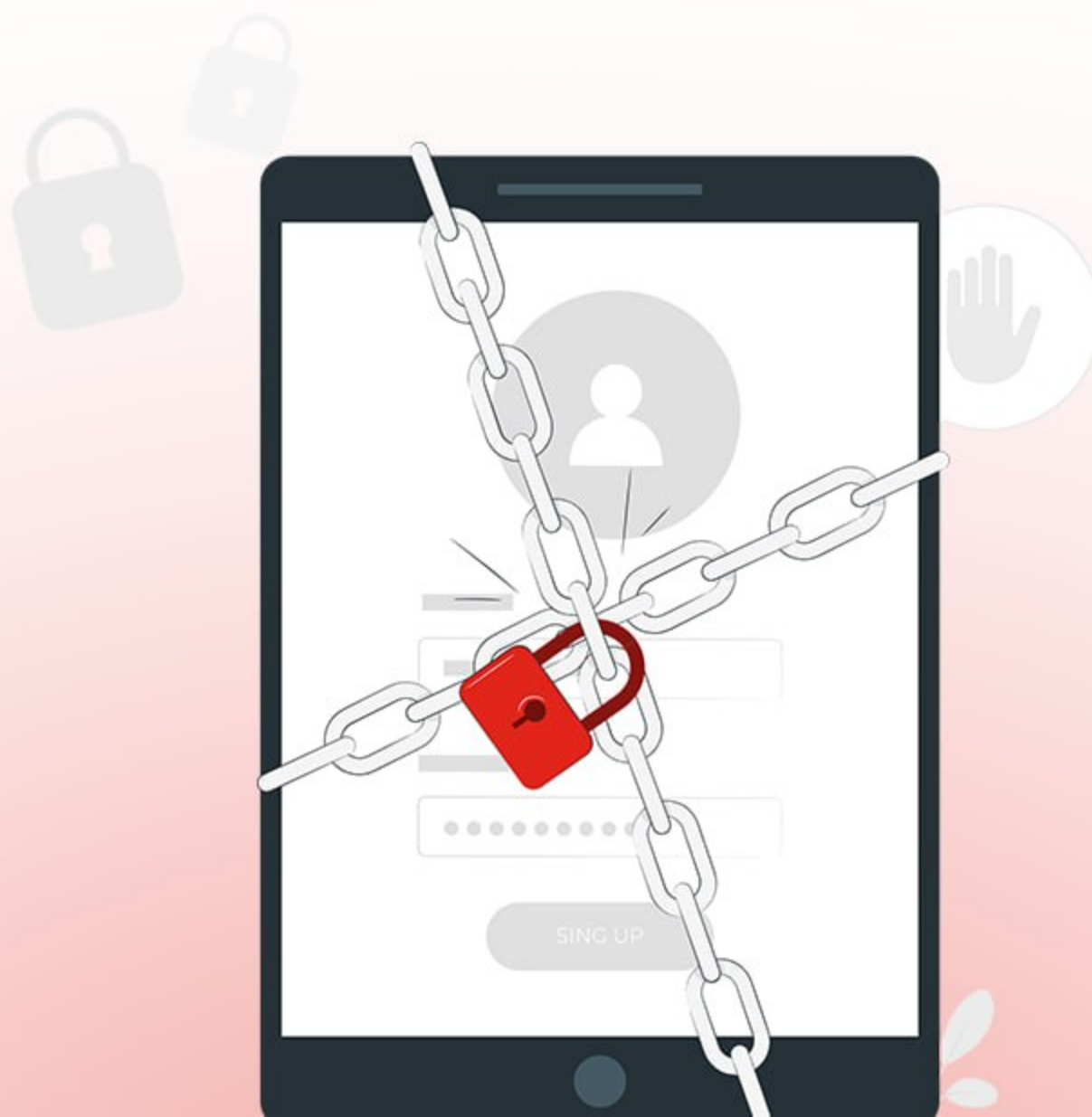




Как **не попасть** в лапы мошенников?

Основные правила безопасности





Не сообщайте никому финансовые сведения:

- данные банковской карты и её владельца,
- трехзначный код с обратной стороны карты или СМС-код.

Сотрудники банков и государственных структур никогда не запрашивают такую информацию. Не публикуйте её в социальных сетях, на форумах и каких-либо сайтах в Интернете, не храните данные карт и PIN-коды на компьютере или в смартфоне



Не доверяйте сообщениям о крупном выигрыше, победе в конкурсе или лотерее, особенно в случаях, когда для получения выигрыша просят оплатить налог.

Настоящий розыгрыш призов не должен подразумевать денежные выплаты с вашей стороны.



Не отправляйте денежные средства на неизвестные адреса, в том числе с целью приобретения вещей в сети Интернет



Не перезванивайте на номер, с которого пришло сообщение о блокировке карты, не отправляйте ответных СМС-сообщений.

Позвоните в банк, выпустивший и обслуживающий карту.



Когда вам звонят с неизвестных номеров и представляются сотрудниками банка, полиции, ФСБ, кладите трубку.

Официальные органы при необходимости всегда присылают повестку, а с банком можно связаться через горячую линию



Если вы купили новую сим-карту, сразу обновите информацию по всем аккаунтам, к которым был привязан старый номер.

Это займет минимум времени, но надежно защитит от мошенников.



Дополнительные рекомендации

- ◆ Не доверяйте подозрительным сообщениям, звонкам или запросам без должной проверки. Если возникают подозрения относительно какой-либо информации или запросов, свяжитесь напрямую с начальником, родственниками, другими людьми для уточнения ситуации.
- ◆ Придумайте проверочное слово или фразу, которую знают только члены вашей семьи. Это поможет подтвердить личность в Интернете или по телефону, если появится такая необходимость.



- ◆ Установите приложение, которое идентифицирует звонки и сообщения от незнакомых номеров или адресов. Такие приложения блокируют подозрительные звонки и сообщения, предотвращая возможные мошеннические атаки.
- ◆ Регулярно проверяйте активные сессии в своих мессенджерах и социальных сетях. Если обнаруживаете активные сеансы на неизвестных устройствах или местах, немедленно отключите их и измените пароли для безопасности.

