Визитка

ВЛАДИМИР БЕЗМАЛЫЙ, Microsoft Security Trusted Advisor, Certificate Trainer Kaspersky Lab, Consultant UN (Information Security), автор серии книг «Цифровая гигиена», cybercop@outlook.com

Персональная безопасность
в цифровую эпоху

В одной статье невозможно полноценно раскрыть все существующие угрозы. Здесь мы опишем наиболее актуальные и опасные варианты посягательства на вашу информационную безопасность.

Жизнь в цифровом мире заметно меняет реальность – то, что раньше воспринималось как нечто стороннее, второстепенное, становится источником полноценных угроз совсем не абстрактного характера. Теперь забота об информационной безопасности – это забота о скрытых сторонах вашей личной жизни, семейном спокойствии и ваших деньгах. Наступили времена, когда информационная безопасность стала необходимым для изучения предметом не только для специалистов из области ИТ, но и любого человека, сталкивающегося с электронными устройствами.

Тенденция связи с интернетом любой техники, независимо от ее назначения, сделала всех нас максимально уязвимыми. Принимать профилактические меры необходимо так же серьезно, как при эпидемии гриппа – лечиться будет поздно, носите маску! Внешний мир способен вторгнуться в нашу жизнь через наши же личные и общедоступные устройства.

Стоит сразу указать область, которая может рассматриваться как зона приложения информационных технологий. Это практически вся техника, окружающая нас в повседневности:

- средства коммуникации и получения информации – от ПК до смартфонов и навигаторов, умные телевизоры и домофоны;
- средства и инструменты расчетов – банковские карты и приложения, способы обращения к платежным системам;
- любые приборы, имеющие электронные компоненты – от автомобиля до «умного» холодильника, имеющего связь с сетью, в том числе электронные дистанционные замки и выключатели;
- общественная техника – светофоры, видеокамеры, датчики, в том числе и те, что установлены на турникетах в транспорте.

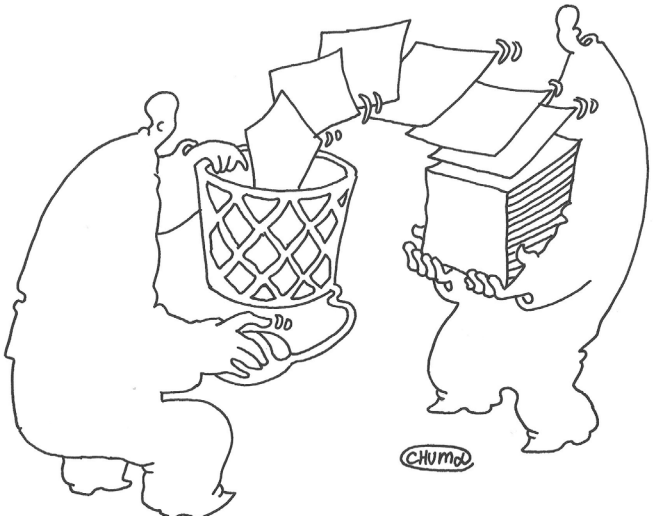
Нет никакой возможности не только отказаться от контактов с цифровой реальностью на личном уровне, но и избежать встречи с ней в повседневной жизни, просто выходя из дома. Угроза есть везде, и мы не можем полностью описать все ее проявления. Остановимся на очевидных проблемах информационной и цифровой безопасности, на тех, что мы можем создать или пропустить сами. Или предотвратить.

Персональные компьютеры

Принято считать, что угрозы вашему ПК исходят от некоего удаленного взломщика или вредоносной программы, вируса. Это важно, реально и опасно, но мы сами создаем условия для потери своих данных – просто вспомните, сколько раз у вас отключалось электричество до сохранения файла, а что еще опаснее, до завершения платежа без возможности выйти из программы или с сайта, на котором остались ваши реквизиты. А достаточно ли надежно установлен ноутбук на вашем рабочем столе? А сколько раз его роняли ваши дети, сколько кофе и хлебных крошек уже скопилось в клавиатуре? Это, конечно, не «чистые» и прямые ИТ-угрозы, но суть не меняется – это угрозы вашим данным и носителям.

Следующий уровень – вы уверены, что приложения, облегчающие, например, смену раскладки клавиатуры, не запоминают все, что вы ввели, в том числе и банковские пароли, отправляя эти данные на удаленный сервер? А как вы относитесь к рутинной процедуре резервного копирования и архивирования? Архивы заполняют жесткий диск? Тогда будьте готовы потерять свои фото, заметки и файлы – от этого никто не застрахован, но вспоминаем мы об этом, только когда потеря уже стала фактом.

Следующий уровень угрозы – ваш компьютер могут зашифровать. Это уже полноценная профильная ИТ-угроза с внешним проникновением. По мнению специалистов в области ИБ, к 2021 году атаки такого рода могут вырасти примерно в 55–57 раз в сравнении с показателями пятилетней давности. Общий ущерб от этих атак может достичь рубежа в 20 миллиардов долларов, и сколько в них составит ваша доля, зависит от вашей внимательности. Опасной чертой этого направления развития вымогательства остается неизбирательность, так как злоумышленник может в равной степени проявить интерес к пользовательскому домашнему ПК или к рабочим станциям корпоративной сети.



Внешний мир способен вторгнуться в нашу жизнь через наши же личные и общедоступные устройства

Как вы можете защитить себя от вымогателей?

Многие пользователи интернета узнали о вымогателях из новостей, когда 12 мая 2017 года началось стремительное распространение по миру зловреда WannaCry, заразившего и заблокировавшего компьютеры крупных компаний, в том числе почтовой системы FedEx, нескольких крупных банков и операторов национальных служб связи. Досталось и транспорту – пострадали Deutsche Bahn и LATAM Airlines.

Атака показала не только возможность использовать системные уязвимости, но и совершенствовать средства доставки зловредов. У локального или корпоративного пользователя есть несколько возможностей противостоять угрозе. Одна из них – закрыть входные ворота.

Что такое вымогатель?

Для начала разберемся, что такое сетевой компьютерный вымогатель, по сути и технически. С точки зрения ПО – это некая программа, которая после попадания на устройство получает возможность заблокировать или ограничить доступ либо к отдельным файлам и разделам ОС, либо к самой системе, лишив вас привилегий и прав авторизации на любом уровне. За возвращение доступа вам предлагают заплатить некую сумму переводом в виде электронного платежа.

В категории вымогателей распространены в основном следующие виды ПО:

- блокировщик Windows, активирующийся после загрузки ОС и показывающий всплывающее окно с требованием выкупа без возможности использовать средства системы;
- блокировщик браузера – активируется при запуске программы и демонстрирует баннер с требованиями выкупа, перенаправляя на одну и ту же страницу;
- шифровальщик данных – позволяет войти в систему, но зашифровывает локальные файлы, не давая возможности их открыть, что особенно опасно в корпоративных сетях при использовании баз данных;
- программа-загрузчик – первичный компонент ПО, проникающий на локальный компьютер или сервер с целью установки исполняемого «вымогателя».

В терминологии и по сути вымогатель и шифровальщики синонимичны, хотя могут использовать разные методики воздействия на ПК, ОС и пользователя. По мнению специалистов служб безопасности, распространение вымогателей пока остается бесконтрольным и несет большую опасность бизнесу, где установщик может передаваться от машины к машине через корпоративные сети. Проблема состоит еще и в том, что первичный троян маскируется под системные программы и потому остается нераспознанным.

В качестве основного принципа защиты остается актуальной кордонная и профилактическая тактика – предотвращение проникновения загрузчика, его обнаружение в системе и дезактивация до начала шифрования. При этом для бизнеса очень важно, чтобы защитное и профилактическое ПО не ограничивало работу ПК и сетей, оставаясь активным в режиме ожидания угрозы и анализа исполняемых файлов после их открытия. Не стоит забывать и о том, что троян-загрузчик, как и шифровальщик, вполне может отправлять вашу информацию удаленному получателю, а это создает дополнительную угрозу конфиденциальности данных.

