

Ваши действия:

- ▶ незамедлительно прекратить разговор и осмыслить ситуацию
- ▶ если остались сомнения, связаться с банком, правоохранительным органом или иной организацией по официальному номеру, набрав его самостоятельно, а не обратным звонком
- ▶ уточнить у оператора мобильной связи информацию о поступившем звонке
- ▶ позвонить близким, коллегам, если речь шла о них или сообщение поступило якобы от них

Что делать, если вас обманули?

1. Заблокируйте карту
2. Поменяйте пароли от личных кабинетов в банковских приложениях и Госуслугах
3. Обратитесь в полицию



Признаки телефонных мошенников

- ▶ сами связываются с вами, часто используют скрытые или подменные номера
- ▶ звонят на Viber, WhatsApp с номеров 900 или 1000
- ▶ запугивают или делают супер-выгодное предложение
- ▶ убеждают не завершать разговор
- ▶ торопят, требуют немедленно принять решение
- ▶ разговор касается денег
- ▶ просят сообщить информацию о банковской карте или другие персональные данные



Виды мошенничества

"Сотрудники службы безопасности банка или Госуслуг"

пугают взломом личного кабинета, говорят об утечке персональных данных, сообщают о попытке хищения денег или оформления онлайн-кредита

"Операторы мобильной связи"

предлагают переоформить или продлить договор, пугают отключением услуг

"Сотрудники полиции"

ведут расследование об утечке персональных данных, предлагают перевести сбережения на "безопасный счет", обвиняют в госизмене, просят содействия в задержании преступников

Ни в коем случае

- ▶ не сообщайте код из СМС, трехзначный код с обратной стороны карты или другие ПИН-коды
- ▶ не переводите деньги незнакомцам
- ▶ не переходите по ссылкам и не набирайте никаких комбинаций на телефоне
- ▶ не давайте дистанционный доступ к телефону или планшету и не включайте демонстрацию экрана



Виды мошенничества

- ▶ СМС-рассылки с сообщением или графическим изображением и ссылкой на неизвестный электронный адрес с поздравлением или просьбой проголосовать в конкурсе
- ▶ Малоознакомый человек отправляет ссылку на покупку билетов или оплату товаров на сервисе Авито
- ▶ Сообщения о внезапном крупном выигрыше, для получения которого необходимо оплатить комиссию или налог
- ▶ Сообщения об оформлении кредита, заявку на которую не подавали, со ссылкой для подтверждения или отказа
- ▶ Сообщения о переводе денежных средств при отсутствии их фактического зачисления



Помните!

- ▶ **Сотрудники банка, правоохранительных органов и иных организаций:**
 - не делают звонков в WhatsApp или Viber
 - не спрашивают реквизиты карты, код из СМС
 - не просят совершать денежные переводы

- ▶ **у вас всегда есть время обдумать ситуацию и посоветоваться с родными или друзьями**

- ▶ **всю информацию, поступающую от незнакомых лиц, необходимо перепроверять**



Кто такой дроппер?

- ▶ Это люди, с помощью которых мошенники обналичивают денежные средства, добытые преступным путем
- ▶ Они могут быть привлечены к ответственности наравне с мошенниками
- ▶ Дропперы являются гражданскими ответчиками по искам о взыскании ущерба, причиненного преступлением

И как им не стать?

- не отдавайте другим людям свои банковские карты или СИМ-карту
- возвращайте ошибочно перечисленные деньги только через заявление в банк