Как создать и хранить надёжные пароли

У Вас, конечно же, уже есть пароль, возможно даже несколько, но обязательно изучите это руководство, чтобы убедиться, что ваш пароль действительно является **сложным и надёжным**.

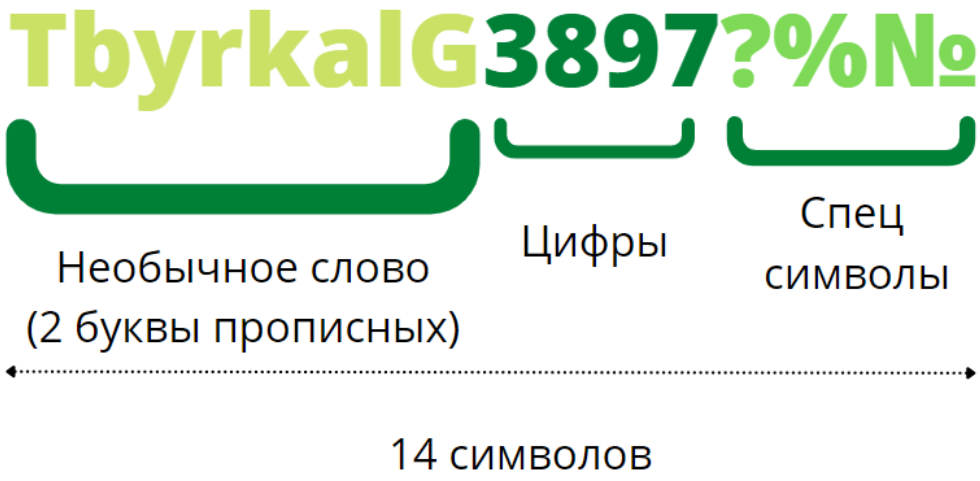
И да, Лаборатория Касперского рекомендует менять пароль каждые 3 месяца!

Правило 1. «СЛОЖНЫЙ» пароль

Все мы знаем, что пароль должен быть сложным, но что значит «**сложный**»?

1. **Хороший пароль** содержит **минимум 10 символов**, чтобы его было сложно взломать (посчитайте, сколько символов в вашем пароле к социальной сети?)
2. **Надёжный пароль** содержит **12 символов и более** (ваш пароль на основную почту должен быть именно таким длинным!).
3. **Сложный пароль** содержит **3 набора символов**: маленькие и БОЛЬШИЕ буквы, специальные символы и цифры: [**PochtiSlozhniyParol321!%**]
4. Пароль не должен содержать **общедоступную информацию** (имя, фамилию, дату рождения, никнейм, важные даты, номера телефонов, ИНН, адреса, как свои, так и родственников — **это не подходит для пароля**! [**PolinaYar1993** – плохой вариант])
5. В Пароле не используем **словарные слова, устойчивые выражения** и простые сочетания слов (используем малораспространённые слова или вообще несуществующие [**TbyrkalG**])

Пример сложного пароля:



Правило 2. На каждый сайт — уникальный пароль

«Зачем мне столько паролей?» - подумаете Вы. Но это действительно важно:

- **Самое важное в сети — это ваш e-mail**, так как почти все сервисы в Интернете привязаны к вашей электронной почте. А Ваша почта, или почта учреждения в **публичном доступе**. И если кто-то получит к ней доступ, то он автоматически получает доступ и ко всему остальному.
- **На ненадёжных сайтах e-mail и пароль хранятся рядом!** Если подобный сайт взломают, то первое что сделают — проверят, подходит ли пароль к вашему **e-mail**, затем попробуют авторизоваться в Вашем аккаунте социальной сети и средствам онлайн-оплаты.
- Злоумышленники продают **базы взломанных аккаунтов** друг другу, поэтому риск взлома всех ваших аккаунтов под одним паролем резко возрастает.

Как же обезопасить себя?

Можно разделить все сервисы на две группы:

1. Для обычных аккаунтов использовать более простые, похожие пароли. Можно делать приставку к стандартному паролю с названием сайта, на котором он будет использоваться;
2. Для важных аккаунтов (e-mail, админка Навигатора, интернет-банкинг,) использовать только сложные, уникальные пароли.

«А как запомнить такое количество сложных паролей?»

Правило 3. Храним пароль надёжно

Память не самый надёжный инструмент, поэтому лучше использовать проверенные способы надёжного хранения паролей.

1. **Бумажный блокнот** — да, даже ведущие специалисты по информационной безопасности не отвергают этот вариант. Только храните этот блокнот подальше от любопытных глаз, да и пароли храните в нём в понятном только Вам виде.
2. **Менеджер паролей** — специальная программа, которая запоминает пароли за Вас, нужно лишь помнить один пароль для доступа к остальной базе.
3. **Текстовый документ** — не самый лучший вариант хранения паролей, но и его можно использовать, если хранить документ безопасно: в архиве с паролем, хотя это уже вариант менеджера паролей.

И для каждого способа обязательно используем **резервное копирование**!

Как НЕЛЬЗЯ хранить пароли

1. На стикере, прикрепленному к монитору или бумажке, лежащей на столе под клавиатурой (есть прецеденты государственного масштаба)
2. В текстовом документе/блокноте на рабочем столе (или на флешке, карте памяти и т.д.)
3. В браузере хранить пароли не рекомендуется!
4. Никому не сообщайте и не отправляйте свои пароли!

В новостном репортаже показали пароль французской телесети TV5 Monde

Правило 4. Параметры восстановления пароля

Вашу почту могут попробовать взломать, попытавшись восстановить пароль. И, если у вас для восстановления доступа используется ответ на секретный вопрос, его могут угадать.

- **Ответ на секретный вопрос должен быть устойчивым к отгадыванию** (используем нелогичные ответы, например: **«Ваш любимый цвет» — «Вода»**)

Если для восстановления используется второй e-mail, все правила этого гайда тоже должны относиться к нему.

- **E-mail для восстановления тоже должен быть надёжно защищён** (проверьте параметры безопасности прямо сейчас, не откладывайте)

Зная эти правила,
можно приступать к созданию
<u>нового</u> сложного пароля.