Публикация на тему

Приватность в информационную эпоху

За нашими передвижениями следят, разговоры записываются, а почту читают. У каждого обладающего соответствующими полномочиями человека есть доступ к этим данным. И это не антиутопия. Это реальность, в которой мы живём. Возможно, вы считаете, что вам нечего скрывать, но вам есть что защищать. Поэтому, давайте разбираться, как сохранить приватность в информационную эпоху...

Анотация

В статье автор рассматривает понятие приватности в информационную эпоху. Особое внимание уделяется информационной гигиене, безопасности в интернет и социальных сетях, использованию VPN и Proxy.

In the article, the author explains the concept of privacy in the information age. Particular attention is paid to information hygiene, security on the Internet and social networks, the use of VPN and Proxy.

Автор

Михалькевич Александр Викторович

Публикация

Наименование Приватность в информационную эпоху

Автор А.В.Михалькевич

Специальность За нашими передвижениями следят, разговоры записываются, а почту читают. У каждого обладающего соответствующими полномочиями человека есть доступ к этим данным. И это не антиутопия. Это реальность, в которой мы живём. Возможно, вы считаете, что вам нечего скрывать, но вам есть что защищать. Поэтому, давайте разбираться, как сохранить приватность в информационную эпоху...,

Анотация

В статье автор рассматривает понятие приватности в информационную эпоху. Особое внимание уделяется информационной гигиене, безопасности в интернет и социальных сетях, использованию VPN и Proxy.

Anotation in English

In the article, the author explains the concept of privacy in the information age. Particular attention is paid to information hygiene, security on the Internet and social networks, the use of VPN and Proxy.

Ключевые слова private, информационная безопасность, vpn, proxy
Количество символов 29273

Содержание

Введение

Цель исследования - формирование привычек безопасного поведения в информационную эпоху.

1 Информационная гигиена

В современном мире потоки информации льются на нас со всех сторон, заставляя так или иначе реагировать. Информация влияет на здоровье человека. И все наши дальнейшие действия по повышению безопасности будут бессмысленны, если мы не будем соблюдать основные правила информационной гигиены. Постоянный неконтролируемый информационный поток приводит к зависимости от (новостей, игр, сериалов, соц.сетей и прочих потоков информации). Также, высокая активность в интернете является повышенным источником рисков различного рода.

Поэтому важно ограничить информационный поток; отказаться от распространения непроверенной информации; избегать конфликтов и ругани в интернете; и, наконец, несмотря на негативный поток информации, следовать привычному образу жизни.

2 Безопасность в интернет

Если вы когда-нибудь заполняли формы на сайтах, указывая там личные данные, то вы добровольно передали персональную информацию третьим лицам. И теперь, любая компания, правительственная организация, грамотный специалист или человек, готовый заплатить за эти данные имеет к ним доступ.

Список компаний, которые занимаются сбором таких данных - огромен. Американская

некомерческая организация "Privacy rights" собирает информацию о таких компаниях. По ссылке https://privacyrights.org/data-breaches можно скачать базу таких компаний с коротким описанием инцидентов, когда эти данные были получены третьими лицами.

Но даже, если вы не заполняли никаких форм и не выкладывали свои данные в публичный доступ, всё-равно, компаниям становятся доступны данные из наших электронных писем, чатов, покупок в интернет-магазинах, посещаемых сайтах, телефонных разговоров и передвижениях. Проблемма в том, что даже, если вы считаете, что вам нечего скрывать, вы можете скомпрометировать себя нарушением закона, о существовании которого даже не догадываетесь. Например, существует перечень животных, которых нельзя содержать дома, существует перечень растений, которые нельзя выращивать. Существуют темы, которые нельзя обсуждать, а за некоторые комментарии могут наказать реальным тюремным сроком или штрафом. Вы уверены, что не нарушили ни одного закона?

Дальше. На вашем компьютере хранится множество файлов, фото и видео. Скорее всего, большинство из этого - безобидные семейные снимки. Но что если они уже все доступны третьим лицам? Даже если мы не хотим ни с кем делиться своими файлами, облачные сервисы лишают нас такой возможности.

3 Как избежать отслеживания телефона

Чтобы подключиться к мобильному оператору, необходимо заключить договор, в котором мы указываем паспортные данные, а иногда и кредитную историю.

