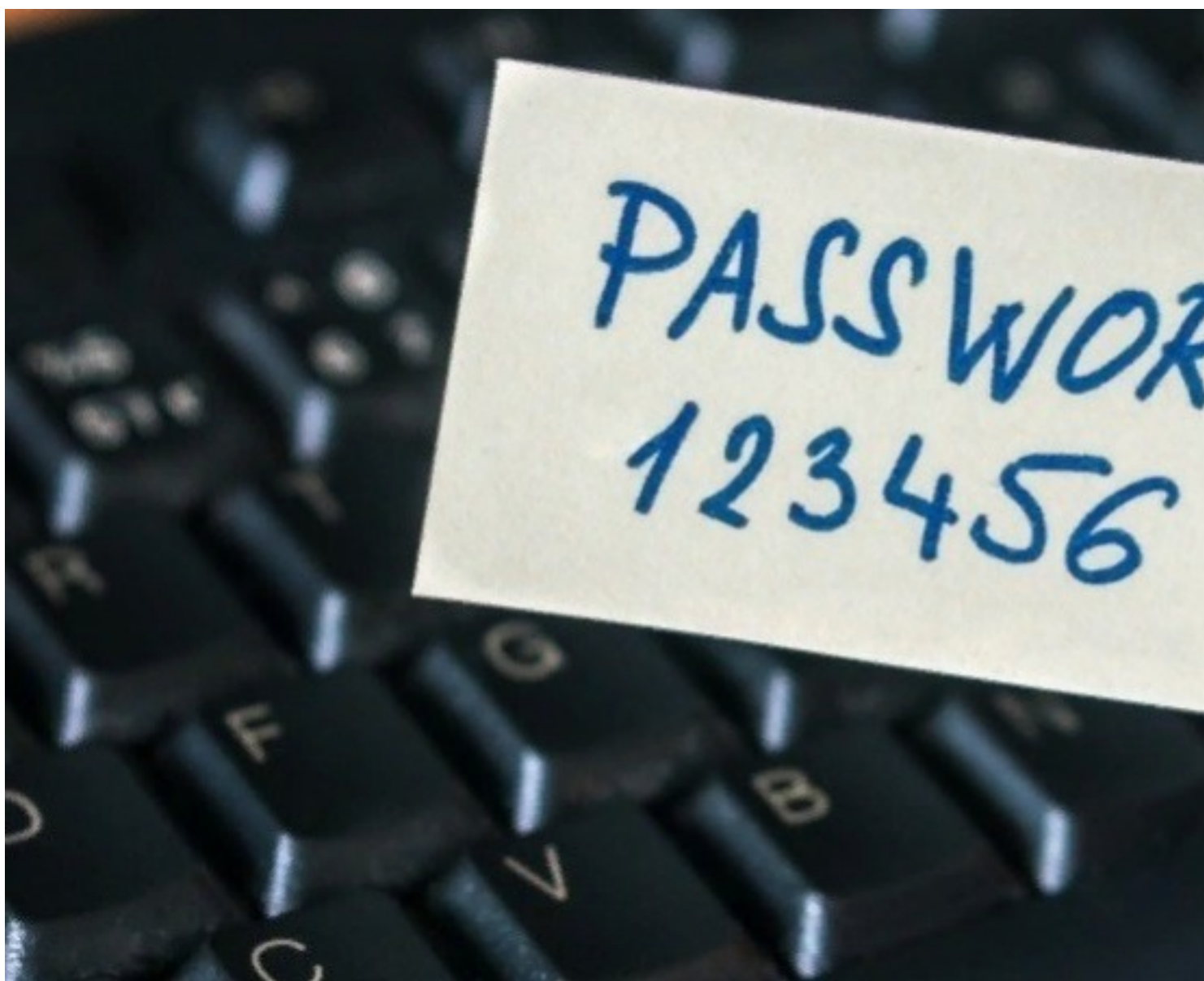


## Как перестать беспокоиться о том, что пароли похитят хакеры

Автор: Administrator  
24.12.2019 11:18 -

---

Электронные аккаунты хранят в себе важную информацию, поэтому стоит как следует позаботиться об их защите. Чтобы злоумышленник не смог добраться до переписок и денег, мы собрали способы, которые сведут к минимуму риски взлома.



### Надежные и уникальные пароли

В сети можно прочитать новости о взломах целых сайтов, где люди хранили свои данные. На самом деле взломать целый сайт не каждому хакеру по зубам. А вот получить доступ к аккаунту (угадав пароль) намного проще.

## Как перестать беспокоиться о том, что пароли похитят хакеры

Автор: Administrator  
24.12.2019 11:18 -

---

Поэтому рекомендуем ставить уникальные пароли. Люди, заинтересованные в ваших данных, находятся среди вас: это не обязательно абстрактный хакер, это может быть любопытный знакомый, который решил сыграть шутку. А он точно знает, как зовут вас, вашу любимую собаку, дату рождения и улицу, на которой вы живете.

Не ставьте в качестве ключа личные данные. Получить доступ к аккаунту будет в разы легче. Составляйте сложные, уникальные пароли.

### Парольные фразы

NIST – стандарт для паролей, обязательный в государственных учреждениях США. В инструкции говорится о составлении парольных фраз. Здесь есть несколько преимуществ:

- пароль будет длиннее, а, значит, угадать третьему лицу его сложнее;
- вы сможете легче запомнить пароль (благодаря ассоциациям), и не придется его восстанавливать.

Да, ключ будет на 40 символов и вводить его придется дольше. Зато риск забыть пароль незначителен.

### Менеджер паролей

Не умеете придумывать пароли? Доверьте это компьютеру.

Менеджер паролей поможет создать большой витиеватый пароль. Его генерирование может происходить на основе слов/данных, которые вы укажете. Есть возможность также создавать парольные фразы. Все это облегчит манипуляции с паролями-ключами: составление, запоминание, хранение.

Однако пользоваться менеджером паролей как хранилищем не рекомендуется. При взломе менеджера злоумышленнику достанется все.

Если есть желание хранить информацию в менеджере, используйте несколько разных сайтов.

### Обновления Google

Защита данных пользователей важна для компании Google. Поэтому «гугловцы» выпускают новые обновления, расширения и программы. Они помогают засечь вход в аккаунт с другого устройства и предпринять соответствующие меры: сменить пароль, выйти из учетной записи со всех устройств.

Одним из таких новинок является расширение Password Checkup (защищает учетную запись, которая была задета при утечке данных).

### Необычные ответы на секретные вопросы

Иногда злоумышленник пытается получить доступ, выдавая себя за пользователя, который забыл пароль. Тогда хакеру придется отвечать на секретный вопрос типа «девичья фамилия матери». Разыскать эту информацию будет несложно, если хакер связан с государством или органами.

Поэтому к таким случаям стоит подготовиться и перестраховаться. Используйте необычные ответы на вопросы.

Например, вместо девичьей фамилии матери пишите улицу, где родились. Или заменяйте символы: А – 4, О – 0, и так далее.

Чтобы защитить свои учетные записи, не забывайте о мерах безопасности. С помощью наших советов вы убережете себя от хакеров.