Практика показывает, что если раньше можно было выявить исполняемый файл или библиотеки вымогателя и, изменив его название, заблокировать процесс, то новые программы успешно создают собственные резервные копии и быстро охватывают даже зашифрованные архивы пользователя. Поэтому необходимо прибегать к профессиональным методам защиты.

Одно из таких решений – Acronis Ransomware Protection, специализированное ПО с облачным пространством, правда, ограниченным всего 5 Гб удаленной памяти. Решение бесплатное, но позволяет пресечь атаки, повторяющиеся примерно каждые 10 секунд. Важно – инструмент не вступает в конфликт с распространенными антивирусами.

Как заблокировать скрипты Cryptomining в вашем веб-браузере

Основная цель скрытого использования чужих ресурсов – криптомайнинг, требующий больших объемов вычислений в реальном времени. С точки зрения злоумышленника, ему

гораздо интереснее запустить средство заражения на производительные устройства в крупной бизнес-сети, чтобы получить доступ к ресурсам. Однако сценарии могут быть разными по техническим и организационным решениям. Возможность генерировать коды криптовалют на чужих мощностях дает высокие прибыли.

Что такое криптоджекинг

Использование криптомайнинга и связанного с ним криптоджекинга началось с 2011 года, но после взлета курсов биткоина произошел качественный скачок этого вида активности. Классический криптоджекинг – это заражение ПК или иного устройства с постоянным доступом к сети вредоносным ПО, с последующим запуском вычислений и большим потреблением локальных ресурсов. При объединении нескольких зараженных ПК в сеть по инициативе майнера или при доступе к готовой сети возможности возрастают в разы за счет суммирования мощностей и постоянного пребывания в интернете некоторого количества машин.

> Важной особенностью современного криптоджекинга стал перенос активности из пользовательской системы на сторонний ресурс

Скрытое использование вашего ПК может показаться не таким опасным, как прямое вымогательство, но для компаний с собственными сетями оно может стать источником разного рода потерь. Если индивидуальный пользователь может и не обратить внимания на отбор сторонней программой примерно 10–20 % производительности компьютера, то в корпоративной сети произойдет суммирование результата, что приведет к потере скорости обмена данными, сбоям и зависаниям баз данных, увеличению расходов на трафик и потребление энергии.

Важной особенностью современного криптоджекинга стал перенос активности из пользовательской системы на сторонний ресурс. Вы открываете вкладку браузера, заходя на сайт, и там запускается процесс майнинга, использующий ваши системные ресурсы. Фактически не требуется непосредственного заражения ПК, так как браузер имеет собственные системные возможности. Зловредный сайт, как правило, имеет свою специфику – это ресурсы, на которых пользователь задерживается надолго, например, для просмотра фильмов. Одна вкладка отбирает немного производительности, и жертва больше склоняется к версии «медленного интернета», чем к подозрению на скрытый майнинг.

Уже упомянутый эффект суммирования дает возможность получать с нескольких зараженных машин и сетей большие суммы, практически не привлекая к себе внимания. При этом распространение носителя остается предельно простым – заставить пользователя пройти по фишинговой ссылке. Далее для заражения сети можно использовать хорошо отработанную методику распространения червей.

В зависимости от возможностей компьютера жертвы, злоумышленник может принять решение о наиболее выгодном его использовании – как части майнинговой сети, как средства вымогательства или организации массовых атак. Сам выбор можно автоматизировать, и тогда организатору останется только получать результаты и заниматься организационными и финансовыми вопросами, не отвлекаясь на технические детали.

Как работает незаконный криптомайнинг

Одним из средств распространения программ для криптоджекинга оказался своего рода универсальный «транспортировщик» – эксплойт EternalBlue, ранее заражавший ПК и серверы вымогателями WannaCry. Опасность же заражения гораздо выше, так как жертвы могут вообще не представлять себе, что происходит кража их ресурсов. Некоторое замедление системы или использования браузера может не привлекать внимания и не вызывать серьезного дискомфорта.

Второй путь заражения – отправка на ПК поддельного обновления штатного ПО, например, замаскированного под очередное обновление распространенных плагинов типа Adobe Flash Player. Третий путь мы уже упоминали – внедрение майнингового кода в рекламные баннеры на сайтах, где пользователь проводит много времени за просмотром фильмов или играя онлайн. В корпоративных сетях противодействовать этому можно, ограничивая доступ к сторонним сайтам, а индивидуальным пользователям потребуется бдительность.

Программы типа Cryptomining проходят стадии развития в направлении незаметности. Теперь майнер не забирает всю мощность вашего процессора, чтобы не привлекать к себе внимания. Новые версии программ рассчитаны на отбор не более пятой части ресурсов и распределение вычислений по созданной или имеющейся сети. Прибыль злоумышленника возрастает, а риск обнаружения минимизируется, распределяясь по множеству машин. Структура сети практически снимает ограничения с таких решений, остается только противодействие на уровне конкретного ПК или узла. Использовать чужие ресурсы можно долго, прибыльно и без потерь при обнаружении.

Еще одна серьезная проблема состоит в доступности ПО. Злоумышленник может приобрести готовый блок или воспользоваться услугой за минимальные взносы в размере полдоллара. Этому способствует естественный для криптовалют уровень конфиденциальности, не позволяющий эффективно отслеживать или воздействовать на транзакции и процесс генерирования кода.

Известные криптоджекеры

Smominru

Это сложная иерархическая сетевая структура, ботнет, включающий более полумиллиона машин с распределением функций от организации и администрирования до непосредственного майнинга. По итогам 2018 года его владельцы собрали в эквиваленте более 3 миллионов долларов, используя интеллектуальный подход к обновлению структуры ботнета. Для создания этой сложной и многоуровневой

системы использовалась украденная у АНБ база EternalBlue, опыт доработки, который сформировался при эпидемии вымогателей за год до начала эпохи массового криптоджекинга – это атаки WannaCry в 2017 году.

BadShell
Представитель «умных» криптомайнеров, способных маскироваться под системные процессы класса Windows PowerShell для выполнения собственных сценариев. Проблема состоит в сложности обнаружения их антивирусами, которые по умолчанию настроены на доверие к системным процессам и игнорируют изменения в их работе. После удаления майнер способен к восстановлению из резервной копии, спрятанной в загрузочной области жесткого диска.

Coinhive
Вредоносная модификация ранее легитимного инструмента монетизации сайтов, которая с трудом распознается из-за актуальности легальной версии. Относится к самым серьезным угрозам по признаку распространенности, маскировки и простоте проникновения.

MassMiner
Комплексный многофункциональный набор эксплойтов, способный применить несколько инструментов для внедрения в систему. ПО работает по принципу взаимодействия внутренних модулей и эксплуатирует известные уязвимости Oracle WebLogic, Windows SMB и Apache Struts. Создатели ПО уже получили в эквиваленте не менее двухсот миллионов долларов.

Prowli
Структурированный ботнет с распределением функций и иерархией устройств, в состав которого может входить, по приблизительным оценкам, примерно 40 тысяч бытовых устройств, серверов и модемов. Специализируется на интернете вещей, что делает крайне сложным его обнаружение в процессе работы. Может заниматься вредоносными перенаправлениями, будучи внедренным в модем или сервер. Для проникновения использует червя, перебирающего пароли, по заданию может устанавливать бэкдоры и использовать скрытые порты для выкачивания конфиденциальной информации.

WinstarNssMiner
Атакующее ПО, способное распознавать антивирусные программы и оставаться пассивным во время проверок. Активируется при ослаблении и отсутствии защиты. Весной 2018 года атака привела к заражению более пятисот тысяч устройств. При обнаружении и попытке удаления провоцирует аварийное завершение работы ПК, а после восстанавливается.