Мобильные операторы отслеживают гео-локацию телефона. Когда мобильное устройство включено, оно находится на связи сразу с несколькими мобильными станциями. Мобильное устройство, даже в выключенном состоянии, периодически передаёт уникальный код, который после расшифровки превращается во временный идентификатор мобильной станции (TMSI) абонента. Данный идентификатор содержит информацию о местоположении пользователя, скорости передвижения, расстояния до ближайших станций. Если при этом абонент совершал звонок, то и информацию о звонке и личности абонента. Все эти данные доступны в файлах.

В некоторых странах можно приобрести одноразовые телефоны, . Однако данные таких телефонов передаются точно также, как и в обычном мобильном телефоне. Даже если у мобильного оператора нет информации о личности пользователя, владельца телефона можно вычислить по звонкам, по уличным и дорожным камерам и т.д.

Подключиться к мобильному телефону с целью прослушки голосовых сообщений можно удалённо от объекта прослушивания.

Так, всё же, как избежать отслеживания, но при этом пользоваться телефоном? Пользоваться проводным телефоном с шифрованием голоса. Но такие аппараты решают проблемму перехвата голоса только в том случае, если применяются обеими сторонами. Либо вместо телефона пользоваться рацией, но и в этом случае, есть проблема открытых диапазонов частот, к которым можно подключиться со стороны.

4 VPN и Proxy для сокрытия IP адреса

Для конфиденциальности при работе в интернете, можно использовать VPN или прокси-сервера. Они повышают безопасность интернет-соединения, но как именно они работают и чем отличаются? Понимание разницы между VPN и прокси-сервером позволит выбрать правильный инструмент и повысить конфиденциальность при работе в интернете.

Определения VPN и прокси-сервера

Как VPN, так и прокси-серверы обеспечивают конфиденциальность за счет того, что позволяют различными способами скрывать IP-адрес. Однако используемые способы и набор дополнительных функций конфиденциальности значительно различаются.

Что такое прокси-сервер?

Обычно при просмотре веб-страниц компьютер подключается напрямую к веб-сайту и начинает загружать страницы для чтения – это довольно простой процесс. При использовании прокси-сервера компьютер сначала отправляет весь веб-трафик на прокси-сервер, затем прокси-сервер перенаправляет запрос на целевой веб-сайт, загружает информацию и передает ее обратно.

Таким образом прокси-серверы маскируют IP-адреса и позволяют пользователям обходить ограничения на контент и мониторинг. Например, пользователи могут просматривать контент с географическими ограничениями: подписчик Netflix из Великобритании, подключающийся к прокси-серверу в США, может получить доступ к контенту Netflix для США.

Что такое VPN?

VPN – это виртуальная частная сеть (Virtual Private Network). VPN создает зашифрованный туннель для передачи данных, защищает личность в интернете, скрывая IP-адрес, и позволяет безопасно использовать публичные точки доступа Wi-Fi.

VPN работает на уровне операционной системы, осуществляя перенаправление трафика, поступающего из браузера или приложения, а также шифруя трафик между интернетом и устройством пользователя. В результате интернет-провайдер не может отслеживать действия пользователя в сети, он видит, только подключение к VPN-серверу. Такой вид шифрования защищает от отслеживания посещаемых веб-сайтов, правительственного контроля и злоумышленников, которые могут попытаться шпионить за устройством.

В чем разница между прокси-сервером и VPN?

Рассмотрим основные различия VPN и прокси-сервера.

VPN шифрует информацию

VPN шифруют любые отправляемые и получаемые данные; прокси-серверы этого не делают. Шифрование данных обеспечивает дополнительную безопасность таких конфиденциальных транзакций, как действия в онлайн-банке и покупки в интернете, а также не позволяет

злоумышленникам отследить данные вашей кредитной карты и учетные данные для входа.

В зависимости от способа доступа, и VPN, и прокси-серверы могут замедлять работу в интернете. Чаще всего более медленными (и менее безопасными) являются бесплатные прокси-соединения, как правило, из-за меньшего количества параметров конфигурации, сокращенной инфраструктуры и неполной поддержки. Скорость VPN зависит от провайдера, однако, как правило, VPN является более быстрым вариантом.

VPN обычно платные

Не рекомендуется использовать бесплатные VPN-сервисы: они ограничены по функционалу и могут собирать ваши данные. Платные VPN обеспечивают лучшее шифрование данных и являются более безопасными. Многие прокси-серверы, в отличие от VPN, являются бесплатными. Как правило, VPN – это более дорогой вариант.

