

объясняемрф



Головоломка для мошенника

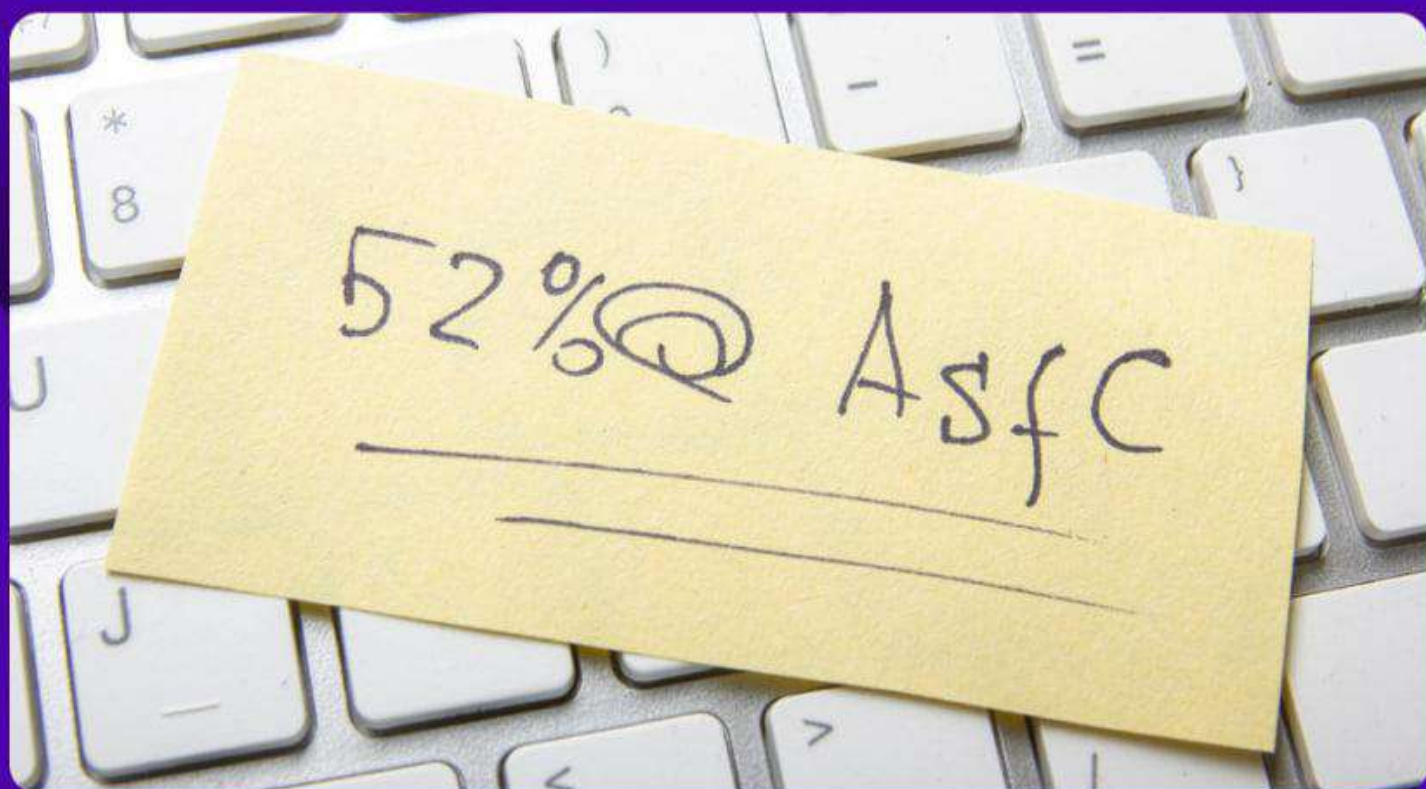
Как придумать
надёжный пароль?

Где не стоит хранить пароли:



- ✦ в приложении «Заметки» в телефоне
- ✦ в диалогах с самим собой в соцсетях и мессенджерах
- ✦ в автозаполнении браузера

Если злоумышленник сумеет получить доступ к вашим устройствам и соцсетям, **ему станут известны сразу все пароли.**



Как ещё можно обезопасить свои данные:

- ✦ **активируйте двухфакторную аутентификацию**, чтобы при входе нужно было вводить не только логин и пароль, но и одноразовый код из СМС или специального приложения
- ✦ раз в полгода, а лучше каждые три месяца **обновляйте пароли**, особенно от сервисов и приложений, где есть ваши личные данные
- ✦ **используйте менеджер паролей** — программу, которая помогает хранить все ключи в зашифрованном виде: вам достаточно будет запомнить только один



Примеры надёжных паролей:



dAmNmO!nAoViZPi?

- ✦ составлен по правилу: первые две буквы из каждого слова кодовой фразы **«Дай мне мороженого! На обед из Питера?»**
- ✦ пароль длинный — 16 символов
- ✦ используются спецсимволы: «!» и «?», прописные и строчные буквы

!NMnrsQ4VaGnJ-kK

- ✦ создан генератором паролей — **символы в случайном порядке**
- ✦ длина — 16 символов
- ✦ используются символы «!» и «-», прописные и строчные буквы

яроСТЬуткапростоЛуна

- ✦ основан на кодовой фразе, в которой есть **понятные, но не связанные между собой слова**
- ✦ длина — 20 символов

Как защитить свой аккаунт:



- ✦ **не используйте одни и те же пароли** в разных приложениях или аккаунтах
- ✦ **заменённые символы должно быть трудно угадать: не используйте, например, ноль вместо буквы «О»**
- ✦ **можно воспользоваться генератором паролей** — программой, сочетающей символы случайным образом

