kaspersky

Надежность пароля

Материал для учителя

kaspersky

Надежность пароля

Пароль – условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов, и предназначенный для подтверждения личности или полномочий. Пароли используются для защиты информации от несанкционированного доступа.

Исследования показывают, что около 40% всех пользователей выбирают пароли, которые легко угадать автоматически. Пароли, которые очень трудно или почти невозможно угадать, считаются более стойкими.

В 2013 году компания Google опубликовала список широко используемых категорий паролей, которые считаются ненадёжными из-за того, что их легко подобрать (особенно после изучения профиля пользователя в социальной сети): кличка домашнего животного, имя родственника, даты рождения и важных событий, место рождения, что-либо, связанное с любимой спортивной командой, слово «password».

Надежность пароля – это показатель эффективности пароля против угадывания или атак методом перебора. Осуществляется оценка количества попыток, которые потребуются злоумышленникам, не имеющим прямого доступа к паролю, чтобы правильно его подобрать. Надежность пароля зависит от длины, сложности и непредсказуемости.

Эффективность пароля заданной надежности в значительной степени определяется конструкцией и реализацией факторов аутентификации. Скорость, с которой злоумышленник может передавать системе угаданные пароли, является ключевым фактором в определении безопасности системы. Некоторые системы вводят тайм-аут продолжительностью в несколько секунд после небольшого количества неудачных попыток ввода пароля.

Каким должен быть «надежный» пароль?

К паролям есть два требования, которые могут показаться не совместимыми. С одной стороны, чтобы надежно защитить учетную запись, нужно придумать пароль, который будет трудно подобрать. С другой стороны, этот пароль должно быть легко запомнить, иначе им невозможно будет пользоваться. Регулярная смена паролей отчасти помогает с первым требованием, но второе делает трудновыполнимым. Но, на самом деле, постоянно менять пароли не так уж эффективно. Гораздо лучше использовать надежные и уникальные комбинации символов.

Утечки данных случаются регулярно, и пароли попадают в руки злоумышленников – как пользователь вы ничего не можете с этим поделать. Если же везде используется один и тот же пароль, то всего одна утечка – и все личные аккаунты будут под угрозой.

Каким должен быть пароль, чтобы его можно было назвать «надежным»? Принципиально важны два простых правила. Во-первых, в нем нужно использовать как можно более разнообразные символы. Во-вторых, пароль должен быть длинным – и чем длиннее, тем лучше.

Надежный пароль вовсе не должен быть случайным набором символов. Случайные комбинации, несомненно, хороши с точки зрения безопасности, но запоминать их – проблема. Лучше придумать легко запоминающийся пароль, минимум 12 символов.

К примеру, пароли

12345-vyshel-zaychik-naprimer

?Y]G9gWJ48zYkFBc@{nKw!'q

обладают близкой надежностью, так как первый пароль компенсирует все свои недостатки большей длиной.

Способы украсть пароль

Многие считают, что киберпреступники смогут заполучить пароль, только если пользователь совершит ошибку – скачает и запустит непроверенный файл, откроет документ от неизвестного отправителя или введет свои учетные данные на сомнительном сайте. Да, все это действительно упрощает жизнь злоумышленникам, но на самом деле в их арсенале гораздо больше способов для захвата учетных записей.

Самые распространенные схемы:

