Вы собрались использовать менеджер паролей? Задумайтесь!

С одной стороны – я считаю что использовать менеджер паролей и включать двухфакторную аутентификацию для каждого сайта, который ее предлагает это необходимо, но с другой, понимаю, что то, что защищает одного может навредить другому. Все люди разные, обладают разными навыками и знаниями в области информационной безопасности. И я понимаю, что эксперты дают те или иные советы, но они не могут РЕШАТЬ за вас! Вы и только вы сами определяете, будете вы использовать те или иные технологии или продолжите все делать вручную.

Если вы не поняли, что это такое, **менеджеры паролей — это программы, которые запоминают для вас пароли** вместе с адресом электронной почты или другим идентификатором пользователя, который вы используете для каждой учетной записи**. Они упрощают использование *надежных* паролей**: достаточно случайных, длинных и разных для всех ваших учетных записей. Они также **облегчают потерю всех ваших паролей одновременно**, или кражу злоумышленником всех ваших паролей одновременно.

Для начала поговорим о преимуществах и рисках использования менеджеров паролей. Сегодня количество разнообразных менеджеров паролей просто изумляет. Практически в каждый основной веб-браузер встроен менеджер паролей, кроме того существует множество автономных менеджеров паролей, которые будут работать в разных браузерах. Кроме того, с помощью менеджеров паролей вы сможете вводить пароль в формы ввода. В некоторых, лучших из них, встроены генераторы случайных паролей, тем самым гарантируя что вы не будете использовать легко угадываемые пароли или повторно использовать одни и те же пароли. Некоторые даже смогут находить повторно используемые пароли и помогут их заменить.

Менеджеры паролей помогают защитить ваши пароли

Если вы не поленитесь, то с помощью менеджера паролей вы сможете создать надежный уникальный пароль для каждой службы, которую вы используете, и избавить вас от необходимости вводить эти пароли.

Менеджеры паролей могут предотвратить атаки с повторным использованием паролей, при которых злоумышленники взламывая веб-сайт, воруют с него адреса электронной почты и пароли пользователей и пытаются войти на другие сайты, используя украденные ими пары электронной почты и пароля. Атаки работают, потому что многие люди повторно используют один и тот же пароль на нескольких сайтах. Менеджеры паролей позволяют легко и просто использовать разные случайные пароли для каждой учетной записи - по крайней мере, после того, как вы заменили все свои старые повторно используемые пароли. Очень важно заменить ваши старые пароли важен, потому что, если вы оставите все свои старые пароли на месте то такая атака становится весьма вероятной.

Менеджеры паролей могут предотвратить фишинг на сайтах-мошенниках. Мошеннический веб-сайт выглядит как веб-сайт, на котором у вас есть учетная запись. Ведь он предназначен для того, чтобы обманным путем заставить вас ввести свой пароль учетной записи. Менеджеры паролей защищают вас от этих атак, потому что они не будут вводить ваш пароль, если вы находитесь на сайте злоумышленника.

Менеджеры паролей могут подвергать риску пароли

Увы, кажется старая пословица о хранении всех ваших яиц в одной корзине относится к менеджерам паролей; да, вы можете сосредоточиться на защите этой корзины, но для того, чтобы потерять все яйца, достаточно одной ошибки. (Если мысль о том, что вы рискуете всеми своими паролями одновременно, заставляет вас прекратить чтение и отказаться от менеджеров паролей сейчас, не делайте этого! В следующем разделе я попробую объяснить, как менеджеры паролей могут быть полезны, даже если вы не доверяете им все ваши пароли.)

Как вы можете потерять все пароли в менеджере паролей одновременно?

Вы можете забыть мастер-пароль, который защищает ваши пароли. После того, как вы заменили свои пароли случайными паролями и полностью полагаетесь на свой менеджер паролей, чтобы ввести их за вас, вы вряд ли сможете вспомнить многие из них. Более того - первоначально продажа менеджеров паролей заключалась в том, что вы не должны их помнить! Если вы потеряете главный пароль, который менеджер паролей использует для защиты других ваших паролей, вы можете потерять все. В некоторых менеджерах существуют варианты восстановления, но ни один не идеален.

