» входящего письма имя отправителя было написано абсолютно точно (без опечаток, неточностей и т.д.), поскольку кто-то может захотеть притвориться знакомым вам человеком.

И последние несколько строк о шифровании электронных писем. Одна из действительно серьезных проблем, о которых нужно помнить, состоит в том, что даже после того, как вы зашифровали письмо, не все данные зашифрованы. Адреса электронной почты отправителя и получателя, тема письма, а также время и дата отправки письма, - все это остается видимым. Шифруются только само сообщение и приложения к письму.

Пример из практики: дело Розена

Дело Джеймса Розена стоит того, чтобы специально о нем упомянуть. И не только потому, что ФБР убедило суд сделать подозреваемым в деле о шпионаже не просто рядового журналиста, а руководителя вашингтонского бюро телеканала Fox News, назвав его соучастником преступления только за то, что он выполнял свою работу журналиста, сотрудничающего с источником из правящих кругов. Это дело стоит отметить в основном из-за того, что оно открывает все недостатки методов работы журналистов и еще раз поднимает вопрос о том, достаточно ли делают репортеры и организации СМИ для защиты своих источников. Как сообщил журналист Guardian Гленн Гринвальд, ФБР отслеживало передвижения Розена, время входа и выхода в здание Госдепартамент США и частоту его телефонных звонков. ФБР даже заполучило ордер на то, чтобы прочитать его электронные письма, в том числе и переписку с источником – Стивеном Цзинь-У Кимом. Тони Лоци в статье «Наблюдение и безопасность» пишет, что «Розен и Ким разговаривали по стационарным и мобильным телефонам в здании Госдепартамента США: репортер воспользовался телефоном в комнате пресс-центра, а Ким – телефоном в своем офисе. Во время телефонного разговора с Розеном Ким резюмировал документ о Северной Корее, просматривая его на компьютере с ограниченным доступом. Розен создал незащищенный аккаунт электронной почты, чтобы общаться с Кимом».

«В письменном показании от ФБР говорится, что они отследили телефонные номера, сверили время звонков со временем посещения аккаунтов на компьютере Кима, расшифровали псевдонимы, которые использовались в качестве кода в переписке, а затем отследили электронные пропуски в Госдепартаменте США, при помощи которых Розен и Ким входили и выходили из здания примерно в одно и то же время».

Насколько пугающей бы ни казалась сейчас администрация Трампа, напомню вам еще раз о том шокирующем факте, что при президенте Обаме Министерство юстиции завело дел по Закону о шпионаже от 1917 года больше, чем все предыдущие администрации вместе взятые, фактически удвоив число всех предыдущих подобных дел. Это правда, что Ким, натурализованный гражданин из Северной Кореи, в 2009 был обвинен в предположительной передаче Розену информации о том, что спецслужбы США полагают, что Северная Корея в ответ на дополнительные санкции ООН будет проводить больше ядерных испытаний. Тем не менее, как хорошо выразился обозреватель Fox News, судья Эндрю Наполитано: «Это первый раз, когда федеральное правительство прилагает столько усилий, чтобы представить рутинные, вполне разумные и законные действия репортера как противозаконные».

Гринвальд приходит к такому же заключению в статье для The Guardian: «...Министерство юстиции особо настаивало на том, что, побуждая свой источник раскрыть засекреченную информацию – действия, которые любой журналист, занимающийся расследованиями, совершает чуть ли не каждый день, – Розен нарушал закон”. Гринвальд называет это «криминализацией расследовательской журналистики как таковой» и указывает на то, что фактически все это началось еще в 2011, когда New York Times сообщила, что «Минюст при Обаме руководствуется такой же «подстрекательной» теорией, чтобы оправдать свое текущее криминальное расследование в отношении WikiLeaks и Джулиана Ассанжа. Все потому, что Ассанж настойчиво попросил или воодушевил Мэннинг на то, чтобы обнародовать секретную информацию, и таким образом правительство США может предъявить обвинения Ассанжу не только как пассивному получателю документов, который потом их опубликовал, но и как соучастнику утечки».

05 ЗАКЛЮЧЕНИЕ

Здесь я расскажу о самых радикальных советах, на которые я натолкнулся, когда писал эту электронную книгу.

Как сказал Мика Ли в своем интервью на тему конфиденциальности для WIRED: «Если ваш компьютер взломают – игра окончена. Создание виртуальной песочницы для серверов, посредством которых вы общаетесь, - хороший способ защитить оставшуюся часть системы. Tor – действительно выдающаяся сеть, которая скроет вашу личность в сети, но если ваш собеседник скомпрометирует себя, ваша анонимность тоже окажется под угрозой. Если вам действительно необходимо сохранить анонимность, вы должны постараться, чтобы защитить себя».

Журналист Тони Лоци описывает эту проблему еще более резкими словами в статье для гарвардского ресурса Nieman Foundation, опубликованной в электронной книге, посвященной будущему международной расследовательской журналистики: «Некоторые журналисты, специалисты в области вычислительной техники и адвокаты, специализирующиеся на защите личной информации, настолько взбудоражены, что советуют репортерам придерживаться методик старой школы… и полагаться на интервью в частном порядке и черепашью традиционную почту».

