Как правильно выбрать пароль?

Абрамян Сергей
www.abrams.ru
9674605@mail.ru

Пароль (от французского parole – слово) — конкретно выбранное засекреченное слово или засекреченная строка символов, которая предъявляется пользователем компьютерной системе. Пароль нужно вводить в целях получения доступа к необходимым программам, файлам, объектам.

Пароль на сегодняшний день является универсальным средством защиты технических данных, которые пользователь желает сохранить в секрете и не допустить несанкционированного проникновения. Аналогичным образом мы ставим железные двери с трудно вскрываемыми замками в квартирах, огораживаем дачные участки, покупаем ракушки для своих драгоценных автомобилей или ставим их на платные стоянки.

Отмечу, что правила, которые существуют в использовании паролей, почти ничем не отличаются от пользования теми же самыми ключами от квартиры или машины. Пароль является очень важным элементом защиты личных персональных данных. Его должны знать только вы и больше никто другой, и лучше не использовать в виде пароля свои: имя, фамилию, отчество, дату рождения, имя матери или отца, кличку питомца, день рождения, серию или номер паспорта, номер телефона и другие личные данные. Также лучше всего не использовать очень простые пароли в виде идущих по порядку цифр: 12345, или повторяющих друг друга цифр: 111111, 6666666. Такие пароли моментально подбираются злоумышленниками, а ваши данные попадают в чужие руки.

Среднестатистическому пользователю сети Интернет приходится периодически пользоваться паролями в количестве около десяти штук. Необходим пароль для входа в саму сеть Интернет, пароль для доступа к почте и получения электронной корреспонденции, пароль, который предоставит доступ к засекреченным на компьютере файлам, пароль для входа в ICQ в целях общения. Также, обязательно нужен пароль для защиты заведённых электронных кошельков, пароли для входа в различные сетевые игры — в общем, список этот можно продолжать сколь угодно долго. У каждого человека свой список засекреченных и приватных областей доступа. Самое главное это то, что пароль действительно необходим каждому пользователю, поэтому так важно заботиться изначально о его правильном составлении и хранении. Хранение тоже является очень важным моментом при пользовании паролями. Конечно, лучше всего будет, если Вы не станете записывать пароли на бумаге или в телефонную книгу, а постараетесь запомнить, воспользуясь какими-нибудь ассоциациями. К примеру, пароль Katie-11viborg, можно запомнить следующим образом: пароль нужен Кате, с которой мы вместе учились в одиннадцатом классе в Выборге. Такой пароль будет являться очень надёжным, лёгким для вашего восприятия и запоминания и его крайне тяжело будет вычислить, а уж взломать и вовсе окажется большой проблемой.

Некоторые пароли, например, от электронных кошельков типа Webmoney, лучше всего записать и хранить отдельно от других данных. При этом данная платёжная система предупреждает о том, что лучше позаботиться заранее о сохранности файлов ключей, при помощи которых можно будет продолжить пользоваться программой. Файл ключей необходим в случае переустановки Windows, переноса программы на другой компьютер и других действий. Файлы ключей лучше всего хранить на съёмном носителе: флэш-карте,

диске или дискете. Дискета является очень ненадёжным носителем, так как при наличии рядом с ней магнитных волн сразу же стирается вся записанная на дискету информация. Диск несколько неудобен, так как нерационально используется большое количество ёмкости, его размеры неудобны для ношения с собой. Самым идеальным и надёжным вариантом хранения паролей и ключей является флеш-карта. При этом никогда не храните файл ключей вместе с кодом доступа к ним и паролем к системе. Пароль в этом случае следует запомнить.

Существуют также программы — менеджеры паролей. Одна из таких программ, которую я предпочитаю всем прочим — это RoboForm и её мобильный аналог RoboForm2Go. Данная программа запоминает все ваши логины и пароли, умеет генерировать правильные пароли, сама заполняет формы для ввода паролей, «вспоминая» какой из паролей для каких целей предназначен. Кроме того, она имеет множество других функций для работы с конфиденциальными данными. Все пароли в такой программе можно надёжно зашифровать. Тогда вам достаточно будет помнить один главный пароль, чтобы пользоваться всеми остальными. Шифрование данных в программе имеет гибкие настройки по степени защиты. Таким образом, решение проблемы хранения и запоминания множества паролей упрощается до запоминания всего одного главного пароля и надёжного резервного хранения файлов данной программы.

Каким же образом лучше всего выбирать составляющие для пароля?

Прежде чем начать составление пароля, не забывайте о том, что некоторые системы являются довольно чувствительными к регистру. Поэтому перед тем, как Вы собрались осуществить ввод, лучше заблаговременно удостовериться в том, не нажат ли Caps Lock, и проверить правильность введения символов. Не всегда набор символов: «aDg» равен набору: «ADG» или «adg». Помните об этом, чтобы впоследствии не забыть составленный вами же пароль. И следите за раскладкой клавиатуры — возможно, вы переключились на русский шрифт, вместо традиционного для паролей английского. Убедитесь, что всё правильно и только тогда переходите к составлению пароля.