Стоимость криптомайнинга

В чем причина распространения несанкционированных криптомайнеров? В первую очередь это огромная разница в стоимости самого процесса и его обеспечения. Криптографическая валюта представляет собой динамическое и разбитое на отдельные области кода (хэши) описание процесса транзакции. Она не имеет признаков «денежной единицы» как таковой, ценность имеет некое множество хэшей, в которых закодирован процесс передачи платежа.

Количество хэшей вообще ограничено, поэтому для получения (создания) одной условной единицы необходимо перебрать массу вариантов, чтобы найти один, уникальный и соответствующий определенным условиям. Это сложнейшая математическая задача, для решения которой необходим мощный аппаратный комплекс. Легальный майнер должен приобрести оборудование и нести огромные затраты на его энергоснабжение и охлаждение. Это очень большие вложения, потому возникает спрос на ПО, способное организовать тот же процесс на сторонних машинах без собственных затрат. На выходе за каждый сгенерированный набор хэшей майнер получает долю условной криптовалютной единицы.

Распространение cryptomining

Браузерные версии криптомайнеров в виде скриптов сложно отнести к вредоносам. Это может быть и вполне легальный инструмент, заменяющий показ оплаченной рекламы на сайте. Так, сайт Quartz предлагал такое решение посетителям, если те давали согласие на использование вкладки (процесса) для майнинга.

При отсутствии прямого предупреждения и запроса согласия майнинг становится мошенническим инструментом, который условно крадет ресурсы пользовательского устройства. Их крайне сложно отразить в денежном эквиваленте, чтобы подсчитать ущерб и предъявить обоснованные претензии. Именно по этой схеме работают нелегальные майнеры, затраты которых на порядок меньше затрат владельцев майнинговых ферм.

Если один пользователь ПК практически не заметит потерь от скрытого браузерного майнинга, то компания, машины которой используются злоумышленниками, понесет дополнительные расходы на электроэнергию, потери от снижения скорости работы сети, обмен данными – при пересчете на количество машин это может сложиться в солидные суммы.

Как определить, был ли ваш компьютер заражен

Выявить заражение по признакам работы криптомайнера довольно сложно. Если не заниматься регулярными проверками производительности и не собирать статистику, то первичным критерием будет только субъективное ощущение замедления скорости работы ПК и загруженности ЦП, быстрой потери заряда батареи ноутбука. Но это очень размытые параметры.

Профилактически проверить компьютер на скрытый майнинг можно через стандартный диспетчер задач Windows или MacOS Activity Monitor во вкладке ПРОЦЕССЫ. Там будет отображено, сколько ресурсов потребляет браузер. Насколько это много или мало – судить вам. Чтобы прервать браузерный майнинг, достаточно завершить процесс. В некоторых браузерах, например, в Chrome, каждой вкладке соответствует отдельный процесс, что может помочь в выявлении майнинговой активности.

Новые майнеры не загружают ЦП полностью, отбирая не более 20% его мощности, потому и определить их сложнее. Для точного выявления придется собирать статистику

загруженности процессора по времени и вкладкам, учитывать скорость передачи данных и даже температуру воздуха. Скорее всего, этот вид майнинга не принесет вам сколько-нибудь серьезных неудобств и останется незамеченным для одного ПК.

Остановка криптомайнинга в браузерах

Вопрос в том, чего вы хотите – прервать несанкционированный майнинг через браузер или принять профилактические меры против него? Поскольку методы идентификации атаки несовершенны или слишком сложны, проще рассчитывать на профилактику. И тут снова поможет кордонный принцип – не пускать или пресекать активность.

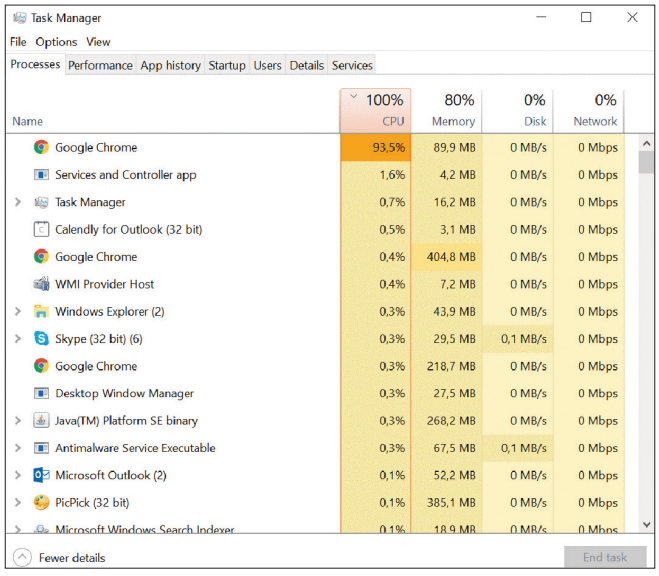
Развертывание расширений браузера

В большинстве распространенных пользовательских браузеров есть экосистема расширений или аддонов, среди которых можно найти и использовать средства выявления и пресечения скрытого майнинга. Они могут предоставляться разработчиками браузера или сообществами, иметь закрытый или открытый исходный код. В качестве примера можно привести No Coin и MinerBlocker для Chrome, Opera и Firefox. Но никто не гарантирует вам полной чистоты и безопасности самих расширений!

Ad-Blocker Software

Для большинства браузеров существуют блокировщики рекламы. Это ПО вполне способно запретить выполнение скриптов на определенных сайтах, а именно скрипт и является основой майнинга. Однако, в последнее время разработчики браузеров стали сами запрещать блокировщики – перекрывая рекламу, они мешают бизнесу поисковиков и заметно снижают монетизацию сайтов. GOOGLE всерьез обещает перекрыть возможности блокирования на сайтах, что может привести и к значительному снижению эффективности этого метода.

Рисунок 1. Диспетчер задач показывает подозрительную загрузку браузера.



GOOGLE всерьез обещает перекрыть возможности блокирования на сайтах, что может привести и к значительному снижению эффективности этого метода

Отключить JavaScript

Радикальная мера. Нет скриптов – нет выполнения сценариев майнинга. Популярность JavaScript и без того быстро снижается, а в некоторых браузерах запрет выставлен по умолчанию или обеспечивается встроенными блокировщиками и аддонами. Часть сайтов продолжает использовать скрипты и в обычном режиме, поэтому отключение может привести к проблемам с просмотром.

Блокировать домены

Если вы пришли к выводу, что определенный сайт или домен занимается скрытым майнингом, достаточно ввести его в список блокировки. В настройках браузера есть такая возможность по URL-адресу. Для блокировки Coinhive достаточно вставить опасную строку https://coin-hive.com/lib/coinhive.min.js в текстовое поле.

Другие угрозы конфиденциальности данных

Достаточно ли заблокировать майнинг в браузере, чтобы почувствовать себя в безопасности? Это несложно сделать даже в профилактических целях, используя набор вполне доступных и описанных выше инструментов.

Но это не решение проблемы скрытого майнинга и возможного присутствия криптоджекеров в системе. Они вполне могут устанавливаться самостоятельно, как отдельные программы, для обнаружения и нейтрализации которых потребуется полноценное антивирусное ПО.

Не стоит забывать, что большинство бесплатных антивирусов имеет ограниченные возможности, и если речь идет о бизнесе и корпоративной безопасности, то имеет смысл приобрести полноценные платные версии.

А теперь пойдет речь об угрозах другого рода. Это несанкционированный, а часто и производимый с вашего согласия отбор информации и выкачивание ваших личных данных с разными целями – от таргетированной рекламы и улучшения ОС до доступа к банковским счетам и шантажа.

