??????

В настоящее время невозможно обойтись без паролей работая с компьютером (ноутбуком, планшетом, мобильным телефоном). Сами устройства просят пароли, приложения и сайты тоже просят пароли. Поэтому нужно уметь правильно работать с паролями. Об этом я и хотел немного рассказать.

???? ??? ?????? ? ???????? (? ?? ??????)

? ?????? ?? ?????

Нередко встречается мнение, что злоумышленники присматривают себе жертву среди богатых или знаменитых, а обычному человеку и бояться нечего. Это не так. Получение контроля над устройством пользователя — любым, от мобильного телефона до мощного игрового компьютера — тоже вполне себе цель злоумышленников. В последствии из взломанных и подконтрольных устройств могут быть организованы сети (или ботнеты), которые помогают преступникам осуществлять свою незаконную деятельность. Помимо этого даже на самого бедного человека можно оформить кредит в интернет банке или мобильном приложении, что вдвойне обидно — денег не было, так теперь ещё и должен банку. В наше время очень важным ресурсом являются Госуслуги, доступ к данным любого человека со стороны злоумышленника может привести к очень печальным последствиям. Есть и другие причины, по которым могут быть взломаны устройства и учётные записи самых обычных пользователей, начиная от банального баловства. Поэтому не стоит поддаваться этому мифу.

??? ?????? ????????

По сути это вариант предыдущего Я никому не нужен. Предполагается, что раз скрывать нечего, то и не нужен никому. Это тоже не всегда так, у пользователя могут быть похищены или скопированы какие-то чувствительные данные и предприняты попытки шантажа или вымогательства. Ну и остальные причины описанные в предыдущем разделе тоже имеют место быть. Не стоит поддаваться мысли, что раз нечего скрывать, то не будут взламывать. Рано или поздно будут.

?????? ??? ?????? ? ????????

Большинство ошибок при использовании паролей так или иначе связаны с мифами либо несознательностью людей. Очень часто совершается сразу несколько ошибок при работе с паролями.

??????? ??????

Пароли наподобие 1234, 12345, Password1, Pa$$word, 4321 и т.п. Их легко запомнить. Но их легко взломать или подобрать. У злоумышленников уже давно есть базы таких простых паролей. Именно по этим базам пытаются подбирать пароли в первую очередь. Таки пароли использовать нельзя.

?????? ?? ?????? ?????? ??????

Сюда можно отнести любые пароли, которые так или иначе связаны с личной жизнью — имя, фамилия, клички животных, улица, номер квартиры, любимая игра и т.п. Обычно использование таких паролей связано с тем, что человеку трудно запоминать большое количество паролей, вот он и придумывает, как упростить себе жизнь. Для усложнения пытаются использовать транслит (замена русских букв английскими), разный регистр букв, добавление цифр или символов в начале или в конце слова. Но даже в таком «защищённом» виде пароль является нестойким и может довольно быстро быть подобран, т.к. у злоумышленников есть специальные программы, которые генерируют возможные пароли на основе личных данных. Это очень упрощает взлом аккаунта.

?????????? ??????

Некоторые пользователи понимают опасность простых паролей или паролей на основе личных данных. Поэтому придумывают себе один или несколько паролей и используют их на разных сайтах. Если пароль достаточно сложный, то подобрать его действительно сложно. Но если такой пароль подобран или был украден из базы паролей какого-то сайта, то все аккаунты пользователя находятся под угрозой.

?????? ?? ?????????

Очень популярная ошибка, когда сложные пароли записываются на листочек (и прикрепляются к монитору), в тетрадку или в обычный файл. Рано или поздно такой пароль может стать известен злоумышленнику, которым может оказаться сосед, сантехник, курьер, врач и т.д. Нельзя хранить пароль в открытом виде и в лёгком доступе.

Есть и другие ошибки при работе с паролями, но эти самые распространённые. Не стоит их повторять. Мы разобрали самые популярные ошибки и мифы, связанные с паролями, самое время теперь узнать, как же правильно работать с паролями и не сломать себе голову.

???????? ? ???????? ?????????

Очевидно, что пароли должны быть сложными (большое количество символов, буквы в разном регистре, цифры, специальные символы), желательно случайными (оказывается человек не может сформировать случайные пароли) и ещё разными для каждой учётной записи. Как же быть, если сейчас столько сайтов и приложений требуют пароли — десятки сложных паролей сложно придумать, а запомнить и вовсе кажется нереальным?

???????? ???????

Правильно использовать менеджер паролей. Это специальная программа, которая помогает человеку запоминать и придумывать пароли. Менеджеров паролей существует довольно много, можно почитать обзоры в сети и выбрать себе подходящий. Существуют менеджеры паролей в составе операционной системы (например, для macOS и iOS), существуют отдельные решения, есть платные и бесплатные, есть надёжные и не очень. Менеджеру паролей нужно доверять, если есть сомнения в его надёжности, то пользоваться им нельзя.

Я пользуюсь менеджером паролей Bitwarden со своим сервером паролей. Мне такое решение видится удобным и надёжным — авторитетный разработчик, работа на всех нужных мне настольных и мобильных платформах, собственный сервер для хранения паролей.

При использовании менеджера паролей можно не запоминать большую часть паролей, но несколько паролей нужно обязательно запомнить — как минимум пароль от системы (компьютера или мобильного устройства) и пароль от самого парольного менеджера. Также может быть потребуется запомнить пароль от зашифрованного диска. Всё зависит от степени паранойи. **Важно, чтобы это были разные пароли.**

????? ?????? ???? ??????