Лучше всего не применять пароль, который является словарным словом. В настоящее время существуют программы, которые взламывают пароли, используя при этом методику так называемой «грубой силы» (Brute force), то есть взламывают пароли перебирая словари. Стандартные пароли, о которых говорилось ранее, типа «11111», «66666», «выва», «qwerty» и другие взламываются без малейших проблем в первую очередь. Чтобы правильно составить пароль можно прибегнуть к использованию конкретного набора определенных символов, и лучше всего, если они будут включать до нескольких знаков препинания.

Можно применять символы из нижнего и верхнего регистров: «А – Я», «а – я», «A – Z», «a – z», а также, цифры от 0 до 9. Также лучше прибегнуть к использованию всего лишь одного или двух символов из других наборов, и Ваш составленный пароль будет очень тяжело взломать. Например, пароль Valentina подобрать с помощью программы не составляет никаких особенных усилий, в отличие от пароля ValenTINA84, над которым изрядно придется попотеть, если вообще что-то получится из затеи по взлому этого пароля.

Самым оптимальным для составления пароля является количество цифр от восьми до десяти. Если составленный пароль меньше восьми символов, то это опасно — такой пароль легче будет перебрать, а пароль длиннее десяти символов не очень удобен в использовании, так как его сложнее запомнить и применять.

Перебор осуществляется последовательно от набора символов, стоящих в самом начале к концу, поэтому лучше всего в начале пароля использовать последние символы из списка цифр, знаков или алфавита. В таком случае существенно увеличится общее время подбора и уменьшится вероятность того, что пароль будет взломан. Пользуясь этим правилом, можно составлять простые для запоминания пароли. Например, пароль «avstria» можно достаточно просто подобрать программным перебором в отличие от пароля «zavstria».

Для администраторов сетей правила можно расширить. Пользуясь сразу несколькими сетевыми идентификаторами, которые располагаются в разнообразных компьютерных сетях, можно пользоваться во всех системах одинаковым паролем, дабы упростить для себя задачу запоминания множества паролей для каждой системы. Существенным недостатком такого способа является то, что если хоть на одной системе будет взломан предложенный Вами пароль, то и на каждой станции с аналогичными паролями будет утеряна вся защитная система. Можно найти решение и в данной ситуации, используя какой-либо секретный базовый шифр, а на его основе уже добавлять символы и знаки для каждой станции в частности. Например, пусть Вашим секретным базовым паролем будет KARINA, тогда на другой станции можно пароль видоизменить до 12_KARINA%12, на следующей станции пароль может иметь вид 1984_KARINA%LOG и так далее. Количество придуманных засекреченных паролей должно соответствовать количеству компьютерных сетей, которыми Вы пользуетесь.

Некоторыми серверами предназначены различные варианты защиты от программ перебора паролей. Один из вариантов защиты такого типа — система блокировки доступа после трёх провальных попыток неправильного ввода пароля. Это очень удобно, когда посторонний пользователь пытается взломать ради удовлетворения собственных интересов вашу почту или ICQ. Способ является вполне надёжным, но несколько неудобным, потому что в том случае, если все три попытки введения пароля не увенчались успехом, нужно будет обращаться по электронной почте к административным работникам системы с просьбой разблокировки запрашиваемого аккаунта. Подобрать необходимый пароль всего с трёх попыток практически невозможно. Некоторые серверы предусматривают защиту в виде наличия графического баннера, который представляет собой картинку с цифрами и буквами (CAPTCHA — Completely Automatic Public Turing Test to Tell Computers and Humans Apart). Способ является очень удобным, но, рассматривая степень надёжности, оставляет желать лучшего. На сегодняшний день существует большое количество программ, которые способны с лёгкостью распознавать надписи на предложенных системами картинках. Также на некоторых серверах предлагается воспользоваться доступом по IP адресу. Этот способ является в равной степени как очень надёжным, так и довольно удобным. При наличии постоянного IP можно не волноваться о проникновении третьего лица на «запретную территорию». Но нужно учесть, что если Вы являетесь обладателем динамического IP, то в таком случае даже Вам будет отказано в доступе.

Если Вы столкнулись с такой ситуацией, что необходимо в какой-то момент ввести засекреченный пароль, а рядом с Вами находится третье лицо, чьё присутствие в такие моменты явно становится нежелательным, то можно прибегнуть к целому ряду уловок, чтобы обезопасить себя от разглашения такой важной информации. Нужно медленно набрать неверный пароль, затем его сбросить и повторить процедуру, снова набрав неправильный пароль. После чего, когда бдительность присутствующего будет несколько ослаблена, быстро набрать верный пароль. Ведь в тот самый первый раз, когда Вы вводили пароль, человек, находившийся рядом, с особенной внимательностью старался запомнить набранную комбинацию цифр и букв. Во второй раз он тоже может

постараться запомнить набранный пароль. Затем он вовсе будет сбит с толку и не сможет уже быстро сориентироваться в производимых манипуляциях, при этом концентрация внимания будет порядком ослаблена. Будет неплохо, если Вы научитесь набирать свой пароль особенно быстро, при этом, даже не смотря на клавиатуру. В таком случае момент ввода пароля можно совместить с беседой. Человеку будет сложно слушать вас и одновременно пытаться запомнить вводимые знаки, не выдав свои намерения.