Что знает о нас Windows

Устанавливая распространяемое по лицензии программное обеспечение, вы заранее соглашаетесь, что поставщик и его разработчики будут получать информацию с целью некоего «улучшения продукта». Операционная система Windows собирает ваши данные вполне легально, на условиях пользовательского соглашения.

При этом вы никогда не узнаете о полном объеме и целевом назначении этого сбора и отправки информации. Но можете ограничить эти процессы.

Сохранить полную конфиденциальность вам, скорее всего, не удастся, если вы не эксперт в области операционных систем. Вы даже не сможете найти все двери, через которые прямо на ваших глазах происходит утечка. Более того, некоторые опции, касающиеся запрета на сбор информации, носят характер «кнопки вежливости» – вам позволяют что-то запретить или ограничить, но не раскрывают всех возможностей этого слива. Так вам спокойнее.

Рассмотрим возможности ограничения отправки конфиденциальных данных на серверы Microsoft и сторонних разработчиков для ОС Windows 10 на уровне простого пользователя, не имеющего специальных и экспертных знаний в области компьютерных систем и информационной безопасности. Начнем с этапа инсталляции ОС – установки Windows 10 на компьютер. Сразу оговоримся, что речь идет только о лицензионном продукте и использовании штатных средств инсталляции.

Установка Windows 10

Процесс установки начинается с выбора полной или выборочной инсталляции компонентов ОС. Поскольку возможности сбора данных о пользователе заложены по умолчанию, нам потребуется выборочный вариант, позволяющий отказаться от автоматического запуска некоторых компонентов системы.

Используем Customize setting (см. Рис.1).

При переходе ко второму этапу вы можете отключить все варианты (см. рис 2 и 3) или оставить фильтры вредоносных и фишинговых сайтов (SmartScreen). Фильтр является штатным средством, позволяющим обеспечить безопасность примерно на половине подозрительных русскоязычных страниц. Для англоязычных сайтов уровень безопасности доходит до 95%. Есть и тонкость – фильтрация работает только со штатными браузерами ОС – Edge и Internet Explorer. При установке и использовании сторонних программ этот инструмент работать не будет, и его можно с уверенностью отключить. Такая же мера применяется при использовании облачных антивирусов типа Kaspersky Lab – отключаем фильтрацию сразу, смысла в ней нет, а системные ресурсы она будет отбирать.

При отключении параметров передачи данных (рис. 3) уделите внимание разделу геопозиционирования – многие штатные и сторонние программы в ОС не могут работать корректно без данных о местоположении. Выбор за вами: либо вам придется указывать местоположение вручную, либо вы все же разрешите системе передавать эти данные.

При регистрации в системе используйте локальную учетную запись, так гораздо меньше вероятность доступа к системе при взломе ваших данных (рис. 4).

На этапе инсталляции этих действий достаточно, чтобы серьезно ограничить передачу информации о вас средствами системы. Продолжить настройку можно уже после установки. Эти же действия применимы в ситуациях, когда вы уже пользуетесь ОС и решили поднять уровень конфиденциальности.

Настройка параметров конфиденциальности в установленной операционной системе

Добраться до параметров конфиденциальности в инсталлированной ОС можно через стандартное меню ПУСК – раздел

Рисунок 2. Выбор варианта установки.

