Путь к бедности и проблемам с законом начинается с удобного пароля

Безопасность — это неудобно, а все что удобно — небезопасно. Олег Седов, директор по развитию направления «Кибербезопасность населения» ГК «Солар» ПАО «Ростелеком», журналист, главный редактор, содиректор программ кибербезопасности Школы управления Сколково советует принять это утверждение как аксиому и дочитать до конца статью, чтобы, поразмышляв, поменять все свои пароли на более надежные, а значит — защитить свои личные данные, репутацию и финансы.

Один — хорошо, а два лучше

— Дверь довольно удобно открывать ногой, но все-таки мы предпочитаем относиться к ней бережно, а имущество, которое за ней спрятано, защищать надежным запором, а лучше двумя, — говорит Олег Седов. — Мы ставим разные замки на двери квартиры, гаража, машины и сейфа. Имеем от них разные ключи и воспринимаем это как совершенно естественное явление. При этом до сих пор многие используют одинаковые пароли для почтового ящика, социальных сетей и даже онлайн-банка.

Еще одно относительно недавно появившееся новшество — двухфакторная идентификация тоже у многих взрослых людей вызывает раздражение. Почти все используют ее только вынужденно и совершенно неправильно. Эксперты напоминают, что двухфакторной можно назвать только ту идентификацию, где пароли приходят на разные устройства по разным каналам связи. Она так же не поможет, если вы храните два устройства в одном рюкзаке и так же вместе их теряете.

— Когда мы объясняем на пальцах, что безопасники требуют сложный пароль не из вредности, а по-настоящему о нас переживая, люди начинают более ответственно относиться к собственным аккаунтам, — говорит Олег Седов.

«Брутфорс» — это метод «грубой силы», другими словами, простой перебор вариантов паролей, который способен свести с ума кого угодно, но не машину. Даже не самый мощный компьютер потратит одну секунду на то, чтобы подобрать пароль из одного-трех знаков. На подбор семи символов у робота уйдет девять дней. И, внимание… над паролем из восьми знаков робот будет биться 11 месяцев.

Осознав, что нас взламывают неутомимые и бездушные машины, у которых нет логики, но есть алгоритм, нужно просто принять тот факт, что совет сисадмина менять пароль раз в полгода идет от сердца.

Роботы анализируют даже наши старые пароли, пытаясь на их основе предположить, каким будет новый. Случайно перепутанные местами логин и пароль также могут попасть в даркнет и оттуда — в руки злоумышленников.

И при всем этом сегодня, когда ИИ щелкает наши пароли, как орешки, 17% пользователей используют пароль 123456. Около 26% владельцев смартфонов защищают их одним из 20 самых распространенных цифровых сочетаний. Он может защитить ваш телефон от мониторинга со стороны жены, но легко вскроется злоумышленником.

Существует предрассудок, что чаще всего жертвами мошенников становятся старики, дети и скучающие домохозяйки. Но на самом деле очень часто жатвой для аферистов служат самоуверенные люди, которым их высокий статус внушает веру в неуязвимость.

Основные правила безопасности в интернете: иметь отдельный пароль для каждого аккаунта, выбирать надежный пароль, чаще его менять, проводить смены с надежного устройства (помните, что администратор публичного вайфая имеет возможность мониторить весь трафик).

Надежный — значит сложный

Выбирая пароль, люди снова забывают, что роботы не следуют человеческой логике. Набрав латиницей русское слово , обмануть машину не получится. Она имеет доступ к словарям всех языков мира и давно знает эту нашу хитрость. Как и банальные подмены «о» на ноль, s на $ и так далее.

Также нельзя использовать в паролях номера телефонов, дни рождения и простые слова.

— Многие приходят в отчаяние от всего этого перечня, ведь запомнить случайно сгенерированный пароль почти невозможно, — соглашается Олег Седов. — Но есть несколько вариантов решить проблему. Робот быстрее, умнее и настойчивее, но только человек может быть талантлив и придумать свою уникальную систему.

Как вариант эксперт предлагает взять пословицу или строчку стихотворения и набрать латиницей первые буквы каждого слова, некоторые из них сделав заглавными. Такого набора букв точно нет ни в одном словаре!

Люди с музыкальным образованием могут попробовать использовать в пароле гитарные аккорды.

Если применить в секретном коде показания ваших домашних счетчиков, то точно можно быть уверенными, что этот набор цифр никому другому не известен.

Пароль из несложной химической формулы, плюс пара специальных символов даст стойкость пароля на миллионы лет.

Пароли не стоит хранить в заметках телефона, даже под кодом, но можно записать их на листке бумаги, надежно спрятать его или сфотографировать и уничтожить. В этом случае, правда, придется проверить, нет ли у вас в настройках установки сохранять все фото с телефона в облачных хранилищах.

Можно воспользоваться современными сервисами в виде менеджера паролей. Тогда вам нужно запомнить лишь один надежный пароль — для самого приложения. Но в этом случае лучше выбрать платный сервис. В любом бесплатном таятся свои подводные камни.

Использование биометрии для ограничения доступа к устройствам — это удобно. А в самом начале мы договорились, что все удобное не слишком надежно. В гаджетах установлены очень простые сканеры, совсем не такие, как в банковских хранилищах или секретных лабораториях. Их не слишком сложно обойти профессионалу.

Используя на андроиде графические ключи, сразу откажитесь от шлейфа. Это красиво, но до предела облегчает задачу злоумышленника. Сама же система довольно надежна, если использовать ее грамотно. Выбирая узор из девяти узлов, мы увеличиваем число вариаций до 389112. Но, как обычно, люди редко идут сложным путем. А, используя не больше пяти, мы получаем лишь 8000 комбинаций, 4 узла дадут еще в разы меньше — 1624 варианта.

Люди не только ленятся, но и действуют предсказуемо, выбирая рисунок. 44% пользователей ведут линию из левого верхнего угла, 77% — начинают в одном из углов, чаще всего палец движется слева направо и сверху вниз — так, как мы читаем книги. Выберите другое направление с обязательным пересечением линий и почаще протирайте свой гаджет. Это и гигиенично, и не позволит по следам на стекле предположить форму вашего графического кода.

Основные правила установки безопасного пароля: любой пароль по умолчанию нужно менять, стараться не давать свое устройств в руки чужим людям, блокировать экран, даже если вам нужно отойти от него на минуту.

Ради собственного спокойствия помните, что к любой камере в вашем доме могут подключиться. Недавно в сеть слили пикантные кадры, которые наснимал робот-пылесос.

Даже пароль роутера надо обновлять. Не так жаль, если кто-то научится качать ваш трафик, как неприятно будет объясняться с полицией, если с вашего IP-адреса будут совершаться противоправные действия.

Да, и Алиса слишком много знает. Загляните в список ваших обращений к ней и попробуйте проанализировать, сколько информации о вас можно почерпнуть на основе этих вопросов…

https://www.kommersant.ru/doc/6466014