Как создать надежный пароль

1. Придумывать сложные пароли

Пароли достаточно часто критикуют, как с точки зрения безопасности, так и удобства, что делает их менее идеальным методом аутентификации. Однако именно они в комбинации с именами пользователей остаются самой распространенной формой аутентификации на различных сайтах.

Пароли как ключи к онлайн-профилям справедливо считаются первым и, к сожалению, часто единственным способом защиты, который обеспечивает безопасность цифровых данных пользователей. Однако простые и неуникальные данные входа для каждого устройства и аккаунта не способны защитить конфиденциальную информацию от злоумышленников.

В основе надежных и легких для запоминания паролей лежат ключевые фразы, которые, как правило, являются более безопасными и удобными. Чтобы создать пароль, который способен обеспечить безопасность Ваших профилей, специалисты рекомендуют придерживаться таких простых правил:

- Использовать не менее 7 слов, однако более длинная фраза обеспечивает больший уровень безопасности. С каждым дополнительным символом количество возможных комбинаций для подбора растет в геометрической прогрессии, что снижает вероятность успеха атак с использованием подбора паролей.
- Лучше воздержаться от использования фраз из ежедневного потребления. Названия книг, известные цитаты, тексты песен уже, как правило, легко идентифицируются вредоносными инструментами.
- Отдельные слова должны быть в произвольном порядке и, в идеале, комбинироваться со специальными символами, при этом сохраняя скрытый смысл и будучи легкими для запоминания.
- Создать уникальный пароль для каждой учетной записи

Для каждого аккаунта нужно создать уникальную ключевую фразу. Таким образом утечка одной из комбинаций не поставит под угрозу другие и, возможно, более ценные учетные записи. К сожалению, опасная практика повторного использования одинакового пароля для многих профилей является довольно распространенной. Именно поэтому этим часто пользуются киберпреступники, получая доступ к аккаунтам пользователей с помощью автоматизированных запросов.

Вполне вероятно, что сегодня вы используете слишком много учетных записей, поэтому запомнить отдельную фразу для каждого из них нелегко. В

этом случае стоит подумать о надежном менеджере паролей, который облегчает управлением данными входа. В частности, такой инструмент может генерировать случайные и сложные пароли.

Вместо десятка разных комбинаций вам достаточно будет запомнить только одну от менеджера паролей, который, в конце концов, дает доступ ко всем аккаунтам. Однако на него тоже распространяются требования относительно надежности и уникальности, поскольку этот пароль является своеобразным ключом ко всем вашим личным данным.

2. Использовать двухфакторную аутентификацию

Двухфакторная (2FA) или многофакторная аутентификация (MFA) является прекрасным способом улучшить безопасность учетных записей, особенно в сочетании с аппаратными ключами и специализированными приложениями, а тем более с использованием SMS-сообщений. Несмотря на то, что многие онлайн-сервисы предоставляют возможность использования двухфакторной аутентификации, только некоторые из них требуют ее применения. Использование двухфакторной аутентификации требует дополнительных усилий, однако это может помочь в различных ситуациях, в том числе, защитит вас от несанкционированного доступа к учетным данным в случае кражи паролей.

На самом деле, вполне вероятно, что некоторые из ваших данных входа уже были похищены и размещены на теневых рынках онлайн. Источником этих утечек являются атаки на онлайн-сервисы, магазины, гостиничные сети. Организация может обеспечивать недостаточную защиту данных входа пользователей, например, хранить пароли в виде обычного текста. Также поставщики услуг могут вообще не знать об атаках, пока позднее хакеры не похитят данные пользователей или приобретут их в теневом сегменте сети Интернет. Кроме этого, в таких случаях дополнительный фактор аутентификации, как правило, препятствует попыткам несанкционированного доступа к учетной записи.

3. Удалить неактивные аккаунты

Также следует уменьшить количество учетных записей, которые вы больше не используете. Действительно, многие профилей создавались давно, и некоторые данные вхожа уже нелегко вспомнить.

Проблема со старыми аккаунтами заключается в том, что каждый из них является потенциальным источником опасности. Сервис может стать жертвой атаки, в результате которой ваш пароль попадет в руки злоумышленников или может быть продан новым владельцам с преступными намерениями. Также киберпреступники смогут использовать аккаунт для входа в один из ценных

учетных записей. Кроме этого, злоумышленники могут использовать ваш профиль для распространения спама.

Поэтому рассмотрите возможность ограничить связь учетных записей с приложениями и службами, особенно с программами, которые больше не используются. Эти программы также могут быть несанкционировано использованы как точки входа для незаконного сбора данных. Чтобы ограничить их связь с важными данными, перейдите к настройкам конфиденциальности и безопасности онлайн-сервиса, что, как правило, занимает всего несколько кликов.

В связи с постоянным совершенствованием тактик киберпреступников специалисты также рекомендуют пользователям быть осторожными при работе в сети Интернет и использовать надежные решения для эффективной защиты личных данных и конфиденциальной информации.

Источник: https://eset.ua/ru/news/view/649/nadezhnyy-parol-sposoby-sozdaniya-parolya-ot-spetsialistov-eset