Я надеюсь, что моя работа помогла людям определенных профессиональных кругов и другим получить некоторое представление о том, что нужно и можно сделать, чтобы обезопасить себя и источники в это неспокойное время.

06

СПИСОК ИСТОЧНИКОВ НАСТОЯЩЕГО ЭЛЕКТРОННОГО ПОСОБИЯ

Безопасность для журналистов: как защитить свою информацию и свои источники (Security for journalists: How to keep your sources and your information safe).
http://www.ire.org/blog/car-conference-blog/2016/03/12/security-journalists-how-keep-your-sources-and-you/

Как защитить свои данные, свои источники и себя (Securing data, sources and yourself).
http://www.ire.org/blog/car-conference-blog/2017/03/05/securing-data-sources-and-yourself/

Наблюдение и безопасность: достаточно ли делают репортеры и новостные организации, чтобы защитить свои источники? (Surveillance and Security: Are reporters and news organizations doing enough to protect sources?).
http://niemanreports.org/articles/surveillance-and-security/

Разоблачения стали мировым трендом: будущее международной расследовательской журналистики (Muckraking Goes Global: The Future of Cross-Border Investigative Journalism).
http://niemanreports.org/books/muckraking-goes-global-the-future-of-cross-border-investigative-journalism/

Совершенное руководство о том, как сохранить конфиденциальность в сети (The Ultimate Guide for Online Privacy).
https://www.vpnmentor.com/blog/ultimate-guide-online-privacy/

Что такое DNS-кеш? (What Is a DNS Cache?)
https://www.lifewire.com/what-is-a-dns-cache-817514

Как оставаться анонимным, чем бы вы ни занимались в сети (How to Anonymize Everything You Do Online).
https://www.wired.com/2014/06/be-anonymous-online/

19 способов сохранить анонимность и защитить свою конфиденциальную информацию в сети (19 ways to stay anonymous and protect your online privacy).
https://www.extremetech.com/internet/180485-the-ultimate-guide-to-staying-anonymous-and-protecting-your-privacy-online

Эдвард Сноуден о том, как отстоять свое право на конфиденциальность (Edward Snowden explains how to reclaim your privacy).
https://theintercept.com/2015/11/12/edward-snowden-explains-how-to-reclaim-your-privacy/

СПИСОК ИСТОЧНИКОВ НАСТОЯЩЕГО ЭЛЕКТРОННОГО ПОСОБИЯ

Информационная безопасность для журналистов: как защитить себя в сети? (Information security for journalists: staying secure online).
https://www.journalism.co.uk/news/information-security-for-journalists-/s2/a562525/

АНБ отслеживает тех, кто пытается сохранить личные данные в тайне (NSA targets the privacy-conscious).
http://files.gendo.nl/presentaties/CIJ_Infosec&countersurv_4-07-2014.pdf

Минюст Обамы официально обвинило журналиста в совершении преступления в деле об утечке информации (Obama DOJ formally accuses journalist in leak case of committing crimes).
https://www.theguardian.com/commentisfree/2013/may/20/obama-doj-james-rosen-criminality

Ваши секреты из WhatsApp теперь в безопасности, но Большой Брат все еще следит за вами! (Your WhatsApp secrets are safe now. But Big Brother is still watching you…).
https://www.theguardian.com/commentisfree/2016/apr/10/whatsapp-encryption-billion-users-data-security

Преследуя разоблачителей, правительство Обамы грозит всем информаторам (Obama Pursuing Leakers Sends Warning to Whistle-Blowers).
http://www.bloomberg.com/news/2012-10-18/obama-pursuing-leakers-sends-warning-to-whistle-blowers.html

6 ошибок при шифровании, которые приводят к утечке информации (6 encryption mistakes that lead to data breaches).
https://www.crypteron.com/blog/the-real-problem-with-encryption/?gclid=Cj0KEQiA9P7FBRCtoO33_LGUtPQBEiQAU_tBgDgBzD9wIXv94vwhj3qwhc6ewEYYeyjIeiXtMQiwF3caAsFn8P8HAQ

ОБ АВТОРЕ

Майкл Деган в настоящее время начинает активно заниматься контент-маркетингом для развивающихся компаний, до этого он 25 лет занимал руководящие редакторские должности в «Гаарец Груп», ведущем СМИ Израиля. На своем последнем рабочем месте он занимал должность заместителя главного редактора и отвечал за все операции, связанные с распространением печатных и цифровых версий издания на иврите и английском языках; также он отвечал за проведение конференций и аналогичных мероприятий.

Деган – опытный редактор СМИ, который за долгие годы работы контролировал ведение множества журналистских расследований. Так, он занимался этим, будучи главным редактором еженедельного журнала «Гаарец» и экономического ежемесячника TheMarker (ставшего под руководством Дегана ведущим изданием страны). Деган внедрил множество инноваций «Гаарец» в еженедельник (ставший в настоящее время одним из ведущих активов компании), и запуск iPad-версии журнала был одной из них. При всем при этом господин Деган – не параноик, и его можно найти в социальных сетях: @mikedagan в Twitter, Michael Dagan - в Linkedin.