- **Вредоносное ПО.** Существенную часть активных зловредов составляют трояны-стилеры. Они ждут, когда пользователь зайдет на какой-нибудь сайт или сервис, копируют введенный им пароль и отправляют своему владельцу. Если не пользоваться защитными решениями, то такие трояны могут годами скрываться в системе. Их трудно заметить, поскольку они тихо занимаются своим делом, не причиняя видимого вреда. Иногда киберпреступники внедряют в сайты веб-скиммеры, которые собирают всю информацию, вводимую пользователями (имена, данные учетных записей и банковских карт и т.д.).
- **Публичный Wi-Fi.** Злоумышленники могут перехватить данные (в том числе пароли), отправляемые по сети, если использовать сеть Wi-Fi без шифрования или защищенную старым протоколом WEP. Другой вариант кражи: хакер создает точку Wi-Fi с открытым доступом, используя название, похожее на существующую сеть. Не замечая разницы, пользователи подключаются к фальшивой точке – и весь их интернет-трафик оказывается под контролем злоумышленника. Избежать таких утечек можно, если внимательно проверять названия сетей, не пользоваться сомнительными точками доступа и не позволять устройствам подключаться к беспроводным сетям автоматически.
- **Фишинговое письмо.** Это один из тех подходов к краже чужих учетных данных, которые действительно рассчитаны на ошибку пользователя. В сети ежедневно появляются сотни фишинговых сайтов и тысячи рассылок, призванных заманить туда будущих жертв. У киберпреступников была масса времени, чтобы изобрести множество уловок, основанных на социальной инженерии и трюков, позволяющих им мимикрировать под легитимных отправителей.
- **Уязвимость браузера.** Нередко пароли крадут через уязвимости браузеров или через браузерные расширения. В первом случае специально созданный вредоносный код на веб-странице позволяет подсадить шпиона. А во втором случае пользователь самостоятельно устанавливает себе шпионский скрипт под видом полезного браузерного плагина или расширения. После этого, когда пользователь заходит, например, на сайт банка, этот скрипт будет перенаправлять трафик через хакерский прокси-сервер и таким образом «сливать» учетные данные.
- **Пароли где попало.** Многие до сих пор записывают пароли на стикерах и других бумажках, оставляя в местах, где их легко может увидеть посторонний. Не менее опасно записывать пароли в незащищенных текстовых файлах на своем компьютере или смартфоне, а также не рекомендуется сохранять пароли в браузере для автоматической подстановки.
- **Внешние утечки.** Все, что сказано выше, касается потери пароля на пользовательской стороне. Но утечки часто происходят и в удаленных интернет-сервисах. Это может быть интернет-магазин, социальная сеть, криптобиржа или любой другой ресурс, где при входе используется аутентификация. В результате взлома такого сайта хакеры могут получить огромную базу пользователей вместе с их паролями и другими персональными данными. При этом владельцы сайтов не всегда спешат сообщать о таких взломах. А злоумышленники тем временем обмениваются украденными базами или выставляют их на продажу в дарквебе. Специалисты по безопасности

отслеживают публикации таких баз и предупреждают пользователей. Правда, иногда под видом таких специалистов высока вероятность наткнуться на мошенников.

Многофакторная аутентификация

В том случае, когда для подтверждения прав доступа (аутентификации) используется несколько разных методов одновременно – это и называется многофакторной аутентификацией. Чаще всего цифровые сервисы работают с двухфакторной аутентификацией**.** Многофакторную аутентификацию используют, потому что по отдельности все методы подтверждения права доступа имеют те или иные изъяны.

Основная идея многофакторной аутентификации: чем больше разных факторов используется одновременно, тем больше вероятность, что доступ к аккаунту пытается получить пользователь, который действительно имеет на это право.

Важно понимать, что для многофакторной аутентификации методы, которыми пользователь подтверждает свои права, должны быть действительно разными. То есть в том случае, если некий сервис просит пользователя вводить два пароля, а не один (или, например, пароль и ответ на секретный вопрос), то это нельзя считать двухфакторной аутентификацией, поскольку тут дважды использован один и тот же метод подтверждения прав – знание некой информации.

Таким образом, ответ на вопрос «зачем нужна многофакторная аутентификация?» звучит следующим образом: чтобы сервис мог уверенно понимать, что вы – это вы, и благодаря этому аккаунт было труднее украсть.

Рекомендации:

- Не используйте один и тот же пароль для нескольких учетных записей.
- Создавайте длинные и надежные пароли.
- Храните пароли в защищенном месте.
- Если имеется информация об утечке данных из сервисов или с сайтов, которыми пользуетесь, то сразу же меняйте пароль для доступа к ним.
- Пользуйтесь менеджером паролей.
- Используйте двухфакторную аутентификацию везде, где она доступна.

www.kaspersky.com/
www.securelist.com