Существуют ситуации, когда приходится осуществлять набор своего личного пароля не на своём компьютере. Например, выходя в Интернет с компьютера друга или Интернет-кафе. В последнем варианте риск пользованием Вашим персональным паролем минимален, а вот находясь в гостях, старайтесь все же воздержаться от предоставления подобных данных, ведь на некоторых компьютерах стоит система сохранения пароля. После вашего ухода хозяину компьютера достаточно будет лишь введения одной буквы вашего логина и заветная цель уже перед нежелательными взорами.

Также существуют специальные программы, которые перехватывают набранные символы. Они способны перехватить ваш пароль посредством так называемого клавиатурного шпиона. Эти программы способны осуществлять запись всего, что было ранее набрано на клавиатуре конкретного компьютера. Помимо прочего программа указывает, в каких программах был произведен определённый набор. А потом, с помощью дедуктивного метода, злоумышленнику не составит особого труда определение того, какой логин и пароль подходит для той или иной системы. Но существуют способы, позволяющие сбить с толку такого клавиатурного шпиона.

Перед тем, как Вы решили осуществить набор своего секретного пароля в какой-либо конкретной программе, лучше всего одновременно в новом другом окне осуществить набор и произвести копирование в буфер определённой части Вашего пароля. Затем можно смело вставлять текст в необходимое поле и набрать ту часть пароля, которой не достаёт. Также будет хорошо, если Вы не будете сразу вводить логин с паролем, а запутаете клавиатурного шпиона, постоянно перепрыгивая на другие окна и кликая там клавиатурой в разнообразных сочетаниях.

Не забывайте также о необходимости создавать надёжные контрольные ответы на вопросы, используемые для восстановления доступа. В службах бесплатной почты, форумах и других онлайновых сервисах вам может быть предложен контрольный вопрос и ответ на него. С особенной тщательностью походите к выбору вопроса и ответа. Стандартные вопросы таких систем, как правило, ограничиваются общими: любимым блюдом, девичьей фамилий матери, кличкой домашнего животного, номером паспорта и другими простыми вопросами. Ответы на эти вопросы не сложно получить злоумышленнику в процессе общения с вами или из некоторых закрытых источников. А зная ответ на контрольный вопрос, можно прибегнуть к интерактивной процедуре смены пароля. Таким образом, хотя ваш пароль не станет известен злоумышленнику, но будет изменён. То есть, доступ к определённой системе будет взломан. Если это доступ к почтовому ящику, то через него могут быть восстановлены или изменены и другие ваши пароли.

Нередко новички в Интернете с началом пользования сетью регистрируют свой первый почтовый ящик, пренебрегая всеми правилами защиты конфиденциальности данных. Например, в открытой анкете на почтовом сервере указывают свои интересы и предпочтения, которые и являются ответами на контрольные вопросы для восстановления доступа. А первые пароли вообще не отличаются оригинальностью и являются весьма простыми, типа пяти пятёрок или шести нулей. Иногда используются инициалы с датой

рождения. Новички не всегда осознают опасности последующего взлома таких паролей. С течением времени у пользователя появляются различные учётные записи, электронные деньги и другие материальные ценности, доступные виртуально. Между тем, во всех первых регистрациях в качестве почтового ящика для восстановления последующих учётных записей фигурирует тот самый плохо защищённый первый e-mail пользователя. Через доступ к нему злоумышленник может получить доступ к остальным почтовым ящикам и учётным записям пользователя.

Если подобная ситуация вам знакома, то не медлите и измените все пароли для тех ящиков, которые вы когда-то регистрировали. Также поменяйте ответы на контрольные вопросы и проверьте, нет ли у вас забытой почты с простым паролем доступа. Вообще, пароли следует менять с заданной периодичностью, частота которой зависит от ценности хранимой информации и активности пользователя в Интернете. В идеале менять все ваши пароли каждые три месяца и ежегодно проводить ревизию ваших учётных записей, уничтожая ненужные. Тогда у злоумышленников, желающих нанести вам вред, не будет никаких шансов.

Используя описанные выше способы, можно быть уверенным в том, что ни одна из шпионских программ не сможет достоверно распознать ваш пароль, и, соответственно, ваши данные останутся в целости и сохранности, собственно говоря, чего вы и добивались! А чтобы сделать защиту более эффективной используйте специальные программы для обнаружения вирусов, шпионских и других вредоносных программ. И не забывайте регулярно обновлять свои программы защиты.

Научившись правильно создавать пароли и безопасно пользоваться ими, вы получите спокойствие и уверенность в сохранности и конфиденциальности своих данных.

Ссылки по теме:

www.captcha.ru
www.roboform.com/ru/