• Псевдографика. Достаточно сложный, но хорошо запоминающийся пароль можно создать с помощью псевдографики — использования символов шрифта для создания графических изображений. Например, набор символов _>(0:o:0)<_ похож на кошачью мордочку.

Чтобы сделать надежный пароль, необходимо использовать несколько различных видов шифрования. Возьмем слово ПАРОЛЬ, транслитерируем — GFHJKM, добавим через одну букву шесть цифр, но в обратном порядке — G6F5H4J3K2M1, а теперь поменяем цифры через одну на соответствующие им символы — G6F%H4J#K2M!.
Одну и ту же систему шифрования можно использовать для разных паролей, добавив систему индексов, например: ПАРОЛЬMAIL.RU, ПАРОЛЬ GMAIL.COM, ПАРОЛЬVK.COM. Это существенно упростит процедуру запоминания паролей и сделает их достаточно надежными и безопасными.

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

Управление Роскомнадзора по Ростовской области

(863) 285-08-66
(863) 285-08-67

ул. Металлургическая, 113/46
г. Ростов-на-Дону, 344029

rsockanc61@rkn.gov.ru

61.rkn.gov.ru
pd.rkn.gov.ru
персональные данные. дети

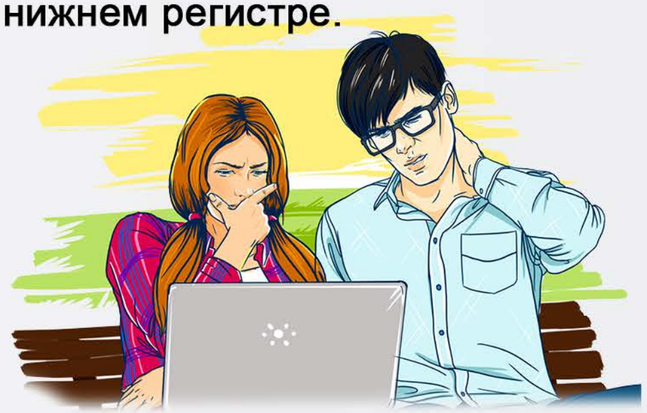
КАК ПРИДУМАТЬ НАДЕЖНЫЙ ПАРОЛЬ

БЕЗОПАСНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНТЕРНЕТЕ

ПРАВИЛА СОСТАВЛЕНИЯ НАДЕЖНЫХ ПАРОЛЕЙ

Признаки надежного пароля

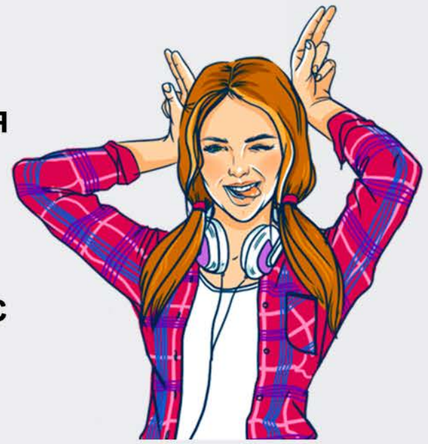
Надежный пароль должен:
– состоять из 8–16 символов;
– включать в себя буквы, цифры и специальные символы;
– включать в себя символы в верхнем и нижнем регистре.



• Не следует использовать слова, словосочетания, а также комбинации, которые можно легко угадать.
• Целесообразно использовать двухэтапную аутентификацию с помощью мобильного телефона.
• Для каждого аккаунта необходимо иметь свой пароль.
• Необходимо менять пароли ко всем аккаунтам раз в 3–6 месяцев.
• При столкновении с попыткой взлома одного из аккаунтов необходимо поменять пароли на всех аккаунтах.

СПОСОБЫ СОСТАВЛЕНИЯ НАДЕЖНОГО ПАРОЛЯ

Для получения сложного, но легко запоминающегося пароля можно использовать любое слово, зашифровав его с помощью одного из следующих методов:



• Транслитерация. Если взять любое слово русского языка и набрать его на клавиатуре с латинской раскладкой, то получится бессмысленное сочетание символов. Например, RJYUHTUFWBZ — это слово «конгрегация». К сожалению, этот метод плохо подходит для устройств с виртуальной клавиатурой, где отсутствует двойная подпись клавиш.
• Смещение по клавиатуре. Если при написании слова каждый раз смещаться по клавиатуре на одну клавишу влево, мы используем простое смещение, например ВПЬЦЩ — это слово «арбуз». Если менять направление смещения по или против часовой стрелки, мы используем сложное смещение, например ЛПТВЛПР — это слово «барабан».

СПОСОБЫ СОСТАВЛЕНИЯ НАДЕЖНОГО ПАРОЛЯ

• Акроним. Если взять первые буквы слов из известной фразы, то мы получаем акроним, который можно использовать в качестве пароля. Например МДСЧПКНВШЗ — это первые две строки из романа А.С. Пушкина «Евгений Онегин».
• Известные последовательности. Также для составления пароля можно использовать первые буквы известных последовательностей слов. Например, ЯФМАМИИАСОНД — это двенадцать месяцев. Всегда можно усложнить последовательность, например, изменив направление и величину шага. ДОАИАФНСИММЯ — это последовательность месяцев наоборот и через один.
• Чередования символов. Любой пароль можно усложнить, добавив последовательность цифр или знаков, которые можно чередовать с зашифрованным словом. Например П1А2 Р3О4Л5Ь6.