Установка и использование пароля

Пароль — условное слово или набор знаков, предназначенный для подтверждения личности или полномочий. Появилось от фразцуского слова «Parole» — слово.

Пароль устанавливается:

1. При заходе в операционные системы любых персональных устройств: компьютер, смартфон, планшет и.д.

2. При заходе в отдельные программы;

3. При заходе в профайл сайтов, сервисов и приложений;

4. Для банковских карт, платежных сервисов и других.

Получение пароля позволяет осуществлять любые действия от вашего имени, поэтому его безопасность важнейший вопрос.

Пароль не должен быть простым, поскольку простой пароль — это наибольшая угроза вашей учетной записи. Обычные слова (marina, begemot), а также предсказуемые сочетания букв (qwerty, 123456) могут быть легко подобраны программами для взлома паролей. Особенно популярный пароль, содержащий данные ФИО, дату, месяц и год рождения, например, пароль «Ivan1996».

Важно обеспечить сложные и разные пароли, поскольку в случае взлома злоумышленники получат доступ только к одному профилю в сети, а не ко всем.

Специалисты рекомендуют использовать два вида паролей:

1. для платежных систем длинные и сложные пароли, которые состоят как минимум из 10 символов, включают буквы верхнего и нижнего регистра, цифры и специальные символы, не содержат имя пользователя и известные факты о нем;

2. простые и легко запоминающееся для форумов и других сайтов, не представляющих опасности для денег.

Для того чтобы создать сложный пароль, следует использовать и прописные, и строчные латинские буквы; цифры; знаки пунктуации (допускаются знаки ` ! @ # $ % ^ & \* ( ) \_ = + [ ] { } ; : « \ | , . < > / ?).

Хороший вариант для пароля – написать какое-нибудь русское словосочетание в английской раскладке клавиатуры. Такой пароль легко запомнить, и в то же время сложно взломать. Например, буквосочетание «вишневый пирог» в английской раскладке выглядит как «dbiytdsq gbhju».

Кроме этого, возможно написание слова и цифр задом наперед, например, ьтсонсапозебребик\_8102 (кибербезопасность\_2018).

Надежным пин-кодом, состоящим из 4 цифр, может быть сумма цифр, которую знает только владелец, например, год покупки смартфона, первой поездки в летний лагерь, появление домашнего питомца и другие.

Специалисты также отмечают одноразовые пароли как один из самых безопасных методов защиты: финансовые сервисы, банки и другие сервисы предоставляют возможность входа в аккаунт с помощью одноразового пароля, который направляется смс-сообщением владельцу аккаунта для подтверждения входа или оплаты.

Объединяют две вышеуказанные технологии двухэтапная авторизация, представляющая собой авторизацию в два этапа:

1. Введение установленного пользователем пароля;

2. Ввода кода подтверждения, который приходит пользователю в виде сообщения через мессенджеры, электронную почту или СМС.

Кроме этого, необходимо обеспечить конфиденциальность паролей, в частности:

1. не сообщать их другим людям;

2. не хранить список паролей в файле на компьютере или на бумаге;

3. в браузере отключить автоподстановку и сохранение паролей;

4. не сохранять пароль на чужом или общественном компьютере, использовав специальную функцию «Чужой компьютер», которая позволяет сервису забыть ваш аккаунт после закрытия браузера;

5. не передавать учетные данные (логины и пароли) по незащищенным каналам связи, которыми являются открытые и общедоступные wi-fi сети.

Рекомендуется обновлять пароли каждые три или четыре месяца.

Для восстановления пароля возможно использовать различные средства, среди которых привязка аккаунтов к мобильному номеру телефона, другая электронная почта и использование контрольного вопроса:

1. Привязка аккаунта к мобильному номеру телефона может быть использована при условии указания в настройках аккаунта актуального и работающего номера телефона;

2. Привязка аккаунта к другой электронной почте актуальна для почтовых сервисов, что позволяет в случае утери одной почты восстановить ее через другую;

3. Контрольный вопрос представляет собой перечень заранее подготовленных вопросов, на которые пользователь дает свой ответ. Например, «Девичья фамилия матери», «Кличка первого животного» и пользователь вводит, например, следующие ответы «Иванова», «Шарик». Таким образом, выбрав функцию восстановления пароля сервис предложит ответить на контрольный вопрос. Рекомендуется не выбирать простые и нейтральные вопросы, ответ на которые легко подобрать или найти, например, в социальной сети.

Необходимо помнить, что восстановить пароль к вашему аккаунту также могут попытаться злоумышленники, а в случае неудачи вы можете потерять свой аккаунт, поэтому к вопросам восстановления необходимо отнестись ответственно.

Как и в случае пароля, так и контрольного вопроса необходимо помнить, что нужно использовать слово или словосочетание, цифра или комбинация цифр, которые известны и понятны только пользователю, чтобы их можно было легко запомнить.