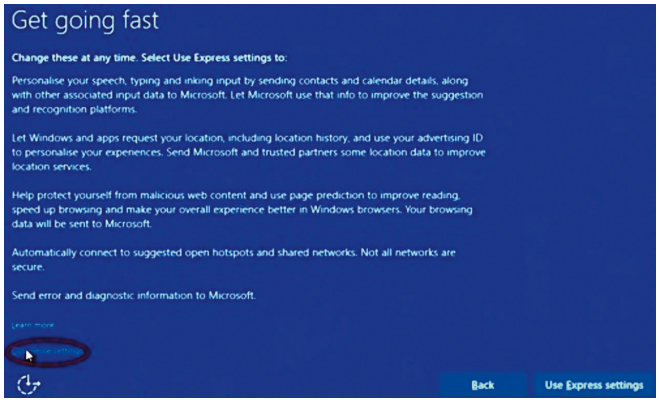


Рисунок 3. Первая часть окна настройки параметров выборочной установки

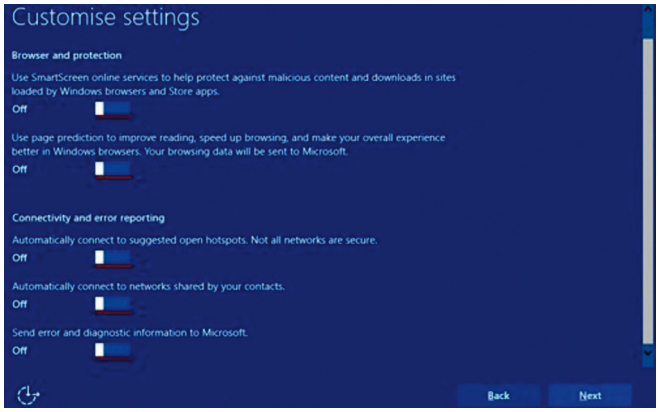


Рисунок 4. Вторая часть окна настройки параметров выборочной установки

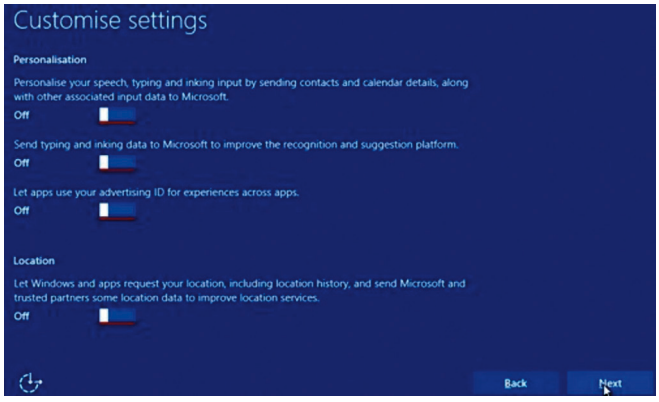


Рисунок 5. Используйте локальную учетную запись

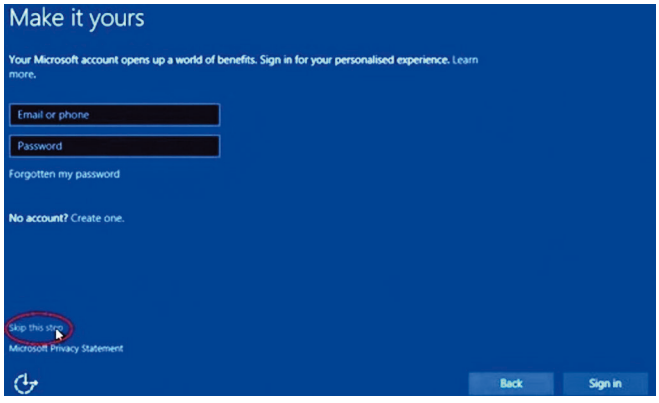


Рисунок 6. Параметры Windows 10

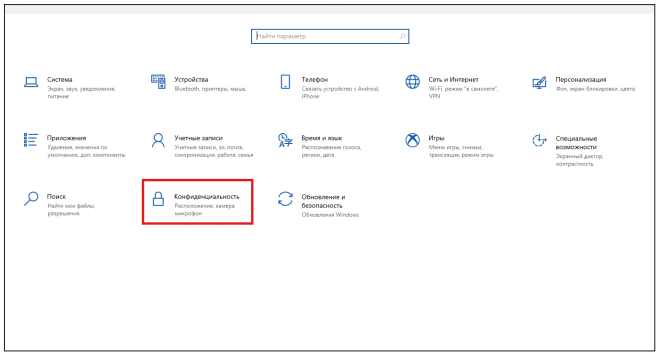


Рисунок 7. Общие параметры конфиденциальности

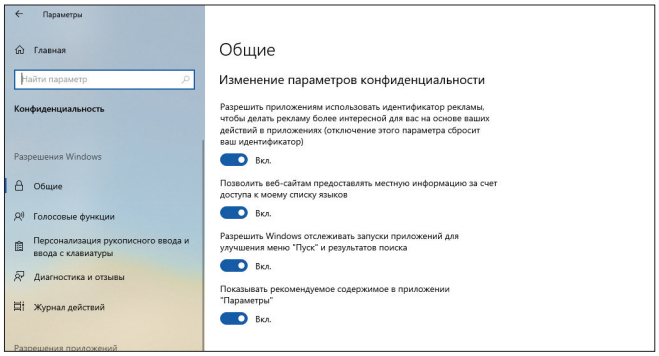


Рисунок 8. Местоположение

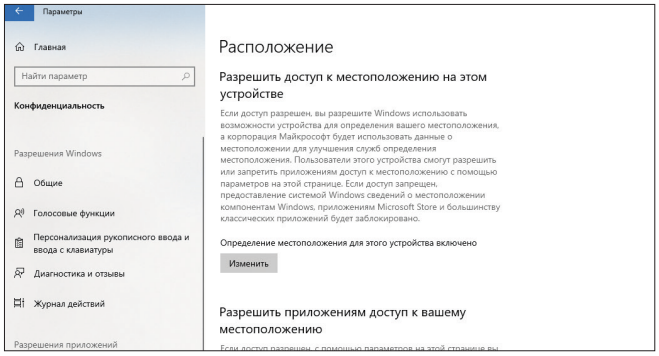


Рисунок 9. Использование местоположения приложениями

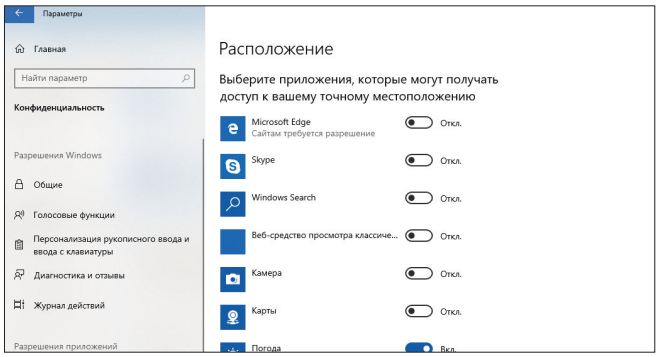
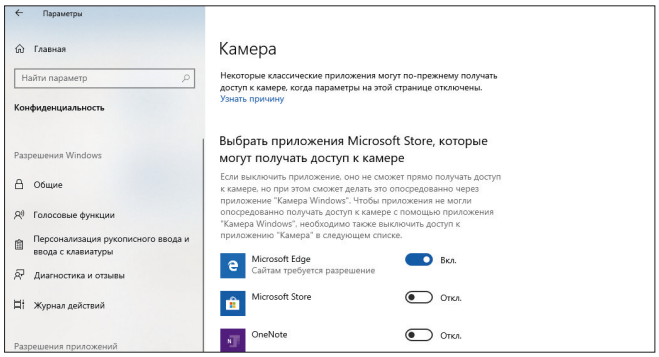


Рисунок 10. Камера



ПАРАМЕТРЫ (рис. 5) – окно ПАРАМЕТРЫ Windows – ПАРАМЕТРЫ КОНФИДЕНЦИАЛЬНОСТИ.

На рис.6 изображен экран раздела «Общие». Здесь можно отключать все. Ущерба работе системных программ, приложений и стороннего ПО это не нанесет.

Снова возвращаемся к геоданным (рис. 7), обращая особое внимание на то, что есть отдельная возможность разрешить определенным приложениям доступ к этой информации. Тем, кто знаком с настройками iOS и MacOS, рис. 8 покажется очень знакомым. Будьте внимательны, поскольку от корректных геоданных зависит работа поисковиков и других программ. Баланс конфиденциальности и корректности работы приложений вы определяете сами.

На рис. 9 показано, как можно настроить разрешение приложениям включать и использовать встроенную видеокамеру устройства или подключенный прибор для записи видео. Возможно полное отключение камеры.

Система уведомлений работает следующим образом:

- при включении камеры приложением происходит активация ее подсветки (при наличии);
- при включении камеры приложением на экран выводится кратковременное уведомление о начале использования средств видеозаписи.

В системах с корпоративной лицензией часть настроек камеры недоступна локальному пользователю. В этом случае появляется предупреждение о том, что настройки находятся под управлением организации – владельца лицензии.

Для любого пользователя – независимо от версии ОС и прочих особенностей, в списке приложений для разрешения не фигурируют встроенные, предусмотренные системной установкой программы. Они устанавливаются либо в процессе инсталляции ОС, либо из официальных источников. Для таких приложений в системных папках, по умолчанию скрытых от пользователя, уже размещены динамические библиотеки dll, а запуск их производится активацией файлов с расширением *exe. Настройка использования и режима включения камеры в них производится во встроенном меню самой программы.

Пользователю рекомендуется учитывать разницу между «классическими» приложениями и облачными – в последней версии ОС таких много. Они не расположены на локальном устройстве, их запуск происходит в облачном сервисе, поэтому некоторые настройки конкретного ПК могут ими

игнорироваться. И файлов запуска в привычном формате *exe для них не предусмотрено.

Здесь есть интересная особенность – независимо от настроек разрешения приложениям использования камеры, некоторые программы активируют ее в режиме ожидания. В этом случае не производится запись или фотосъемка, но камера уже начинает принимать сигнал. Непосредственно запись начинается только при нажатии экранных кнопок «Видео» и «Фото».

В версии ОС Windows Hello столь тонкая настройка использования камеры приложениями не работает – если вообще запретить этот параметр, камера все равно будет включаться.

На рис. 10 приведены настройки еще одного важного инструмента – встроенного или присоединенного микрофона. Тонкости аналогичны настройкам видеокамеры – список разрешений, права на использование, возможность выбора для локального пользователя или корпоративные ограничения.

Для использования голосового и рукописного ввода текстов (команд) системе потребуется не просто разрешение, а анализ индивидуальных особенностей почерка и голоса. Ведется и журнал действий, потому для строгой конфиденциальности все это стоит просто запретить и отключить, особенно в корпоративных сетях. При несанкционированном доступе (взломе) системы или канала, по которому данные уходят на сервер разработчика, в руках злоумышленника могут оказаться технические данные, по которым возможно подтверждение идентификации личности.

Серьезное отношение к сохранности данных диктует и необходимость отключения параметра «Сведения об учетной записи» – пусть эта информация не достанется никому, кроме вас! Не менее важно проанализировать список приложений, которым разрешен доступ к контактам. Если это почтовые программы и мессенджеры, то все понятно. Если это нечто иное, то возникает вопрос, кому нужны такие сведения.

• • •

Параметры конфиденциальности выбираете вы сами, исходя из собственных представлений о балансе возможностей и системных ограничений. Это вопрос вашей безопасности, и никто его за вас не решит.

Но не стоит забывать о том, что другие мощные структуры – поисковые системы и IT-корпорации собирают о вас данные в своих интересах, и информации там, в самом деле, очень много.

Если говорить о сборе и торговле персональными данными, то, в первую очередь, стоит задуматься о том, сколько интересного мы с вами отдаем такой корпорации как Google. Вы удивитесь!

Привыкайте! Вы - товар!

