№1

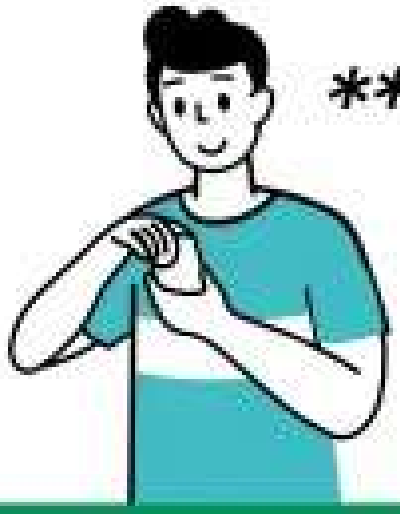
Не используйте в пароле собственные имя и фамилию, информацию о родственниках, клички животных и даты дней рождений

Часто мы размещаем эти данные в открытом доступе на страницах в социальных сетях. Потратив немного времени, злоумышленники вполне смогут все узнать и разгадать ваш пароль.

№2

Создавайте пароль длиной как минимум 10–12 символов. Добавляйте в него заглавные и строчные буквы, цифры и символы

Избегайте распространенных слов, составляя пароль. Даже если вы задействуете их, выбирайте те, которые не связаны по смыслу, расставляйте их нелогичным образом. Это поможет противостоять словарному подбору.



****

№3

Меняйте пароль хотя бы раз в месяц и не используйте один и тот же шифр в почте, интернет-банке, соцсетях и мессенджерах

Создавайте новый пароль так, чтобы он не был похож на предыдущий.
Менять в пароле лишь несколько символов – вредная привычка. Лучше придумать новый.

мои финансы

№4

Не забывайте обновлять антивирус и пользоваться двухфакторной аутентификацией

Такая процедура позволяет устроить дополнительную проверку безопасности после успешного ввода пароля. **Как правило, она требует доступа к данным, которые есть только у вас: sms, отпечаток пальца, Face ID.** Двухфакторная аутентификация не пропустит мошенников и злоумышленников в ваш аккаунт, даже если они украдут ваши пароли.

Как составить надёжный пароль?

Пример:

1. Берем фразу «*Черепаха хвост поджала и за зайцем побежала*».
2. Заменяем буквы «ч», «з» и «о» на схожие цифры.
3. Добавляем точку в конце фразы.
4. Пишем кириллицей, но в английской раскладке клавиатуры.

Итог: 4thtgf[f[d0cng0l;fkfb3f3fqwtvg0,t;fkf.

№5

Отдавайте предпочтение домашнему интернету, а не общественному Wi-Fi

По возможности подключайтесь только к известным открытым сетям, особенно если при подключении у вас спрашивают какую-либо личную информацию (адрес электронной почты, номер телефона). *Помните, что даже известные Wi-Fi-операторы не застрахованы от утечек данных, которые они собирают.*

мои финансы