Чем длиннее пароль, чем больше разных символов и из разного набора (буквы в разном регистре, цифры, спецсимволы) используется, чем более случайным образом сформирован пароль, тем лучше. К счастью большинство менеджеров паролей предлагаю сформировать пароль автоматически. Это очень важная и полезная функция.

В сети есть разного рода таблицы, в которых сравнивается стойкость (надёжность) пароля в зависимости от его длины и используемого набора символов. Например, пароль длиной 6 символов, состоящий из любых доступных знаков, взламывается практически моментально. Для взлома пароля из десяти таких символов потребуется 5 месяца. Пароль из 13 только строчных и заглавных букв подбирается за 1000 лет. Выглядит уже более надёжно. Но надо учитывать, что эти данные могут устаревать, т.к. техники перебора паролей усовершенствуются, как и оборудование, которое используется для взлома.

Надёжный пароль это пароль от 12 символом разного типа, но лучше больше. К сожалению не все сайты принимают пароли большой длины и с любыми символами. В таком случае придётся подстраиваться.

????????? ?????

Альтернативой паролю может быть парольная фраза. Это набор несвязанных друг с другом слов (из словаря редких слов). Для усложнения слова могут быть разделены спецсимволами, начинаться с заглавной буквы и содержать цифры. Такая парольная фраза гораздо легче запоминается. Длина фразы из 5-6 слов считается довольно надёжной.

?????

Помимо случайного пароля можно сильно затруднить жизнь злоумышленникам, если использовать случайные логины. Это особенно удобно там, где логин используется только для входа.

В качестве резюме. Надо запомнить два надёжных пароля (или проще две парольные фразы) от компьютера и от менеджера паролей. Эти пароли обязательно держать в секрете, не записывать и не сообщать никому. Если есть подозрение, что кто-то их подсмотрел, то следует их заменить (и снова запомнить). Со всеми остальными паролями должен работать надёжный парольный менеджер.

?????? ??????

Может ли что-то ещё использоваться кроме пароля? На самом деле да. Современная информационная безопасность говорит о трёх способах подтверждения того, что ты это ты — знание, владение, признак. Знание это как раз пароль. Разберёмся с двумя остальными.

????????

Если знание это то, что ты знаешь, то владение это то, что у тебя есть. Это может быть карта доступа, брелок для входа в систему (с USB разъёмом на подобие флешки), механический ключ в конце концов. Школьная карта для прохода в школу это как раз владение. Как и ключ от квартиры. Существует способ входа в систему при помощи такой карточки или USB-брелока. Из преимуществ — даже подсмотрев, как выглядит брелок, купив похожий, в систему не войдёшь. Из недостатков — брелок могут украсть, его можно потерять.

???????

Признак это то, что есть у пользователя. Это его внешность, группа крови, папиллярные узоры на пальцах, рисунок радужной оболочки и т.п. Признак нельзя передать кому-то, как это можно сделать со знанием (паролем) или владением (ключом). Часто признак сложно подделать. Наиболее популярны признаки, которые сейчас используются как замена паролю — отпечаток пальца (например, Touch ID для iPhone) и внешность (например, Face ID для iPhone). Рекомендуется использовать признак там, где он поддерживается, т.к. он позволяет реже использовать пароль.

?????????????? ???????????

Обычно это не замена паролю, а дополнение, т.е. использование вместе с паролем либо признака, либо владения, либо и того и другого.

2FA — двухфакторная авторизация — использование двух способов подтверждения личности, например, пароль и брелок доступа. MFA — использование всех трёх способов подтверждения личности. Иногда 2FA тоже называют MFA.

Часто под 2FA/MFA подразумевают подтверждение входа по SMS. Но это не совсем правда и не стоит доверять такому методу. Во-первых, номер телефона не принадлежит абоненту (только закреплён за ним). Во-вторых, есть способы подделать или клонировать SIM-карту, или попросту украсть.

??????????? ??????

Оказывается есть и такие. Одноразовые пароли (OTP, one-time password) — пароли, которые работают один раз. Некоторые банки выдают клиентам карточку с одноразовыми кодами (обычно скрытыми под стираемым слоем). При подтверждении важной операции требуется указать помимо обычного пароля ранее неиспользовавшийся код с такой карточки (обычно следующий по номеру). Это очень надёжный способ, гораздо надёжнее SMS, но требуется хранить карточку в надёжном месте.

Развитием OTP является TOTP (time-based one-time password, одноразовые пароли на основе времени). Это криптографический алгоритм, который позволяет обойтись без карточки. При создании TOTP формируется ключ, который используется специальной программой и передаётся на сервер (или сайт), на котором требуется подтверждение входя по TOTP. При входе требуется указать временный пароль, который генерирует программа. пароль действует ограниченное время (обычно 30 секунд). Этого достаточно, чтобы зайти на сайт, но такой украденный пароль фактически бесполезен. Гораздо удобнее OTP с пластиковой карточкой. Исходный ключ должен храниться в секрете. Рекомендуется использовать TOTP вместо SMS, там, где это поддерживается. Для работы с TOTP рекомендуется установить приложение на смартфон.

Revision #2
Created 2024-04-21 13:09:25 UTC by Oleg
Updated 2024-04-21 15:12:20 UTC by Oleg