

Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей Хабаровского края)»



ПАМЯТКА

СОЗДАНИЕ НАДЕЖНЫХ ПАРОЛЕЙ



г. Хабаровск, 2021 год



Памятка «Создание надежных паролей» / Сост. Е.А. Фомина –
г. Хабаровск: КГАОУ ДО РМЦ, 2021. – 4 с.

Ответственный за выпуск: О.В. Монахова



СОЗДАНИЕ НАДЕЖНЫХ ПАРОЛЕЙ

Вам нужно будет создать пароль, чтобы делать практически все в Интернете, от проверки электронной почты до онлайн-банкинга. И хотя использовать короткий, легко запоминающийся пароль проще, это также может представлять серьезную угрозу для вашей безопасности в Интернете. Для того чтобы защитить себя и свою информацию, вам нужно использовать пароли, которые долго и трудно разгадать кому-то другому, но все еще относительно легкими для вас, чтобы запомнить.



ЗАЧЕМ МНЕ НУЖЕН НАДЕЖНЫЙ ПАРОЛЬ?

На этом этапе вы можете спросить, зачем мне вообще нужен надежный пароль? На самом деле, хотя большинство веб-сайтов безопасны, всегда есть небольшая вероятность, что кто-то попытается получить доступ к вашей информации или украсть ее. Это обычно называется взломом. Надежный пароль - один из лучших способов защитить ваши учетные записи и личную информацию от хакеров.



СОВЕТЫ ПО СОЗДАНИЮ НАДЕЖНЫХ ПАРОЛЕЙ

Надежный пароль - это тот, который легко запомнить, но трудно угадать другим. Давайте рассмотрим некоторые из наиболее важных вещей, которые следует учитывать при создании пароля.

- 1** Никогда не используйте личную информацию, такую как ваше имя, день рождения, имя пользователя или адрес электронной почты. Этот тип информации часто является общедоступным, что позволяет кому-то легко угадать ваш пароль.
- 2** Используйте более длинный пароль. Ваш пароль должен быть не менее шести символов, хотя для дополнительной безопасности он должен быть еще длиннее.
- 3** Не используйте один и тот же пароль для каждой учетной записи. Если кто-то обнаружит ваш пароль для одной учетной записи, все остальные ваши учетные записи будут уязвимы.

4 Старайтесь включать числа, символы, а также прописные и строчные буквы.

5 Случайные пароли - самые надежные. Если у вас возникли проблемы с его созданием, вы можете вместо этого использовать генератор паролей. Например, <http://www.onlinepasswordgenerator.ru/>

Генератор паролей

Хотите сгенерировать пароль? Просто заполните форму ниже и нажмите кнопку "Создать пароль".

Настройки генератора:

- Цифры
- Прописные буквы
- Строчные буквы
- Спец. символы %, *, ., ?, @, #, \$, ~

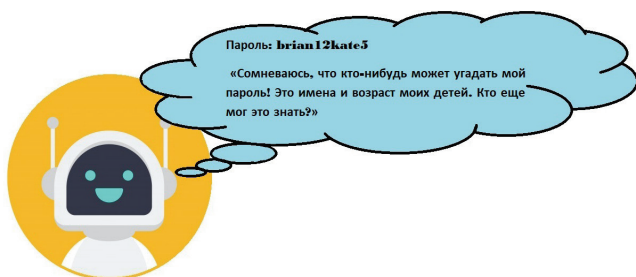
Длина пароля: [6] - символов

Ваши сгенерированные пароли:

- eISwtz
- LjGxj5
- eRk9XR
- 2nhCj9
- ie0CID
- hKwCok
- MRmObg
- qzZbjj
- BFMIV
- 3JBrit

ТИПИЧНЫЕ ОШИБКИ ПАРОЛЕЙ

Некоторые из наиболее часто используемых паролей основаны на именах родственников, хобби, или просто слова из песни. Хотя эти типы паролей легко запомнить, они также являются одними из наименее безопасных. Давайте посмотрим на некоторые из наиболее распространенных ошибок паролей и способы их исправления.



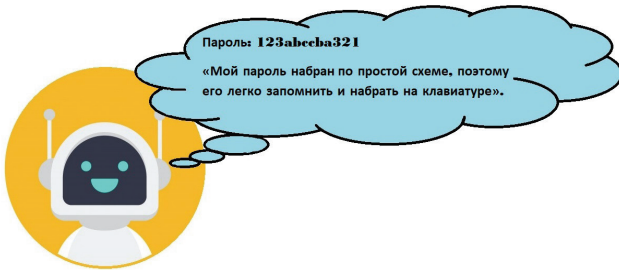
Проблема: в этом пароле используется слишком много личной информации, а также общие слова, которые можно найти в словаре.