Личная информация давно уже покупается и продается. А мы с вами просто стали товаром. Появились биржи, которые торгуют этой информацией, и чем дальше, тем становится все сложнее. Люди постепенно привыкли к тому, что они товар. И уже вполне спокойно к этому относятся. Мы доверяем информацию о себе кому угодно. Компьютеры, планшеты, смартфоны, облака…

Люди постепенно привыкли к тому, что они товар. И уже вполне спокойно к этому относятся. Мы доверяем информацию о себе кому угодно

Давайте рассмотрим, что известно о нас на примере информации, хранящейся в нашем аккаунте Google. Эта информация доступна нам по адресу https://myaccount.google.com . Здесь вы можете проверить настройки конфиденциальности.

Настройки конфиденциальности

История приложений и веб-поиска

По умолчанию включено, используется Google Assistant, Google Maps и другими сервисами. Фактически в вашем аккаунте хранятся сведения о ваших действиях на сайтах и в приложениях Google, включая поисковые запросы и связанные данные, например, информация о местоположении. Google также сохраняет сведения об используемых приложениях, историю браузера Chrome и данные о том, какие сайты вы посещали.

Благодаря этому работают такие функции, как автозаполнение при поиске, а также персональные рекомендации в Картах, Ассистенте и других сервисах Google.

При желании вы можете изменить эти настройки.

Как включить или отключить историю приложений и веб-поиска

На компьютере

1. Откройте страницу Отслеживание действий https://myaccount.google.com/activitycontrols/search на компьютере. При необходимости войдите в аккаунт Google.

2. Включите или отключите историю приложений и веб-поиска.

3. Если функция включена, вы можете установить флажок «Добавлять историю Chrome, а также данные о действиях в приложениях и на сайтах, использующих сервисы Google».

Примечание. В некоторых браузерах и на отдельных устройствах могут использоваться дополнительные настройки, которые влияют на отслеживание действий.

На Android

1. На телефоне или планшете Android откройте настройки Google – Аккаунт Google.

2. Нажмите Данные и персонализация.

3. В разделе «Отслеживание действий» выберите История приложений и веб-поиска.

4. Включите или отключите историю приложений и веб-поиска.

5. Если эта функция включена, будет доступен параметр «Также сохранять историю Chrome и данные о действиях на сайтах, в приложениях и на устройствах, которые используют сервисы Google». Установив флажок рядом с этим

параметром, вы можете затем указать, должна ли сохраняться история действий в приложениях на вашем телефоне или планшете.

6. Установите или снимите флажок. В Истории приложений сохраняются сведения о действиях в сторонних приложениях, установленных на этом устройстве (необязательно).

Естественно, вы можете удалить все эти данные как вручную, так и автоматически. Правда насколько вам от этого будет легче, ведь эти действия все равно вы сможете сделать только после того. Да, учтите, что история поиска ведется не только в браузере, но и в других сервисах, например, YouTube. Об этом, как правило, не задумываются. Вместе с тем стоит помнить, что у вас хранится не только история поиска YouTube, но и история просмотров YouTube.

История местоположений

История местоположений связана с аккаунтом Google. В ней сохраняются данные о том, где вы побывали со своими устройствами, на которых:

- выполнен вход в аккаунт Google;
- включена история местоположений;
- разрешена отправка геоданных.

Вы сами выбираете, какие данные будут сохраняться. Проверить список посещенных мест, а также отредактировать или удалить историю местоположений можно в хронологии Google Карт

Если история местоположений включена, вам доступны дополнительные возможности в сервисах Google: персонализированные карты, рекомендации с учетом посещенных мест, помощь в поиске своего телефона, сведения о загруженности дорог и более актуальные рекламные объявления.

По умолчанию история местоположений отключена. Ее запись можно приостановить в разделе Отслеживание действий.

Вы сами выбираете, какие данные будут сохраняться. Проверить список посещенных мест, а также отредактировать или удалить историю местоположений можно в хронологии Google Карт.

Примечание. Некоторые из перечисленных здесь действий можно выполнить только на устройствах с Android 8.0 и более поздних версий.

Рисунок 1. Google Аккаунт

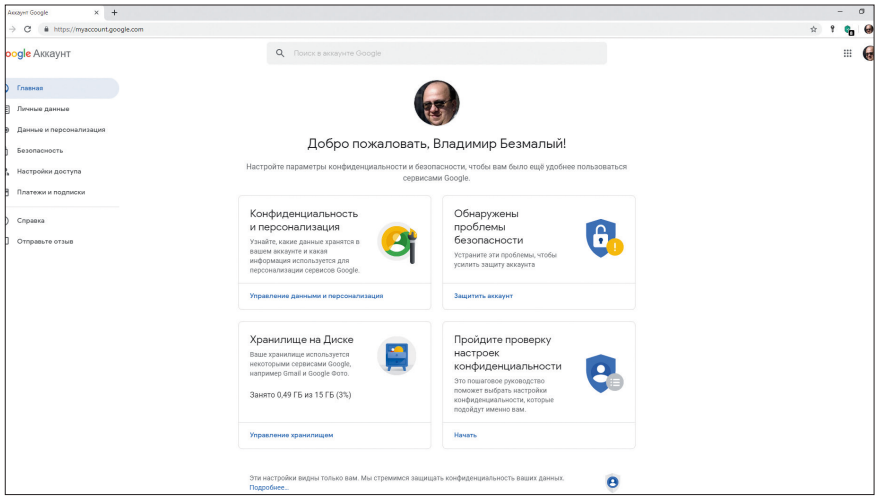
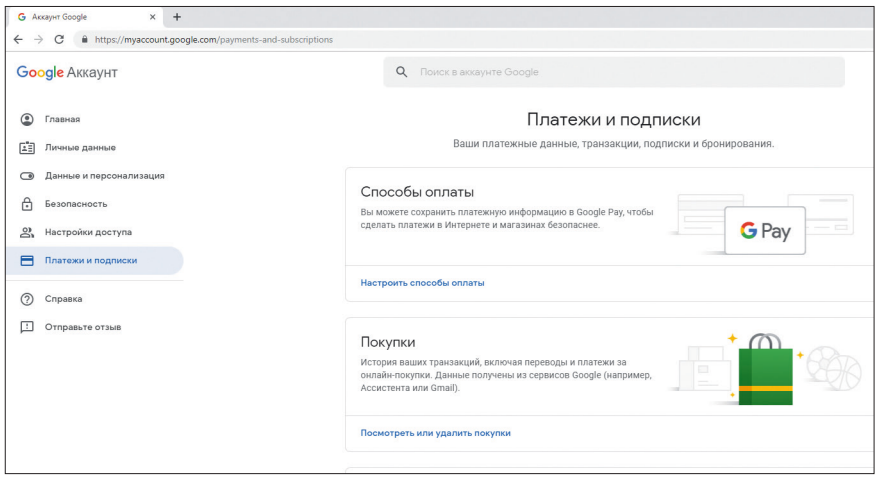


Рисунок 2. Платежи и подписки



Информация с устройств

Функция «Информация с устройств» сохраняет копии определенных данных с телефонов и планшетов. Она сохраняет следующее:

- контакты;
- календари;
- приложения;
- музыку;
- сведения об устройстве (например, уровень заряда батареи).

Эта информация конфиденциальна. Она доступна вам только после входа в аккаунт Google.

Как посмотреть или удалить информацию с устройств

1. Откройте страницу Аккаунт Google.
2. На панели навигации слева нажмите Данные и персонализация.

3. В разделе «Отслеживание действий» выберите пункт Информация с устройств.

4. Нажмите Управление историей.

5. Чтобы удалить все данные, в правом верхнем углу экрана нажмите на значок «Еще»-Удалить все.

Информация об устройстве

К информации об устройстве относятся сведения о текущем состоянии экрана, уровне заряда батареи, качестве подключения по Wi-Fi или Bluetooth, данные с сенсорного экрана и датчиков, а также отчеты о сбоях.

Кроме всего прочего, вы храните историю платежей и бронирования (рис.2).

На данной странице вы можете настроить способы оплаты, то есть сохранить платежную информацию в Google Pay, посмотреть историю покупок, а также проверить информацию о подписках и бронировании.