Атака на ваш менеджер паролей может раскрыть все ваши пароли. Даже если вы заблокировали менеджер паролей, злоумышленник сможет получить к нему доступ, когда вы в следующий раз разблокируете его на этом устройстве.

- Если ваш личный ноутбук заражен вредоносным ПО, и вы используете на нем свой менеджер паролей, вредоносное ПО может прочитать каждый сохраненный вами пароль.
- Если вы используете диспетчер паролей на рабочем компьютере, любой, кто имеет административный доступ к этому компьютеру, может скомпрометировать ваши пароли в диспетчере паролей - даже для сайтов, на которые вы никогда не заходите с работы.
- Если ваш телефон украден, если вор может разблокировать ваш телефон, и если у вас не настроен менеджер паролей, требующий разблокировки при каждом использовании, вор теперь имеет доступ ко всем вашим паролям.

Напротив, если вы не используете менеджер паролей и ваше устройство заражено вредоносным ПО, злоумышленник может украсть введенные вами пароли, но не те, которые вы не используете на данном устройстве.

Вы можете решить, что некоторые пароли можно вводить на устройствах с более низким уровнем защиты, а другие следует вводить только на устройствах с более высоким уровнем безопасности.

Наконец, менеджер паролей — это еще одна часть программного обеспечения, установленная на ваших устройствах, которая может быть взломана. Все программное обеспечение содержит ошибки и, несмотря на то, разработано для удовлетворения потребности безопасности, **менеджеры паролей также могут содержать уязвимости безопасности**.

И все же, вы можете начать использование менеджера паролей

Если вышеуказанные риски не позволяют использовать менеджер паролей для *всех* ваших учетных записей, подумайте о том, чтобы начать с тех паролей, о судьбе которых вы меньше всего беспокоитесь.

Начав со своих менее значимых паролей, вы можете ознакомиться с тем, как работают менеджеры паролей, в то время как последствия ошибок невелики. По мере приобретения опыта вы также будете лучше понимать риски и выгоды. Вы можете обнаружить, что когда вам больше не нужно создавать, запоминать и вводить эти пароли с более низким значением, вы можете использовать часть этих сэкономленных усилий для защиты паролей для учетных записей с более высоким значением.

Вы также можете использовать свой менеджер паролей для генерации случайных паролей, которые не следует сохранять. Возможно, вы захотите записать их. Постепенно вы сможете выучить некоторые случайные пароли для нескольких учетных записей.

Большинство пользователей могут начать работу без покупки или загрузки нового программного обеспечения. В конце концов вы же используете браузеры, Safari или Chrome, в них есть менеджеры паролей, которые будут генерировать случайные пароли для вас.

Хотя стоит подчеркнуть, что взломать подобные менеджеры паролей достаточно легко!

Вам, безусловно, следует рассмотреть возможность использования автономных менеджеров паролей, особенно если вы храните пароли для ваших более ценных учетных записей, вы можете легко импортировать в них пароли, которые вы сохранили, используя встроенные менеджеры паролей в Chrome или Safari.

Даже если вы пытаетесь не хранить важные пароли в менеджере паролей, все равно стоит периодически проверять, какие пароли вы сохранили, а какие повторно использовали - некоторые учетные записи, которые казались бесполезными при их создании, могут со временем оказаться более ценными. Некоторые менеджеры паролей также смогут указать какие из ваших паролей явно слабые (например, если они появляются в списках общих паролей). Если вы хотите заменить свои старые пароли, объем работы может быть пугающим.

Увы, менеджеры паролей, которые проверяют, повторно ли вы использовали пароль, будут делать это только в том случае, если вы позволите им сохранить этот пароль. Если вы храните пароли только для малоценных учетных записей, менеджер паролей сможет сообщить вам, какие из ваших малоценных паролей были повторно использованы. Я не знаю ни одного менеджера паролей, который бы предупреждал вас, если вы повторно введете пароль, сохраненный для другого сайта.