Решение: более надежная версия этого пароля будет использовать символы, прописные буквы и более случайный порядок. И вместо того, чтобы использовать фамилии, мы могли бы объединить персонажа из фильма с типом еды. Например, «Чубакка» и «пицца» могут стать «chEwbAccAp! ZZa».



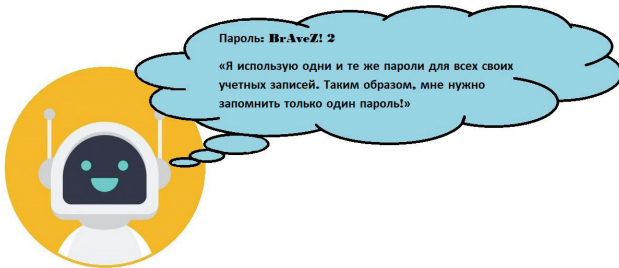
Проблема: это слишком короткий пароль, состоящий всего из пяти символов. Он также включает часть ее адреса, которая является общедоступной информацией.

Решение: более надежная версия этого пароля будет намного длиннее, в идеале более 10 символов. Мы также можем заменить ее текущий адрес на название ближайшей улицы. Например, Pemberly Ave может стать p3MberLY% Av.



Проблема: хотя подобные шаблоны легко запомнить, они также являются одними из первых вещей, о которых хакер может догадаться при попытке доступа к вашей учетной записи.

Решение: помните, что случайные пароли намного надежнее простых шаблонов. Если у вас возникли проблемы с созданием нового пароля, попробуйте вместо этого использовать генератор паролей. Вот пример сгенерированного пароля: #eV\$plg&qf.



Проблема: в этом пароле нет ничего плохого, но помните, что вы никогда не должны использовать один и тот же пароль для разных учетных записей.

Решение: создайте уникальный пароль для каждой учетной записи в Интернете.

ИСПОЛЬЗОВАНИЕ МЕНЕДЖЕРОВ ПАРОЛЕЙ

Вместо того, чтобы записывать пароли на бумаге, где кто-то может их найти, вы можете использовать менеджер паролей, чтобы безопасно хранить их в Интернете. Менеджеры паролей могут запоминать и вводить ваш пароль на разных сайтах, а это значит, что вам не придется запоминать более длинные пароли. Примеры менеджеров паролей включают LastPass, 1Password и менеджер паролей Google Chrome.

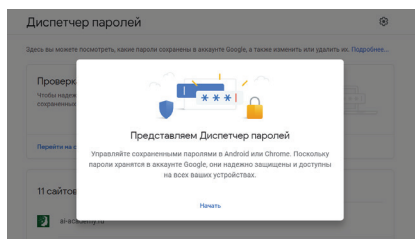
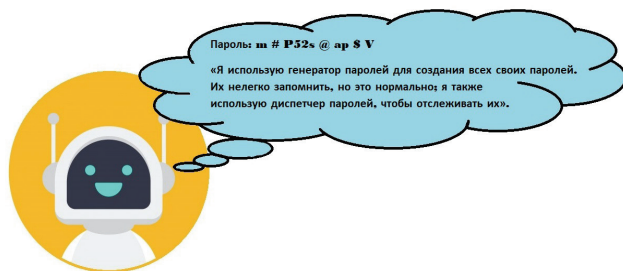


Иллюстрация характера



Это отличный пример надежного пароля. Он сильный, длинный, и его будет сложно угадать. Он состоит из более 10 символов с буквами (как в верхнем, так и в нижнем регистре), числами и символами и не содержит явной личной информации или общих слов. Этот пароль может быть даже слишком сложным для запоминания без диспетчера паролей, что подчеркивает, почему они так полезны при создании надежного пароля.

Не забывайте использовать эти советы всякий раз, когда вы создаете пароль, чтобы сохранить вашу онлайн-информацию в безопасности.

Памятка «Создание надежных паролей»

**Краевое государственное автономное образовательное учреждение
дополнительного образования «Центр развития творчества детей
(Региональный модельный центр дополнительного образования детей
Хабаровского края)»**

680000, г. Хабаровск, ул. Комсомольская, 87

тел. / факс: (4212) 30-57-13

Инстаграм: @dop.obrazovanie27

e-mail: yung_khb@mail.ru

<http://www.kcdod.khb.ru>

Подписано в печать: 30.09.2021 г.