Однако все ли это? Нет, конечно. Есть еще Android, а там все гораздо интереснее.

Итак, начинаем с самого простого.

Статистика использования смартфона Google: Digital Wellbeing

В настоящее время доступно в Android Pie, только на Pixel.

Для запуска необходимо загрузить из Google Play. Далее приложение доступно через настройки. В частности, доступен ежедневный обзор, уведомления, круговая диаграмма: время использования приложения.

Digital Wellbeing: Что хранится

На экране приложения отображается:

> Сколько времени вы проводили в каждом приложении

Ежедневные отчеты:

> Пользовательские таймеры
> Только для одного приложения
> Нет категорий!
> Только на этом устройстве

Нет облачной синхронизации!

Знает ли при этом Google меньше? Нет, конечно.

Следует учесть, что ваш смартфон под управлением Android отслеживает ваши маршруты передвижения. При этом высока точность отслеживания, эффективно используется батарея. Отслеживание постоянно работает, если явно данная функция не отключена. Но самое интересное, что она иногда работает, даже если явно отключено https://www.bbc.com/news/technology-45183041 https://www.macrumors.com/2018/08/13/google-location-history-disabled-still-stores-data/

Ну, а теперь самое интересное. Кто отслеживает ваше местоположение?

> Google (iOS, Android, ПК – Chrome, сервисы Google в любом браузере)
> Apple (iOS, macOS)
> Facebook (на всех платформах)
> Сервисы и приложения третьих сторон
> Да, это возможно, если геолокация выключена

ДА! ЭТО ВОЗМОЖНО!

Для чего Google, Apple, FB отслеживают ваше местоположение?

В первую очередь, чтобы лучше вас обслуживать в таких сервисах, как:

> Google / Apple Maps, навигация
> FB: местные группы и события
> Гораздо более релевантные результаты поиска
> Найти мой телефон / Найти мое устройство
> Удобство: знаете, как работает этот ресторан в это время дня или даже прямо сейчас
> Внутренняя навигация

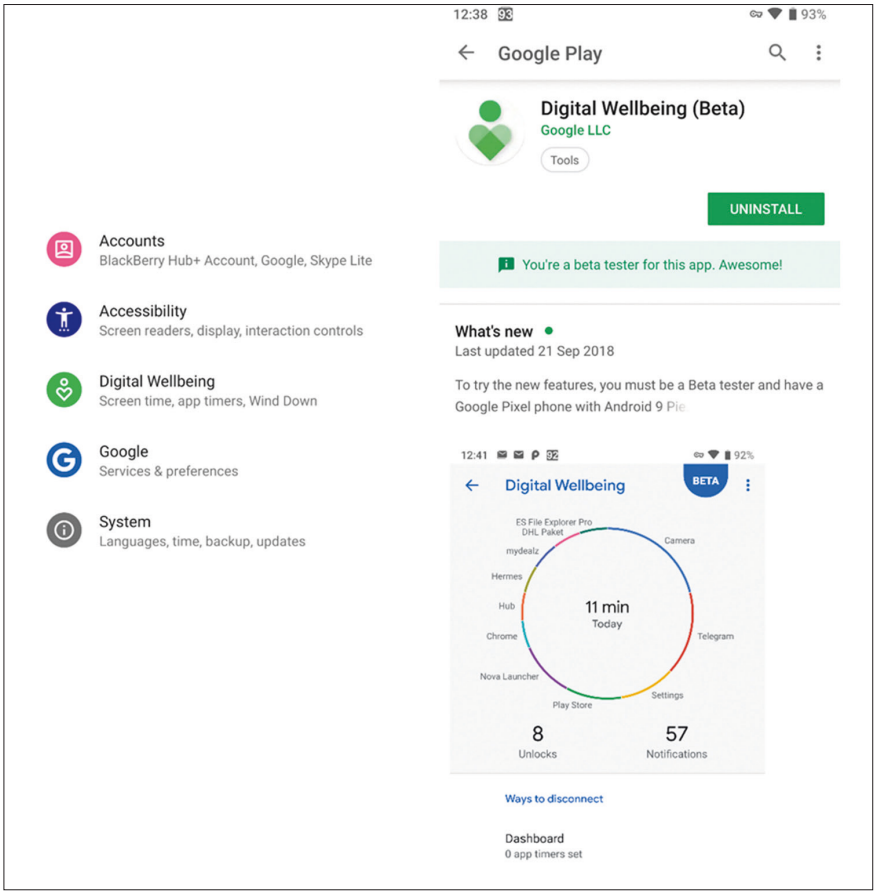
Чтобы продать рекламу

> Основной источник дохода Google объявления на основе местоположения
> Facebook: главная рекламная сеть

Чтобы продать свои данные

> Apple и Google не продают данные о местоположении
> Facebook продает

Рисунок 3. Google: Digital Wellbeing



Сегодня практически все смартфоны при фотографировании сопровождают фотографии EXIF-метками. Эти метки затем можно прочесть как в Windows, так и MacOS

Но разве это все? Нет! Кроме всего прочего сбор геоданных осуществляется приложениями сторонних производителей.

Что собирают приложения третьих сторон? Сбор местоположений, контактов, шаблонов использования телефона и многое другое.

Вы действительно считаете, что игра свободная и бесплатная? Вспомните знаменитую игру Angry Birds. Бесплатная игра? Да. Вот только 1200 раз в неделю она передавала неизвестно кому данные о местоположении игрока. Бесплатная, да?

Как торгуют подобными данными?

> Несколько брокеров покупают такие данные
> Данные о местоположении, собранные повсюду
> Включая сети Wi-Fi и обратный поиск BSSID
> Даже IP-адрес, используемый в качестве источника данных местоположения

Где хранятся геоданные?

Перечень хранилищ достаточно широк:

> Физические устройства (iOS, Android, Windows, macOS X, другие системы)
> Apple iCloud
> Google account
> Облачные хранилища третьих производителей
> Социальные сети
> Приложения Health & fitness
> Instant messengers
> Приложения для знакомств
> Приложения такси
> Приложения для путешествий

EXIF

Сегодня практически все смартфоны при фотографировании сопровождают фотографии EXIF-метками.

Эти метки затем можно прочесть как в Windows, так и MacOS.

> Windows: Свойства файла – Подробно - GPS
> macOS: More Info > Latitude and Longitude
> Третьи производители могут записывать данные
> С помощью ПО для расследования можно извлечь EXIF теги, геоданные, построить маршруты

Стоит учесть, что:

> Android собирает значительно больше данных, чем iOS.
> Google собирает значительно больше информации, чем Apple
> Эти утверждения не эквивалентны
> Android-экосистема, по-видимому, построена для отслеживания
> Каждое второе приложение в магазине Google Play отслеживает ваше местоположение
> Даже с отключенным местоположением
> Даже без разрешения на размещение
> Все приложения для Android имеют доступ в Интернет
> Специального разрешения не требуется
> IP-адрес определяет приблизительное местоположение
> Позволяет сканировать ближайшие Wi-Fi-сети