Выучите надежный мастер-пароль

Большинство менеджеров паролей защищают вашу коллекцию паролей еще одним паролем, обычно называемым *мастер*- паролем. Автономные менеджеры паролей попросят вас создать мастер-пароль, когда вы начнете их использовать. Если вы используете браузер Google Chrome для хранения своих паролей и обмена ими на разных устройствах, ваши пароли будут храниться в Google и будут защищены паролем вашей учетной записи Google (наряду с любыми вторыми факторами, которые вы можете использовать). Брелок Apple iCloud Keychain полагается в первую очередь на пароли вашего устройства и функции разблокировки, чтобы регулярно защищать свои данные, но имеет запасной мастер-пароль, который называется iCloud Security Code.

Никогда не используйте повторно мастер-пароль. Мастер-пароль, который защищает все остальные ваши пароли, действительно должен быть уникальным.

Ваш главный пароль должен генерироваться случайным образом и быть достаточно **длинным** , чтобы защитить ваш пароль, даже если злоумышленники заполучат зашифрованный список паролей на веб-сайте и попытаются сломать это шифрование. Чтобы убедиться, что ваш пароль действительно случайный, сгенерируйте его с помощью вашего менеджера паролей или используйте любой другой рекомендованный метод. Главное – не забудьте его потом. Многие люди ошибочно полагают, что могут генерировать случайный пароль, вызывая буквы в уме или стуча по клавиатуре, но многие психические процессы, которые мы считаем случайными, на самом деле не являются случайными. Хороший менеджер паролей будет использовать криптографический генератор случайных чисел, чтобы гарантировать, что ваш пароль достаточно случайный.

Ваш мастер-пароль должен содержать не менее 12 строчных букв или пять слов. Зачем использовать строчные буквы или слова, если вам, вероятно, сказали (и принуждали) использовать заглавные символы и символы в прошлом? Если вам необходимо ввести пароль на устройстве с помощью экранной клавиатуры (например, телефона), каждая буква или символ в верхнем регистре могут потребовать дополнительных нажатий клавиш. Вы можете получить такую же защиту и избавить себя от многих неприятностей, сделав свой пароль в нижнем регистре всего на 30% длиннее, чем если бы вы использовали большие и маленькие буквы. Другими словами, случайно сгенерированный 13-значный пароль в нижнем регистре, который можно ввести с помощью 13 нажатий клавиш, так же безопасен, как и 10-значный смешанный пароль, который может потребовать гораздо больше усилий для ввода.

Не ожидайте, что вы запомните немедленно новый мастер-пароль - очень немногие могут выучить длинную случайно сгенерированную строку за один присест. Скорее, лучший способ запомнить свой мастер-пароль — это записать его и часто использовать. Вместе с тем, не думайте, что вы не потеряете свою бумажную копию мастер-пароля, пока не запомните, или что вы не забудете позднее ваш мастер-пароль.

Фактор восстановления в выборе менеджера паролей

Поскольку одно из самых больших различий между менеджерами паролей заключается в процессе восстановления ваших данных, в случае утери мастер-пароля, вы не должны выбирать менеджер паролей без исследования процесса аварийного восстановления. После того, как вы сделаете свой выбор, первое, что вы должны сделать, наряду с выбором главного пароля, — это настроить процесс восстановления. Он может понадобиться вам очень скоро, поскольку вы, скорее всего, забудете мастер-пароль вскоре после его создания и до того, как узнаете его при повторном использовании.

Вместе с тем признаюсь, я использую парольный менеджер, в котором нет процедуры восстановления утраченного мастер-пароля. Это неудобно, скажете вы. Согласен, неудобно, зато наиболее безопасно и приучает пользователя помнить! Впрочем, вам самим выбирать, нужно ли вам восстановление или вы готовы пожертвовать этим процессом, но зато быть в полной безопасности.

