Многие ошибочно считают, что никому не понадобится взламывать их учётную запись, поскольку киберпреступника якобы интересуют лишь крупные банковские сервисы или хранилища секретной информации. По этой причине ряд пользователей не утруждает себя придумыванием сложных паролей, используя простые для запоминания аббревиатуры или словосочетания. Но задумывались ли вы, что пароль – это единственное, что защищает вашу учётную запись от доступа к ней злоумышленника, а ваши почта и аккаунты в социальных сетях принадлежат только вам исключительно потому, что защищены паролем? Подобрав пароль, злоумышленник может попросить от вашего имени реквизиты банковской платёжной карты у ваших знакомых, чтобы совершить хищение средств или разослать вредоносное программное обеспечение, прикрываясь вашим именем.

Преступники прежде всего стремятся получить доступ к аккаунтам, защищённым простыми паролями. Для этого они запускают программы, подбирающие пароли, и используют готовые словари и простые сочетания букв с цифрами. «Natashenka2019» - вариант, который программа проверит в числе первых, если почта заведена в 2019 году, а имя пользователя - «Наталья». Такие программы без труда определяют инвертированную раскладку и легко взломают, к примеру, пароль «vjqgfhjkm» (набранное в английской раскладке клавиатуры словосочетание «мойпароль»).

Составляя пароль, используйте комбинации букв, цифр, специальных символов, неочевидные ассоциации и сочетания различных элементов. Имя или номер телефона – не лучший выбор. Правильно оценивайте сложность пароля перед началом использования:

- совсем слабый пароль: общеизвестные аббревиатуры, названия, общеупотребительные фразы и слова (qwerty, admin, pass123, password, root; 4% пользователей используют пароли из первой десятки популярных, а три самых популярных пароля держат лидерство годами);
- плохой пароль, который кажется сложным: дата вашего рождения или рождения кого-то из близких, номер какого-то из ваших документов, кличка вашего домашнего питомца, инверсия в раскладке простого слова, особенно вашего имени, замена пары букв цифрами в применимом к вам слове;
- сложный пароль: имеет не очевидную и не сводимую к одному слову основу для запоминания с обязательным использованием цифр, букв (со сменой регистра клавиатуры) и специальных символов.

Для создания достаточно сложного пароля всегда можно использовать онлайн-генератор паролей, которые зачастую предлагают пользователю несколько вариантов. Выбрав наиболее привлекательный, замените

несколько символов на случайные, после чего используйте. Конечно, запомнить такие пароли порой затруднительно, по этой причине их приходится записывать, однако делать это нужно, соблюдая следующие рекомендации:

- записывайте пароль отдельно от логина или имени пользователя;
- записывайте его не полностью, а лишь частично или разделите пароль на части и поменяйте их местами;
- записывая пароль, зашифруйте его часть или добавьте заведомо для вас лишние символы.

Стоит также помнить, что использовать один пароль для доступа к разным аккаунтам не рекомендуется, поскольку каждый интернет-ресурс использует свои системы защиты и хранения паролей, которые не всегда могут быть реализованы на высоком уровне. Согласно статистике, около 14% пользователей используют один и тот же пароль для авторизации на всех аккаунтах и, получив доступ к одному, злоумышленник непременно получит доступ и к другим.

Очень часто злоумышленники даже не пытаются взломать пароль, а просто стараются его узнать под тем или иным предлогом. Они массово рассылают письма и сообщения с призывом поучаствовать в беспроигрышной акции, проводимой крупной торговой сетью или финансовой организацией, при этом злоумышленники стараются оставить на раздумья как можно меньше времени, чтобы подтолкнуть пользователя на принятие решения немедленно, под влиянием эмоций. Зачастую для участия в таких «акциях» требуется предоставить имя пользователя и/или пароль от какого-либо аккаунта или сведения о банковской платёжной карте. Использование эффекта внезапности – излюбленный приём злоумышленников. Так, обнаруженное в электронном почтовом ящике письмо о якобы заблокированном аккаунте в социальной сети очень часто толкает пользователей на переход по прикрепленной ссылке, которая, в свою очередь, ведёт на поддельную страницу (очень похожую на настоящую), где для отмены блокировки необходимо ввести свои данные. После ввода вся информация попадает в руки злоумышленников. Стоит запомнить, что пароль – это секрет, который должен принадлежать только одному человеку, а если о нём знает кто-то ещё, то это уже не секрет.

В качестве дополнительного способа защиты своей информации рекомендуется также использовать двухфакторную систему идентификации, при которой специально сгенерированное SMS-подтверждение будет поступать на указанный пользователем абонентский номер телефона при каждой попытке входа в аккаунт с нового устройства.

При использовании данной системы злоумышленник не сможет осуществить доступ к аккаунту, даже зная пароль.