Рисунок 4 .Digital Wellbeing

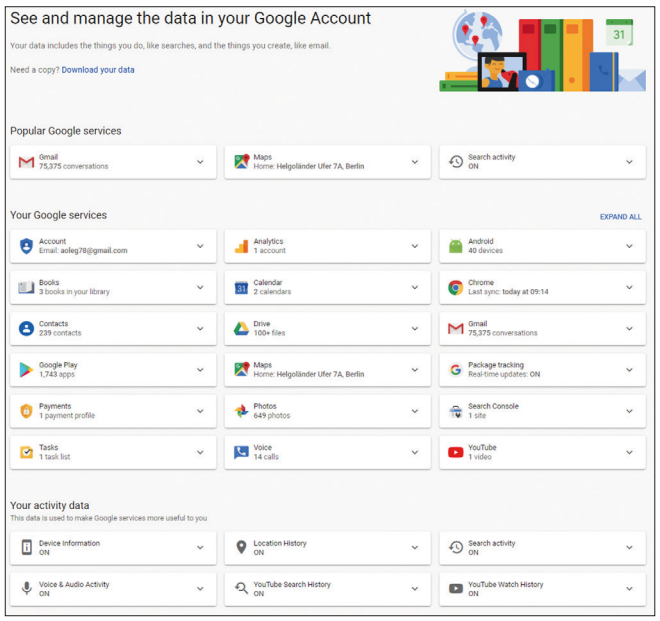
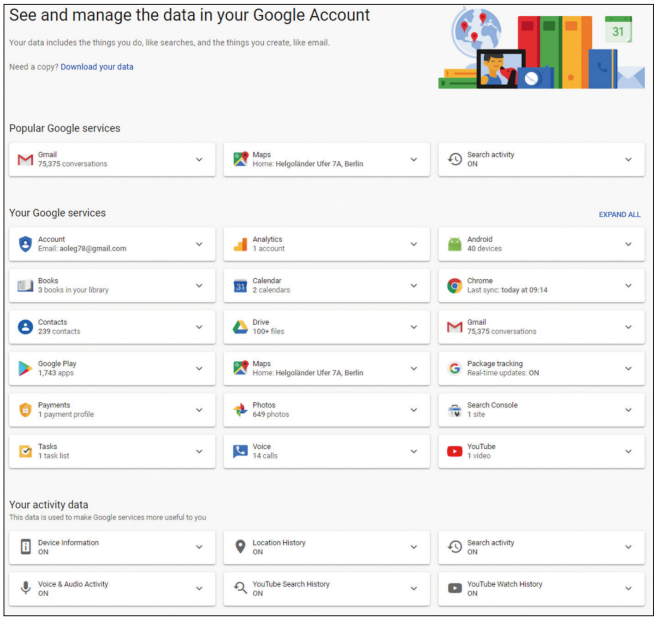


Рисунок 5. Данные в Google Account



- Все приложения для Android могут получить доступ к BSSID подключенного в настоящее время Wi-Fi и
- Все приложения для Android могут сканировать поблизости точки доступа Wi-Fi
- Единый обратный поиск BSSID определяет текущее местоположение в радиусе 20 м
- Триангулирование нескольких BSSID показывает точное местоположение
- Существует множество бесплатных и коммерческих баз данных Geo-Location Wi-Fi Например, openwlanmap.org

Что еще можно извлечь из вашего Android? На самом деле очень много. В частности, можно выяснить, как часто и кому вы звоните, а зная это, можно определить ваш круг общения и задачи, над которыми вы работаете.

Отдельно хотелось бы упомянуть голосового помощника Google. Не так давно по сообщению агентства Associated Press (AP), компания была вынуждена признать, что сотрудники корпорации Google регулярно прослушивают голосовые команды, которые пользователи отдают смарт-динамику Google Home или приложению Google Assistant. С таким признанием выступил в официальном блоге Google менеджер по продукции компании Дэвид Монсис.

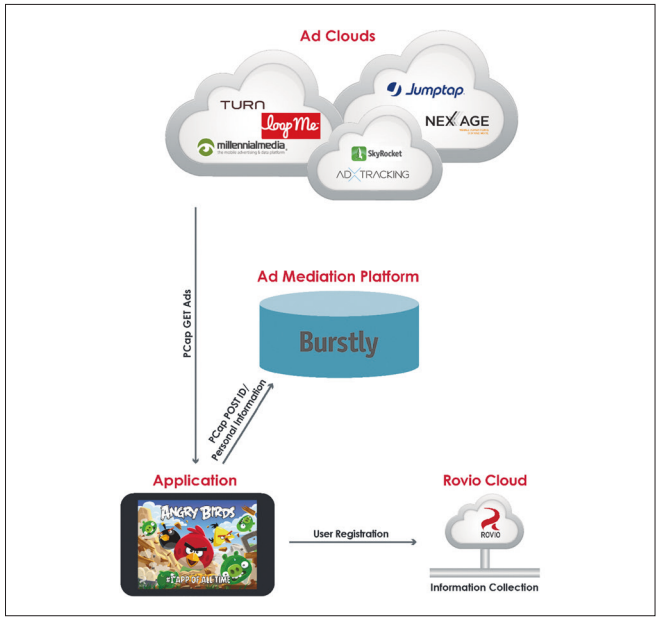
На такой шаг компания вынуждена была пойти после того, как около тысячи голосовых команд, отданных пользователями приложений или смарт-динамиков Google, оказались в доступе бельгийского телеканала VRT. По информации AP, некоторые из них содержали личную информацию о пользователях, а также разговоры, звучащие на заднем плане. Записи были в нарушение правил компании переданы телеканалу одним из экспертов по распознаванию речи, работающим с носителями голландского языка. По словам менеджера Google, компания проводит расследование инцидента и примет все соответствующие меры.

Вы еще используете голосового помощника или умные колонки от Google? Вас устраивает то, что вас слушают, а возможно, когда колонка обзаведется видеокамерой, за вами будут еще и смотреть?

Как видите, данных о вас Google знает не просто много, а очень и даже очень-очень много.

Но основная проблема даже не в том, что корпорация много знает. Основная проблема в том, что смартфоны под Android – крайне дырявы. А значит, ваши данные в опасности!

Рисунок 6 Передача данных приложениями



Вы еще используете голосового помощника или умные колонки от Google? Вас устраивает то, что вас слушают…

Вместе с тем хотелось бы, чтобы читатели понимали, что в облаке Google реально гораздо больше содержится данных, чем в самом аппарате. И если сам аппарат легко сбросить или вычистить конкретные данные, то с данными в облаке так легко не получится. Для «добывания» данных из облака уже сегодня существует ПО таких производителей как российские Elcomsoft, Oxygen Forensic, израильский Cellebrite и еще нескольких. EOF

[1] WannaCry Ransomware Attack: What You Need to Know https://www.acronis.com/en-us/blog/posts/wannacry-ransomware-attack-what-you-need-know

[2] New MassMiner Malware Targets Web Servers With an Assortment of Exploits https://www.bleepingcomputer.com/news/security/new-massminer-malware-targets-web-servers-with-an-assortment-of-exploits/

[3] How do I enable or disable JavaScript in my browser? https://www.computerhope.com/issues/ch000891.htm

[4] Windows 10 и персональная информация Владимир Безмалый https://www.osp.ru/winitpro/2017/02/13051418/

[5] Privacy Concerns Over Windows 10 https://www.bralin.com/is-windows-10-private

[6] Настройки приватности в Windows 10 Владимир Безмалый https://www.itweek.ru/security/article/detail.php?ID=176343

[7] https://myaccount.google.com

[8] Антикриминалистика: как защитить смартфон на Android Oleg Afonin https://blog.elcomsoft.com/ru/2019/07/antikriminalistika-kak-zashhitit-smartfon-na-android/

[9] Насколько безопасен современный Android? Oleg Afonin https://blog.elcomsoft.com/ru/2019/06/naskolko-bezopasen-sovremennyj-android/

[10] Google призналась, что ее сотрудники слушают записи пользователей голосовых помощников https://tass.ru/obschestvo/6657435?fbclid=IwAR1o--Ku7F8V5JjQUEKrsNYc0GOW-AF1Pk048RoSp9wZQk7sA1vJ_2LAzOw

Ключевые слова: персональная безопасность, Интернет, информационная безопасность, геоданные, IoT, stalkerware, Windows 10, Конфиденциальность, Персональные данные, Местоположение, Настройка конфиденциальности, Настройка параметров приложений, Конфиденциальность профиля, История поиска, История местоположения, Геоданные, Android, Digital Wellbeing