Хотя последствия утери ваших паролей могут казаться незначительными и у вас еще нет сохраненных паролей, которые вы можете потерять, вы можете быстро стать зависимым от вашего менеджера паролей. Вы можете ошибочно предположить, что, узнав свой пароль, вы никогда его не забудете. Хотя чаще всего забывают пароли вскоре после их создания, также часто забывают их после периода неиспользования

Почему каждый продукт обрабатывает восстановление по-своему? Отчасти потому, что это действительно сложная проблема даже для компаний, которые являются одними из крупнейших в мире, лучше финансируемыми и известными благодаря своему удобству использования. Рассмотрим iCloud от Apple, в котором хранится цепочка для ключей iCloud, используемая Safari. Один из способов восстановить учетную запись iCloud - через службу поддержки клиентов, но хакеры обманным путем скомпрометировали учетные записи пользователей, в том числе высокопоставленного репортера в 2012 году. Таким образом, Apple также предложила пользователям возможность хранить случайно сгенерированный пароль для восстановления (Apple называл его Ключом Восстановления) и настраивать свои учетные записи таким образом, чтобы служба поддержки клиентов не смогла изменить ваш пароль. Немногие пользователи приняли эту технологию, и некоторые из них были расстроены, когда обнаружили, что, по сути, служба поддержки клиентов больше не может помочь им, когда им это нужно. Apple перестала предлагать ключи восстановления в 2015 году. В настоящее время Apple позволяет сбрасывать

пароли после проверки клиентов по номеру телефона , несмотря на то, что этот процесс весьма уязвим для атаки .

Вместо того чтобы полагаться на непрозрачные правила поддержки клиентов, многие менеджеры паролей используют решения, которые менее уязвимы для атаки, но более уязвимы для случайной потери.

Менеджеры паролей с открытым исходным кодом KeePass и PasswordSafe предоставляют вам возможность найти и сохранить файл с вашими паролями, а также ключ, используемый для защиты (шифрования) данных в этих файлах. Итак, если вы хотите поделиться своими паролями между компьютерами, вам необходимо создать учетную запись для хранения файлов в Интернете (например, DropBox). Ваша резервная копия может быть письменной копией главного пароля и пароля для учетной записи общего доступа к файлам. Если вы используете двухфакторную аутентификацию для этой учетной записи, вам также потребуется резервная копия.

LastPass , Keeper и Dashlane позволяют предварительно авторизовать экстренные контакты для доступа к вашей учетной записи при условии, что они также имеют учетную запись с тем же менеджером паролей. Это требование выполняется, потому что эти продукты используют криптографию, чтобы ваши друзья, но не компании, могли получить доступ к вашим данным. Это помогает защитить вас, если их сервис взломан или злоумышленник успешно выдает себя за персонал службы поддержки. Недостатком является то, что злоумышленник, который скомпрометирует учетную запись вашего контакта, может затем скомпрометировать вашу. Вы можете уменьшить вероятность того, что это произойдет, установив задержку до того, как ваша информация будет передана вашему экстренному контактному лицу. Если вы знаете людей, использующих один из этих продуктов, которым вы доверяете в качестве экстренного контакта, этот продукт может оказаться для вас лучше, чем те, которые не используют ваши контакты.

С 1Password ваш главный секрет на самом деле состоит из двух частей: секретный ключ, который программное обеспечение хранит на каждом устройстве, на котором вы установили свои пароли, и ваш главный пароль. Чтобы использовать новое устройство с 1Password, вы должны передать ему свой секретный ключ. Вы можете сделать резервную копию своего секретного ключа, создав «аварийный комплект», PDF-файл, который вы можете распечатать, который содержит ваш секрет и место для записи вашего мастер-пароля. Как и LastPass и Dashlane, 1Password разработал свой онлайн-сервис таким образом, чтобы они не хранили эти секреты и чтобы служба поддержки клиентов не могла помочь злоумышленнику - или вам - получить доступ к вашим данным без них. В отличие от LastPass и Dashlane, процесс их восстановления не требует взаимодействия со службой или кем-либо еще. Это делает 1Password возможно самым приватным вариантом, но каждый клиент, обладающий таким уровнем конфиденциальности, платит за это: 1Password не может знать, какая часть клиентов распечатала наборы для восстановления, сколько их успешно использовало и сколько навсегда утратило свои пароли. Единственные данные, которые они получают, чтобы помочь им повысить надежность процесса восстановления, поступают от добровольных пользователей, если они обращаются в службу поддержки.

Если вы используете Chrome с учетной записью Google и двухфакторной аутентификацией, вы можете получить десять одноразовых паролей восстановления (восьмизначные числа, которые они называют резервными кодами), которые могут заменить один из двух ваших факторов. Google рекомендует вам «распечатать или загрузить» их. Google также хранит эти коды, и поэтому, в отличие от правильно управляемых случайно сгенерированных паролей, ваши коды могут быть скомпрометированы, если кто-то взломает вашу учетную запись Google.