VPN обеспечивает большее покрытие

VPN работают на уровне операционной системы и перенаправляют весь трафик через VPN-сервер, а прокси-серверы работают на программном уровне и перенаправляют трафик только определенного приложения или браузера. Это означает, что VPN шифруют все действия в интернете, независимо от сайта и приложения, а прокси-серверы в каждый момент времени могут скрыть только один сайт или приложение. В результате VPN обеспечивают большее покрытие.

Большинство VPN не регистрируют трафик

Большинство провайдеров VPN не регистрируют веб-трафик, чего нельзя сказать о прокси-серверах. Для полной конфиденциальности рекомендуется использовать услуги провайдера VPN с политикой отсутствия журналов. Такие провайдеры не отслеживают и не сохраняют действия пользователей в интернете. Бесплатные прокси-серверы, напротив, могут регистрировать трафик для продажи данных третьим лицам.

Что лучше: VPN или прокси-сервер?

Для сокрытия IP-адреса подойдет и прокси-сервер, и VPN. Если важна скорость просмотра и требуется скрыть IP-адрес только от одного сайта или приложения, бесплатный прокси-сервер справится с этой задачей.

С другой стороны, для сокрытия действий в интернете лучше подключаться к нему через VPN, поскольку VPN шифруют данные во время работы в интернете, а прокси-серверы – нет. В результате VPN обеспечивает большую безопасность при выполнении таких действий, как онлайн-банкинг или покупки в интернете.

Основные провайдеры VPN взимают плату за свои услуги, однако обеспечиваемая ими безопасность гарантирует защиту конфиденциальной, личной и финансовой информации от злоумышленников.

Подводя итог: VPN обеспечивает большую конфиденциальность и безопасность, чем прокси-сервер, поскольку направляет трафик через защищенный VPN-сервер и шифрует его. Прокси-сервер просто направляет трафик через промежуточный сервер, не обязательно обеспечивая при этом дополнительную защиту. В отличие от прокси-сервера, VPN работает на уровне операционной системы и защищает весь трафик.

Если вы уже используете VPN, то использовать прокси-сервер не надо. VPN выполняет ту же функцию, что и прокси-сервер, но предлагают больше расширенных возможностей.

5 Невидимость в браузере

Скрытие геолокационных данных

На странице http://benwerd.com/lab/geo.php можно проверить, знает ли браузер ваши геолокационные данные.

Если ваше местоположение определилась, а вы хотите оставаться невидимым, то эту функцию можно отключить.

В **Firefox** для отключения опции определения местоположения, необходимо в адресной строке набрать:

```
about:config
```

Далее найти пункт `geo.enabled` и присвоить ему значение `false`.

В **Chrome** нужно перейти в `Настройки (Options)`. Далее `Дополнительные (Under the Hood) - Настройки контента -> Геоданные (Content Settings -> Location)`. И сделать переключатель неактивным `Спрашивать разрешение на доступ Do not alow any site to track my physical location`

В других браузерах тоже должна присутствовать аналогичная возможность.

Изменение геолокационных данных

В Firefox для изенения геолокационных данных можно скачать и установить приложение **Change Geolocation**

В браузере Google Chrome существует встроенная функция изменения геоданных.
Для этого необходимо перейти в `Инструменты разработчика (Developer Tools) - More Tools -> Sensors`. Найти раскрывающийся список **Geolocation**. И здесь можно указать точную широту и долготу. После чего сайты будут определять местоположение по этим координатам.

6 Безопасный поиск

Google при выдачи ответов на поисковые запросы учитывает все введёные ранее запросы. Таким образом, данный поисковик подтасовывает результат выдачи.

Для безопасного поиска лучше воспользоваться ресурсом duckduckgo.com, данный поисковик не подстраивает поисковую выдачу в соответствии с нашими предыдущими предпочтениями и местоположением. **DuckDuckGo** - online поиск без слежки.

7 Безопасность общественных сетей

При подключении к беспроводной сети, MAC-адрес, который является уникальным идентификатором подключаемого устройства, фиксируется сетевым оборудованием.

Поэтому, прежде чем подключаться к общественной сети WiFi, чтобы оставаться невидимым необходимо изменить MAC-адрес. Также важно в это время не заходить ни в какие личные аккаунты.

