Защита паролей

Узнайте о том, как создавать надежные безопасные пароли и как их защитить.

1. Что такое надежные пароли? Зачем их создавать?

Надежность паролей — важнейший аспект защиты паролей. Надежный пароль сложно угадать или взломать.

Надежные пароли значительно усложняют хакерам и другим злоумышленникам получение несанкционированного доступа к вашим учетным записям и похищение ваших данных и информации.

Но надежные пароли тяжело запомнить. Подумайте об использовании менеджера паролей, чтобы контролировать и надежно хранить ваши пароли!

2. Характеристики надежного пароля

Воспользуйтесь следующими рекомендациями по созданию паролей:

- Чем длиннее пароль, тем лучше.
  - Пароль должен содержать минимум 12 символов.
- Используйте сочетание разных символов:
  - большие и маленькие буквы;
  - цифры;
  - символы.
- Используйте редкие слова.

Не используйте запоминающиеся сочетания клавиш или распространенные слова, особенно такие, как «password», «login» или «qwerty». И не используйте в паролях вашу

персональную информацию, например ваш день рождения, адрес, имена домашних животных или членов семьи и т. д.

3. Повышение надежности паролей

Ниже приведены распространенные пароли, которые можно сделать более надежными. В ячейках ниже предложите способы повышения надежности указанных паролей.

Пароль	Как повысить надежность	Какими способами вы воспользовались?
P4ssw0rd		
Fluffy0212		
1234567		
Yankees87 *(Спортивная команда + год вашего рождения)*		
Austin2010 *(Памятная поездка + год)*		

Eva23 *(Имя ребенка + год окончания школы)*		

4. Создание надежного пароля с нуля

Для создания надежного пароля воспользуйтесь следующими рекомендациями.

A) Используйте генератор паролей.

Генераторы паролей создают случайные пароли, которые трудно взломать. Единственный их недостаток заключается в том, что их сложно запомнить, поэтому для хранения таких паролей можно использовать менеджер паролей. Случайные пароли могут стать хорошим способом создания паролей с повышенной надежностью для учетных записей с важными данными.

Придумайте области применения случайных паролей и запишите их здесь:

B) Используйте вместо паролей кодовые фразы.

Вместо слова придумайте запоминающуюся фразу. Итак, создайте кодовую фразу, затем, используя первую букву каждого слова фразы, а также символы и цифры, вы получите пароль. Для этого метода также подходит сочетание цифр, символов и уникального написания фразы или цитаты.

Вот несколько примеров от Cybernews.com.

> Пример фразы: «I first went to Disneyland when I was 4 years old and it made me happy» («Впервые я посетил Диснейленд, когда мне было 4, и я был счастлив»).
>
> Пример пароля: I1stw2DLwIw4yrs&immh
>
> Пример фразы: «One for all and all for one»: The Three Musketeers («Один за всех и все за одного», Три мушкетера)
>
> Пример пароля: 14A&A413Mu$keteers!

Придумайте области применения кодовых фраз и идей для фраз и запишите их здесь:

C) Смешение слов.

Также вы можете выбрать несколько случайных слов из словаря и объединить их с сочетанием букв, цифр и символов для создания надежного пароля. Только не ограничивайтесь одним словом, поскольку хакеры могут его легко угадать.

Придумайте области применения этого метода и запишите их здесь:

4. Защита паролей

Ознакомьтесь со следующим списком и обсудите, как вы можете улучшить защиту паролей. Подумайте вместе и поделитесь своими идеями!

- Для каждой учетной записи должен быть отдельный пароль.
- Используйте многофакторную аутентификацию.
- Используйте менеджер паролей.
- Будьте внимательны, регистрируя учетные записи.
- Используйте минимальный объем данных и будьте осторожны, когда вы делаете информацию общедоступной.
- Остерегайтесь фишинга.
- Регулярно меняйте пароли.
- Проверяйте параметры конфиденциальности в разных учетных записях.

Что еще вы можете предложить?