Если вы используете распечатанный секрет восстановления с помощью Chrome или 1Password или создаете свой собственный для KeePass или PasswordSafe, вам нужно будет решить, где хранить секреты восстановления после их печати. Может подойти сейф, особенно если он у вас уже есть.

Нет технической причины, по которой вы не могли бы делиться распечатками ваших секретов восстановления с друзьями. В противном случае вы можете не захотеть, чтобы на листе было указано, для кого он предназначен, поскольку исключение этого факта может обеспечить небольшую защиту в случае кражи. Другой вариант - дать двум доверенным контактам половину кода или три доверенных контакта по две трети каждого кода (чтобы любые два контакта могли вам помочь).

Если вам не нравится какой-либо из перечисленных выше вариантов, вы можете периодически распечатывать все свои пароли или записывать их. Если вы печатаете, вы будете полагаться на то, что ваш принтер защищен.

Ваш основной пароль электронной почты также требует особого внимания при планировании стратегии восстановления, поскольку многие другие пароли могут быть сброшены по электронной почте. Это может быть самый важный пароль для изменения на случайно сгенерированный пароль, но он также нужен вам. Если вы меняете этот пароль, вам следует рассмотреть возможность его записи или резервного копирования.

Тщательно продумайте, прежде чем хранить ценные пароли

На самом деле основные проблемы начинаются как только вы решите хранить пароли важных для вас сервисов. При этом ответ, который подходит для одного человека, может не подходить для другого.

Первое решение будет состоять в том, какие устройства получат доступ к вашим паролям. Учитывая, как часто вы, вероятно, используете свой телефон, и насколько болезненно набирать пароли на телефоне, вы, вероятно, захотите синхронизировать свои пароли с телефоном. Если вы это сделаете, все ваши пароли теперь будут храниться на вашем телефоне. Возможно, вы захотите узнать, как быстро ваш телефон заблокируется после того, как вы перестанете им пользоваться, и какие механизмы вы позволите разблокировать. Если ваши дети или партнеры знают ваш PIN-код, доверяете ли вы им также все ваши пароли? Если люди, которым вы не доверяете, знают ваш ПИН-код, вы можете использовать автономный менеджер паролей, который имеет второй механизм разблокировки после разблокировки телефона. Готовы ли вы выполнять дополнительную работу каждый раз?

Вам придется принимать эти решения не только для вашего телефона, но и для *каждого* устройства, на котором вы вводите пароли. Для этого общего семейного планшета вам нужно будет выбрать между установкой менеджера паролей или вводом нового случайного пароля.

Вы устанавливаете свой менеджер паролей на рабочий ноутбук, к которому у всех в IT есть доступ? Если вы проводите большую часть своего времени в офисе, вы, вероятно, в конечном итоге будете выполнять много персональных вычислений на своих рабочих устройствах, даже если вы предпочитаете делать это где-то еще.

Вы устанавливаете свой менеджер паролей на устройства, которые используете только время от времени, и, таким образом, не можете получать обновления безопасности так часто, как вам хотелось бы? Как насчет ноутбуков, на которые вы устанавливаете много случайных программ? А как насчет ноутбука, на который члены вашей семьи могут также устанавливать программное обеспечение? Готовы ли вы вручную скопировать бесценные пароли, которые вам нужно использовать на этих устройствах, с устройства, которому вы доверяете?

Как ваш менеджер паролей будет взаимодействовать с вашей стратегией двухфакторной аутентификации?

Вам нужно будет решить, сохранять ли пароли для ценных учетных записей.

Как я упоминал ранее, вы можете использовать свой менеджер паролей для генерации случайных паролей для своих ценных учетных записей независимо от того, разрешите ли вы менеджеру паролей сохранять их или нет. Если вы уже запомнили надежные уникальные пароли для этих учетных записей, основной причиной их добавления в диспетчер паролей является предотвращение случайного ввода этих паролей на веб-сайты мошенников.