Чтобы изменить MAC-адрес нужно следовать инструкциям конкретной операционной системы - Linux, Windows, Android, macOS или iOS. После перезагрузки устройства, возвращается исходный MAC-адрес, поэтому делать это нужно каждый раз при подключении к общественной сети.

8 Безопасность общественных компьютеров

В информационной безопасности есть принцип "минимальных полномочий", согласно которому пользователь должен получать тот минимум полномочий, которого будет достаточно для выполнения своей задачи. Так, в терминалы регистрации электронных ж/д билетов, возможно совершение только одного действия - покупки билета.

Однако во многих интернет-кафе имеются компьютеры с правами системного администратора, что позволяет устанавливать любое программное обеспечение, а это нарушает принцип "минимальных полномочий" и повышает риск того, что кто-то уже установил вредоносную программу. Такие программы достаточно сложно выявить, поэтому исходим из того, что вредоносное ПО уже установлено. А это значит, что все логины и пароли, которые вы вводите на интернет-ресурсах общественных компьютерах становятся известны третьим лицам. Также не забываем про камеры видеонаблюдения, которые установлены в интернет-кафе таким образом, чтобы видеть действия пользователя.

Поэтому для решения личных вопросов лушче обзавестить личной точкой доступа (которая уже имеется в любом смартфоне или мобильном телефоне), либо отложить дела до тех пор, пока не верётесь домой. Если всё же пользуетесь общественными компьютерами, то уходя, необходимо закрывать и разлогиниваться из всех посещаемых ресурсов, сбрасывать флажки типа "запомнить меня", удалять куки, чистить историю посещений... так, чтобы никто даже не догадался, что тут кто-то был.

9 Безопасные фотографии и файлы

Однажды, один джихадист, находясь на военной базе сделал селфи и выложил в интернет. На другом конце света американские военные определили координаты того места, откуда была сделана фотография. Вскоре военная база джихадистов был полностью уничтожена.

Координаты снимка были извлечены из метаданных файла с помощью стандарта EXIF. Стандарт EXIF позволяет сохранить полученные с приёмника GPS координаты места съёмки. Как правило, фотоаппараты добавляют к файлу информацию, специфичную только для данной конкретной камеры. Правильно интерпретировать такую информацию могут только программы от изготовителя фотоаппарата.

Кроме того, даже если подделать метаданные изображения, определить местоположение можно по фону, мизансцене и другим визуальным зацепкам фотографии.

10 Опасные социальные сети

Существуют ли безопасные социальные сети? Наверное, да. Только если вы сами являетесь разработчиком такого ресурса (или хотя бы знаете как происходит шифрование данных на этом ресурсе) и уверены в безопасности сервера.

Однако большинство людей пользуются популярными социальными сетями, такими как Facebook, Google, Instagram. Так в чём же их опасность? Давайте разбираться.

Facebook использует технологию распознавания лиц. И если вы загрузите на сайт фотографию, Facebook попытается определить людей на фото. Таким образом Facebook-у становится известно кто на фото, а благодаря методанным также когда и где было создано фото. Злоумушленники могут воспользоваться этим. А если вы еще выкладываете правдивую персональную информацию (адрес, место работы, учёбы), то вы упрощяете им задачу.

В своих профилях лучше всего указывать ложную персональную информацию.

С Google дело обстоит ещё хуже. Google тоже определяет людей по фото, определяет наше местоположение, но еще и персонализирует рекламу и поисковую выдачу.

11 Банковские карты

В первую очередь необходимо обеспечить безопасность своих банковских карт. Естественно, данные банковских карт нельзя передавать третьим лицам. Но чтобы защититься от мошеннеческих транзакций (например, когда вы оплачиваете одну сумму, а снимается другая) этого недостаточно.

Можем сделать следующее. Заводим еще две банковские карты. Одна - обычная, пластиковая, вторая - виртуальная. Расчитываемся только виртуальной. Но деньги храним на другой. На карту, которой расчитываемся, переводим только необходимую для транзакции сумму.

Заключение

Осталось еще множество моментов в информационной безопасности, с которыми еще предстоит разобраться. Например, безопасность умного дома и интернет-вещей, безопасность современных автомобилей, безопасность общественного транспорта и т.д. Но это уже предметы исследования будущих статей.

Список использованных источников

Приложения