Чтобы получить такую защиту, ваш пароль должен быть сообщен каждому устройству, на котором установлен менеджер паролей, и разблокирован всякий раз, когда вам нужен какой-либо из ваших других паролей. Другими словами, вы должны решить, готовы ли вы компенсировать повышенный риск кражи вашего пароля из вашего менеджера паролей и устройств, на которых вы его установили, в обмен на защиту, которую вам дает менеджер паролей.

Правильный ответ зависит от того, к какой атаке *вы* более подвержены, и - позвольте мне сказать это еще раз - все люди разные.

Если вы проводите большую часть своего времени в веб-браузере и в основном используете операционные системы, которые помещают в «песочницу» все программное обеспечение (например, iOS и Android), вероятность стать жертвой мошеннического сайта может быть относительно выше, и вы можете выбрать менеджер паролей. Если частью вашей работы является оценка того, какой пакет программного обеспечения может лучше всего решить проблему, и вы проводите большую часть своего времени в Windows или MacOS, заражение вредоносным ПО может быть более вероятным.

Специфика аккаунта тоже имеет значение. Если это учетная запись, которую вы будете использовать каждый день, и вам придется печатать каждый день, то, если ваш компьютер скомпрометирован, злоумышленнику не придется долго ждать, пока вы не наберете свой пароль повторно. В этом случае сохранение пароля в вашем менеджере паролей может не увеличить риск. Если вы используете этот пароль только на самом безопасном устройстве и редко, то добавление его в диспетчер паролей может значительно увеличить риск его взлома вместе с одним из ваших устройств.

Увы, единой рекомендации для всех просто нет!

Подведение итогов

Вы можете принести больше вреда, чем пользы, если вы установите менеджер паролей, позволите ему хранить ваши старые пароли и не будете использовать функции, которые могут реально повысить вашу безопасность.

Менеджеры паролей могут защитить вас от атак на повторно используемые пароли только в том случае, если вы хотите позволить им заменить ваши старые пароли случайно сгенерированными уникальными паролями. Они также могут наилучшим образом защитить вас от случайного ввода ваших паролей на веб-сайты мошенников («фишинг»), если только они, а не вы, помнят ваши пароли для целевых учетных записей. Таким образом, если вы получаете диспетчер паролей для повышения безопасности, вам нужно позволить диспетчеру паролей заменить уже запомненные пароли случайными.

Чтобы снизить риск потери всех ваших паролей одновременно, вам понадобится надежный мастер-пароль и надежная стратегия восстановления. Выберите менеджер паролей с опцией восстановления, настройте восстановление *немедленно* и настоятельно рекомендую запомнить длинный произвольный мастер-пароль, сгенерированный вашим менеджером паролей. Вы, вероятно, не хотите хранить свои более ценные пароли, пока не запомните новый мастер-пароль (это может занять несколько недель) и не разработаете свой план восстановления: если он основан на доверенных людях, убедитесь, что они понимают и знакомы с этой ролью. Если

восстановление зависит от вашей способности хранить объект (например, напечатанный код), выберите место, в котором, по вашему мнению, безопасно его хранить.

Поскольку существует огромное количество факторов, которые необходимо учитывать и принимать перед решением использовать менеджер паролей, заранее продумайте все возможные риски его использования.

Решения, которые необходимо принять при использовании менеджера паролей

- Какой менеджер паролей я буду использовать?
- Как мне восстановить доступ к своим паролям, если я потеряю свои устройства и / или мастер-пароль?
- Как я буду хранить свой мастер-пароль, пока не запомню его?
- На каких устройствах я должен установить менеджер паролей?
- Какому из этих устройств потребуется более надежный механизм аутентификации, чтобы гарантировать, что кто-то, кто использует или украдет это устройство, не сможет получить все мои пароли?
- Какое из этих устройств нуждается в более строгих мерах безопасности для защиты от вредоносных программ, которые могут украсть все мои пароли?
- Какие из моих паролей я не должен рисковать хранить в моем менеджере паролей?
- Для каких учетных записей я должен иметь свой менеджер паролей для создания новых случайных паролей? (Не забывайте, что он может генерировать, но не хранить пароли для учетных записей, которыми вы не хотите управлять.)